Form 5500

Department of the Treasury
Internal Revenue Service

Department of Labor
Employee Benefits Security Administration

Pension Benefit Guaranty Corporation

Annual Return/Report of Employee Benefit Plan

This form is required to be filed for employee benefit plans under sections 104 and 4065 of the Employee Retirement Income Security Act of 1974 (ERISA) and sections 6057(b) and 6058(a) of the Internal Revenue Code (the Code).

▶ **Complete all entries in accordance with the instructions to the Form 5500.**

OMB Nos. 1210-0110
1210-0089

2025

This Form is Open to Public Inspection

Part I Annual Report Identification Information

For calendar plan year 2025 or fiscal plan year beginning 01/01/2025 and ending 12/31/2025

A This return/report is for:
- [ ] a multiemployer plan
- [ ] a multiple-employer plan (Filers checking this box must provide participating employer information in accordance with the form instructions.)
- [X] a single-employer plan
- [ ] a DFE (specify) _____

B This return/report is:
- [ ] the first return/report
- [ ] the final return/report
- [ ] an amended return/report
- [ ] a short plan year return/report (less than 12 months)

C If the plan is a collectively-bargained plan, check here. . . . . ▶ [ ]

D Check box if filing under:
- [X] Form 5558
- [ ] automatic extension
- [ ] the DFVC program
- [ ] special extension (enter description)

E If this is a retroactively adopted plan permitted by SECURE Act section 201, check here. . . . . ▶ [ ]

Part II Basic Plan Information—enter all requested information

1a Name of plan
HENDRICKS COMMUNITY HOSPITAL ASSOCIATION 403(B) PLAN

1b Three-digit plan number (PN) ▶ 001

1c Effective date of plan 02/01/2007

2a Plan sponsor's name (employer, if for a single-employer plan)
Mailing address (include room, apt., suite no. and street, or P.O. Box)
City or town, state or province, country, and ZIP or foreign postal code (if foreign, see instructions)
HENDRICKS COMMUNITY HOSPITAL ASSOCIATION

503 EAST LINCOLN STREET
HENDRICKS, MN 56136

2b Employer Identification Number (EIN)
41-0307617

2c Plan Sponsor's telephone number
507-275-3134

2d Business code (see instructions)
622000

Caution: A penalty for the late or incomplete filing of this return/report will be assessed unless reasonable cause is established.

Under penalties of perjury and other penalties set forth in the instructions, I declare that I have examined this return/report, including accompanying schedules, statements and attachments, as well as the electronic version of this return/report, and to the best of my knowledge and belief, it is true, correct, and complete.

SIGN HERE	Filed with authorized/valid electronic signature.	10/06/2026	TRAVIS OLSEN
	Signature of plan administrator	Date	Enter name of individual signing as plan administrator
SIGN HERE			
	Signature of employer/plan sponsor	Date	Enter name of individual signing as employer or plan sponsor
SIGN HERE			
	Signature of DFE	Date	Enter name of individual signing as DFE

3a	Plan administrator's name and address [X] Same as Plan Sponsor	**3b**	Administrator's EIN
		3c	Administrator's telephone number
4	If the name and/or EIN of the plan sponsor or the plan name has changed since the last return/report filed for this plan, enter the plan sponsor's name, EIN, the plan name and the plan number from the last return/report:	**4b**	EIN
a	Sponsor's name	**4d**	PN
c	Plan Name		

5	Total number of participants at the beginning of the plan year	**5**	208
6	Number of participants as of the end of the plan year unless otherwise stated (welfare plans complete only lines **6a(1), 6a(2), 6b, 6c,** and **6d**).		
a(1)	Total number of active participants at the beginning of the plan year	**6a(1)**	175
a(2)	Total number of active participants at the end of the plan year	**6a(2)**	180
b	Retired or separated participants receiving benefits	**6b**	0
c	Other retired or separated participants entitled to future benefits	**6c**	30
d	Subtotal. Add lines **6a(2)**, **6b**, and **6c**.	**6d**	210
e	Deceased participants whose beneficiaries are receiving or are entitled to receive benefits.	**6e**	1
f	Total. Add lines **6d** and **6e**.	**6f**	211
g(1)	Number of participants with account balances as of the beginning of the plan year (only defined contribution plans complete this item)	**6g(1)**	123
g(2)	Number of participants with account balances as of the end of the plan year (only defined contribution plans complete this item)	**6g(2)**	117
h	Number of participants who terminated employment during the plan year with accrued benefits that were less than 100% vested.	**6h**	2
7	Enter the total number of employers obligated to contribute to the plan (only multiemployer plans complete this item)	**7**	

8a If the plan provides pension benefits, enter the applicable pension feature codes from the List of Plan Characteristic Codes in the instructions:

2F 2G 2L 2M 2T 3D

b If the plan provides welfare benefits, enter the applicable welfare feature codes from the List of Plan Characteristic Codes in the instructions:

9a Plan funding arrangement (check all that apply)		**9b** Plan benefit arrangement (check all that apply)	
(1)	[X] Insurance	**(1)**	[X] Insurance
(2)	[ ] Code section 412(e)(3) insurance contracts	**(2)**	[ ] Code section 412(e)(3) insurance contracts
(3)	[X] Trust	**(3)**	[X] Trust
(4)	[ ] General assets of the sponsor	**(4)**	[ ] General assets of the sponsor

10 Check all applicable boxes in 10a and 10b to indicate which schedules are attached, and, where indicated, enter the number attached. (See instructions)

a Pension Schedules

- **(1)** [X] **R** (Retirement Plan Information)
- **(2)** [ ] **MB** (Multiemployer Defined Benefit Plan and Certain Money Purchase Plan Actuarial Information) - signed by the plan actuary
- **(3)** [ ] **SB** (Single-Employer Defined Benefit Plan Actuarial Information) - signed by the plan actuary
- **(4)** [ ] **DCG** (Individual Plan Information) – Number Attached _____
- **(5)** [ ] **MEP** (Multiple-Employer Retirement Plan Information)

b General Schedules

- **(1)** [X] **H** (Financial Information)
- **(2)** [ ] **I** (Financial Information – Small Plan)
- **(3)** [ ] **A** (Insurance Information) – Number Attached _____
- **(4)** [X] **C** (Service Provider Information)
- **(5)** [ ] **D** (DFE/Participating Plan Information)
- **(6)** [ ] **G** (Financial Transaction Schedules)

Part III Form M-1 Compliance Information (to be completed by welfare benefit plans)

11a If the plan provides welfare benefits, was the plan subject to the Form M-1 filing requirements during the plan year? (See instructions and 29 CFR 2520.101-2.) ..... ☐ Yes ☐ No

If "Yes" is checked, complete lines 11b and 11c.

11b Is the plan currently in compliance with the Form M-1 filing requirements? (See instructions and 29 CFR 2520.101-2.) ..... ☐ Yes ☐ No

11c Enter the Receipt Confirmation Code for the 2025 Form M-1 annual report. If the plan was not required to file the 2025 Form M-1 annual report, enter the Receipt Confirmation Code for the most recent Form M-1 that was required to be filed under the Form M-1 filing requirements. (Failure to enter a valid Receipt Confirmation Code will subject the Form 5500 filing to rejection as incomplete.)

Receipt Confirmation Code_____

SCHEDULE C (Form 5500)	Service Provider Information	OMB No. 1210-0110
Department of the Treasury Internal Revenue Service Department of Labor Employee Benefits Security Administration Pension Benefit Guaranty Corporation	This schedule is required to be filed under section 104 of the Employee Retirement Income Security Act of 1974 (ERISA). ▶ **File as an attachment to Form 5500.**	**2025** **This Form is Open to Public Inspection.**

For calendar plan year 2025 or fiscal plan year beginning 01/01/2025 and ending 12/31/2025

A Name of plan
HENDRICKS COMMUNITY HOSPITAL ASSOCIATION 403(B) PLAN

B Three-digit plan number (PN) ▶ 001

C Plan sponsor's name as shown on line 2a of Form 5500
HENDRICKS COMMUNITY HOSPITAL ASSOCIATION

D Employer Identification Number (EIN)
41-0307617

Part I Service Provider Information (see instructions)

You must complete this Part, in accordance with the instructions, to report the information required for **each person** who received, directly or indirectly, $5,000 or more in total compensation (i.e., money or anything else of monetary value) in connection with services rendered to the plan or the person's position with the plan during the plan year. If a person received **only** eligible indirect compensation for which the plan received the required disclosures, you are required to answer line 1 but are not required to include that person when completing the remainder of this Part.

1 Information on Persons Receiving Only Eligible Indirect Compensation

a Check "Yes" or "No" to indicate whether you are excluding a person from the remainder of this Part because they received only eligible indirect compensation for which the plan received the required disclosures (see instructions for definitions and conditions).. . . . . ☐ Yes ☒ No

b If you answered line 1a "Yes," enter the name and EIN or address of each person providing the required disclosures for the service providers who received only eligible indirect compensation. Complete as many entries as needed (see instructions).

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

(b) Enter name and EIN or address of person who provided you disclosures on eligible indirect compensation

2. Information on Other Service Providers Receiving Direct or Indirect Compensation. Except for those persons for whom you answered "Yes" to line 1a above, complete as many entries as needed to list each person receiving, directly or indirectly, $5,000 or more in total compensation (i.e., money or anything else of value) in connection with services rendered to the plan or their position with the plan during the plan year. (See instructions).

(a) Enter name and EIN or address (see instructions)

LPL FINANCIAL

75 STATE STREET
22ND FLOOR
BOSTON, MA 02109

(b) Service Code(s)	(c) Relationship to employer, employee organization, or person known to be a party-in-interest	(d) Enter direct compensation paid by the plan. If none, enter -0-.	(e) Did service provider receive indirect compensation? (sources other than plan or plan sponsor)	(f) Did indirect compensation include eligible indirect compensation, for which the plan received the required disclosures?	(g) Enter total indirect compensation received by service provider excluding eligible indirect compensation for which you answered "Yes" to element (f). If none, enter -0-.	(h) Did the service provider give you a formula instead of an amount or estimated amount?
27 50		20428	Yes [ ] No [X]	Yes [ ] No [ ]		Yes [ ] No [ ]

(a) Enter name and EIN or address (see instructions)

NEWPORT GROUP, INC.

27-2037969

(b) Service Code(s)	(c) Relationship to employer, employee organization, or person known to be a party-in-interest	(d) Enter direct compensation paid by the plan. If none, enter -0-.	(e) Did service provider receive indirect compensation? (sources other than plan or plan sponsor)	(f) Did indirect compensation include eligible indirect compensation, for which the plan received the required disclosures?	(g) Enter total indirect compensation received by service provider excluding eligible indirect compensation for which you answered "Yes" to element (f). If none, enter -0-.	(h) Did the service provider give you a formula instead of an amount or estimated amount?
99 37 64 50 15		18380	Yes [X] No [ ]	Yes [X] No [ ]	0	Yes [ ] No [X]

(a) Enter name and EIN or address (see instructions)

(b) Service Code(s)	(c) Relationship to employer, employee organization, or person known to be a party-in-interest	(d) Enter direct compensation paid by the plan. If none, enter -0-.	(e) Did service provider receive indirect compensation? (sources other than plan or plan sponsor)	(f) Did indirect compensation include eligible indirect compensation, for which the plan received the required disclosures?	(g) Enter total indirect compensation received by service provider excluding eligible indirect compensation for which you answered "Yes" to element (f). If none, enter -0-.	(h) Did the service provider give you a formula instead of an amount or estimated amount?
			Yes [ ] No [ ]	Yes [ ] No [ ]		Yes [ ] No [ ]

Part I Service Provider Information (continued)

3. If you reported on line 2 receipt of indirect compensation, other than eligible indirect compensation, by a service provider, and the service provider is a fiduciary or provides contract administrator, consulting, custodial, investment advisory, investment management, broker, or recordkeeping services, answer the following questions for (a) each source from whom the service provider received $1,000 or more in indirect compensation and (b) each source for whom the service provider gave you a formula used to determine the indirect compensation instead of an amount or estimated amount of the indirect compensation. Complete as many entries as needed to report the required information for each source.

(a) Enter service provider name as it appears on line 2	**(b)** Service Codes (see instructions)	**(c)** Enter amount of indirect compensation
(d) Enter name and EIN (address) of source of indirect compensation	**(e)** Describe the indirect compensation, including any formula used to determine the service provider's eligibility for or the amount of the indirect compensation.	

(a) Enter service provider name as it appears on line 2	**(b)** Service Codes (see instructions)	**(c)** Enter amount of indirect compensation
(d) Enter name and EIN (address) of source of indirect compensation	**(e)** Describe the indirect compensation, including any formula used to determine the service provider's eligibility for or the amount of the indirect compensation.	

(a) Enter service provider name as it appears on line 2	**(b)** Service Codes (see instructions)	**(c)** Enter amount of indirect compensation
(d) Enter name and EIN (address) of source of indirect compensation	**(e)** Describe the indirect compensation, including any formula used to determine the service provider's eligibility for or the amount of the indirect compensation.	

Part II Service Providers Who Fail or Refuse to Provide Information

4 Provide, to the extent possible, the following information for each service provider who failed or refused to provide the information necessary to complete this Schedule.

(a) Enter name and EIN or address of service provider (see instructions)	**(b)** Nature of Service Code(s)	**(c)** Describe the information that the service provider failed or refused to provide

(a) Enter name and EIN or address of service provider (see instructions)	**(b)** Nature of Service Code(s)	**(c)** Describe the information that the service provider failed or refused to provide

(a) Enter name and EIN or address of service provider (see instructions)	**(b)** Nature of Service Code(s)	**(c)** Describe the information that the service provider failed or refused to provide

(a) Enter name and EIN or address of service provider (see instructions)	**(b)** Nature of Service Code(s)	**(c)** Describe the information that the service provider failed or refused to provide

(a) Enter name and EIN or address of service provider (see instructions)	**(b)** Nature of Service Code(s)	**(c)** Describe the information that the service provider failed or refused to provide

(a) Enter name and EIN or address of service provider (see instructions)	**(b)** Nature of Service Code(s)	**(c)** Describe the information that the service provider failed or refused to provide

Part III Termination Information on Accountants and Enrolled Actuaries (see instructions)

(complete as many entries as needed)

a Name:

b EIN:

c Position:

d Address:

e Telephone:

Explanation:

a Name:

b EIN:

c Position:

d Address:

e Telephone:

Explanation:

a Name:

b EIN:

c Position:

d Address:

e Telephone:

Explanation:

a Name:

b EIN:

c Position:

d Address:

e Telephone:

Explanation:

a Name:

b EIN:

c Position:

d Address:

e Telephone:

Explanation:

SCHEDULE H (Form 5500)

Department of the Treasury
Internal Revenue Service

Department of Labor
Employee Benefits Security Administration

Pension Benefit Guaranty Corporation

Financial Information

This schedule is required to be filed under section 104 of the Employee Retirement Income Security Act of 1974 (ERISA), and section 6058(a) of the Internal Revenue Code (the Code).

▶ **File as an attachment to Form 5500.**

OMB No. 1210-0110

2025

This Form is Open to Public Inspection

For calendar plan year 2025 or fiscal plan year beginning 01/01/2025 and ending 12/31/2025

A Name of plan
HENDRICKS COMMUNITY HOSPITAL ASSOCIATION 403(B) PLAN

B Three-digit plan number (PN) ▶ 001

C Plan sponsor's name as shown on line 2a of Form 5500
HENDRICKS COMMUNITY HOSPITAL ASSOCIATION

D Employer Identification Number (EIN)
41-0307617

Part I Asset and Liability Statement

1 Current value of plan assets and liabilities at the beginning and end of the plan year. Combine the value of plan assets held in more than one trust. Report the value of the plan's interest in a commingled fund containing the assets of more than one plan on a line-by-line basis unless the value is reportable on lines 1c(9) through 1c(14). Do not enter the value of that portion of an insurance contract which guarantees, during this plan year, to pay a specific dollar benefit at a future date. **Round off amounts to the nearest dollar.** MTIAs, CCTs, PSAs, and 103-12 IEs do not complete lines 1b(1), 1b(2), 1c(8), 1g, 1h, and 1i. CCTs, PSAs, and 103-12 IEs also do not complete lines 1d and 1e. See instructions.

Assets		(a) Beginning of Year	(b) End of Year
a Total noninterest-bearing cash	1a	35	0
b Receivables (less allowance for doubtful accounts):			
(1) Employer contributions	1b(1)		
(2) Participant contributions	1b(2)		
(3) Other	1b(3)		
c General investments:			
(1) Interest-bearing cash (include money market accounts & certificates of deposit)	1c(1)	252964	417209
(2) U.S. Government securities	1c(2)		
(3) Corporate debt instruments (other than employer securities):			
(A) Preferred	1c(3)(A)		
(B) All other	1c(3)(B)		
(4) Corporate stocks (other than employer securities):			
(A) Preferred	1c(4)(A)		
(B) Common	1c(4)(B)		
(5) Partnership/joint venture interests	1c(5)		
(6) Real estate (other than employer real property)	1c(6)		
(7) Loans (other than to participants)	1c(7)		
(8) Participant loans	1c(8)	82410	95272
(9) Value of interest in common/collective trusts	1c(9)		
(10) Value of interest in pooled separate accounts	1c(10)		
(11) Value of interest in master trust investment accounts	1c(11)		
(12) Value of interest in 103-12 investment entities	1c(12)		
(13) Value of interest in registered investment companies (e.g., mutual funds)	1c(13)	6615117	6810321
(14) Value of funds held in insurance company general account (unallocated contracts)	1c(14)		
(15) Other	1c(15)		

		(a) Beginning of Year	(b) End of Year
1d Employer-related investments:			
(1) Employer securities	1d(1)		
(2) Employer real property	1d(2)		
1e Buildings and other property used in plan operation	1e		
1f Total assets (add all amounts in lines 1a through 1e)	1f	6950526	7322802
Liabilities			
1g Benefit claims payable	1g		
1h Operating payables	1h		
1i Acquisition indebtedness	1i		
1j Other liabilities	1j		
1k Total liabilities (add all amounts in lines 1g through1j)	1k		
Net Assets			
1l Net assets (subtract line 1k from line 1f)	1l	6950526	7322802

Part II Income and Expense Statement

2 Plan income, expenses, and changes in net assets for the year. Include all income and expenses of the plan, including any trust(s) or separately maintained fund(s) and any payments/receipts to/from insurance carriers. Round off amounts to the nearest dollar. MTIAs, CCTs, PSAs, and 103-12 IEs do not complete lines 2a, 2b(1)(E), 2e, 2f, and 2g.

Income		(a) Amount	(b) Total
a Contributions:			
(1) Received or receivable in cash from: **(A)** Employers	2a(1)(A)	181921	
(B) Participants	2a(1)(B)	327047	
(C) Others (including rollovers)	2a(1)(C)	17895	
(2) Noncash contributions	2a(2)		
(3) Total contributions. Add lines **2a(1)(A), (B), (C),** and line **2a(2)**	2a(3)		526863
b Earnings on investments:			
(1) Interest:			
(A) Interest-bearing cash (including money market accounts and certificates of deposit)	2b(1)(A)	15569	
(B) U.S. Government securities	2b(1)(B)		
(C) Corporate debt instruments	2b(1)(C)		
(D) Loans (other than to participants)	2b(1)(D)	0	
(E) Participant loans	2b(1)(E)	7244	
(F) Other	2b(1)(F)		
(G) Total interest. Add lines **2b(1)(A)** through **(F)**	2b(1)(G)		22813
(2) Dividends: **(A)** Preferred stock	2b(2)(A)		
(B) Common stock	2b(2)(B)		
(C) Registered investment company shares (e.g. mutual funds)	2b(2)(C)	131923	
(D) Total dividends. Add lines **2b(2)(A)**, **(B)**, and **(C)**	2b(2)(D)		131923
(3) Rents	2b(3)		
(4) Net gain (loss) on sale of assets: **(A)** Aggregate proceeds	2b(4)(A)		
(B) Aggregate carrying amount (see instructions)	2b(4)(B)		
(C) Subtract line **2b(4)(B)** from line **2b(4)(A)** and enter result	2b(4)(C)		
(5) Unrealized appreciation (depreciation) of assets: **(A)** Real estate	2b(5)(A)		
(B) Other	2b(5)(B)		
(C) Total unrealized appreciation of assets. Add lines **2b(5)(A)** and **(B)**	2b(5)(C)		

		(a) Amount	(b) Total
(6) Net investment gain (loss) from common/collective trusts	2b(6)		
(7) Net investment gain (loss) from pooled separate accounts	2b(7)		
(8) Net investment gain (loss) from master trust investment accounts	2b(8)		
(9) Net investment gain (loss) from 103-12 investment entities	2b(9)		
(10) Net investment gain (loss) from registered investment companies (e.g., mutual funds)	2b(10)		933181
c Other income	2c		
d Total income. Add all **income** amounts in column (b) and enter total	2d		1614780
Expenses			
e Benefit payment and payments to provide benefits:			
(1) Directly to participants or beneficiaries, including direct rollovers	2e(1)	1202725	
(2) To insurance carriers for the provision of benefits	2e(2)		
(3) Other	2e(3)		
(4) Total benefit payments. Add lines **2e(1)** through **(3)**	2e(4)		1202725
f Corrective distributions (see instructions)	2f		
g Certain deemed distributions of participant loans (see instructions)	2g		971
h Interest expense	2h		
i Administrative expenses:			
(1) Salaries and allowances	2i(1)		
(2) Contract administrator fees	2i(2)	18380	
(3) Recordkeeping fees	2i(3)		
(4) IQPA audit fees	2i(4)		
(5) Investment advisory and investment management fees	2i(5)	20428	
(6) Bank or trust company trustee/custodial fees	2i(6)		
(7) Actuarial fees	2i(7)		
(8) Legal fees	2i(8)		
(9) Valuation/appraisal fees	2i(9)		
(10) Other trustee fees and expenses	2i(10)		
(11) Other expenses	2i(11)		
(12) Total administrative expenses. Add lines **2i(1)** through **(11)**	2i(12)		38808
j Total expenses. Add all **expense** amounts in column (b) and enter total	2j		1242504
Net Income and Reconciliation			
k Net income (loss). Subtract line **2j** from line **2d**	2k		372276
l Transfers of assets:			
(1) To this plan	2l(1)		
(2) From this plan	2l(2)		

Part III Accountant's Opinion

3 Complete lines 3a through 3c if the opinion of an independent qualified public accountant is attached to this Form 5500. Complete line 3d if an opinion is not attached.

a The attached opinion of an independent qualified public accountant for this plan is (see instructions):

(1) [X] Unmodified **(2)** [ ] Qualified **(3)** [ ] Disclaimer **(4)** [ ] Adverse

b Check the appropriate box(es) to indicate whether the IQPA performed an ERISA section 103(a)(3)(C) audit. Check both boxes (1) and (2) if the audit was performed pursuant to both 29 CFR 2520.103-8 and 29 CFR 2520.103-12(d). Check box (3) if pursuant to neither.

(1) [X] DOL Regulation 2520.103-8 **(2)** [ ] DOL Regulation 2520.103-12(d) **(3)** [ ] neither DOL Regulation 2520.103-8 nor DOL Regulation 2520.103-12(d).

c Enter the name and EIN of the accountant (or accounting firm) below:

(1) Name: ABDO, LLP **(2)** EIN: 41-1397419

d The opinion of an independent qualified public accountant is **not attached** as part of Schedule H because:

(1) [ ] This form is filed for a CCT, PSA, DCG or MTIA. **(2)** [ ] It will be attached to the next Form 5500 pursuant to 29 CFR 2520.104-50.

Part IV Compliance Questions

4 CCTs and PSAs do not complete Part IV. MTIAs, 103-12 IEs, and GIAs do not complete lines 4a, 4e, 4f, 4g, 4h, 4k, 4m, 4n, or 5. 103-12 IEs also do not complete lines 4j and 4l. MTIAs also do not complete line 4l. DCGs do not complete lines 4e, 4f, 4k, 4l, and 5, and DCGs generally complete the rest of Part IV collectively for all plans in the DCG, except as otherwise provided (see instructions).

During the plan year:

		Yes	No	Amount
a Was there a failure to transmit to the plan any participant contributions within the time period described in 29 CFR 2510.3-102? Continue to answer "Yes" for any prior year failures until fully corrected. (See instructions and DOL's Voluntary Fiduciary Correction Program.)	**4a**		X	
b Were any loans by the plan or fixed income obligations due the plan in default as of the close of the plan year or classified during the year as uncollectible? Disregard participant loans secured by participant's account balance. (Attach Schedule G (Form 5500) Part I if "Yes" is checked.)	**4b**		X	
c Were any leases to which the plan was a party in default or classified during the year as uncollectible? (Attach Schedule G (Form 5500) Part II if "Yes" is checked.)	**4c**		X	
d Were there any nonexempt transactions with any party-in-interest? (Do not include transactions reported on line 4a. Attach Schedule G (Form 5500) Part III if "Yes" is checked.)	**4d**		X	
e Was this plan covered by a fidelity bond?	**4e**	X		1000000
f Did the plan have a loss, whether or not reimbursed by the plan's fidelity bond, that was caused by fraud or dishonesty?	**4f**		X	
g Did the plan hold any assets whose current value was neither readily determinable on an established market nor set by an independent third party appraiser?	**4g**		X	
h Did the plan receive any noncash contributions whose value was neither readily determinable on an established market nor set by an independent third party appraiser?	**4h**		X	
i Did the plan have assets held for investment? (Attach schedule(s) of assets if "Yes" is checked, and see instructions for format requirements.)	**4i**	X		
j Were any plan transactions or series of transactions in excess of 5% of the current value of plan assets? (Attach schedule of transactions if "Yes" is checked and see instructions for format requirements.)	**4j**		X	
k Were all the plan assets either distributed to participants or beneficiaries, transferred to another plan, or brought under the control of the PBGC?	**4k**		X	
l Has the plan failed to provide any benefit when due under the plan?	**4l**		X	
m If this is an individual account plan, was there a blackout period? (See instructions and 29 CFR 2520.101-3.)	**4m**		X	
n If 4m was answered "Yes," check the "Yes" box if you either provided the required notice or one of the exceptions to providing the notice applied under 29 CFR 2520.101-3.	**4n**			

5a Has a resolution to terminate the plan been adopted during the plan year or any prior plan year? [ ] Yes [X] No

If "Yes," enter the amount of any plan assets that reverted to the employer this year _____.

5b If, during this plan year, any assets or liabilities were transferred from this plan to another plan(s), identify the plan(s) to which assets or liabilities were transferred. (See instructions.)

5b(1) Name of plan(s)	**5b(2)** EIN(s)	**5b(3)** PN(s)

5c Was the plan a defined benefit plan covered under the PBGC insurance program at any time during this plan year? (See ERISA section 4021 and instructions.) ..... ☐ Yes ☐ No ☐ Not determined

If "Yes" is checked, enter the My PAA confirmation number from the PBGC premium filing for this plan year _____.

SCHEDULE R (Form 5500)

Department of the Treasury
Internal Revenue Service

Department of Labor
Employee Benefits Security Administration

Pension Benefit Guaranty Corporation

Retirement Plan Information

This schedule is required to be filed under sections 104 and 4065 of the Employee Retirement Income Security Act of 1974 (ERISA) and section 6058(a) of the Internal Revenue Code (the Code).

▶ **File as an attachment to Form 5500.**

OMB No. 1210-0110

2025

This Form is Open to Public Inspection.

For calendar plan year 2025 or fiscal plan year beginning 01/01/2025 and ending 12/31/2025

A Name of plan
HENDRICKS COMMUNITY HOSPITAL ASSOCIATION 403(B) PLAN

B Three-digit plan number (PN) ▶ 001

C Plan sponsor's name as shown on line 2a of Form 5500
HENDRICKS COMMUNITY HOSPITAL ASSOCIATION

D Employer Identification Number (EIN)
41-0307617

Part I Distributions

All references to distributions relate only to payments of benefits during the plan year.

1 Total value of distributions paid in property other than in cash or the forms of property specified in the instructions ..... | 1 | 0

2 Enter the EIN(s) of payor(s) who paid benefits on behalf of the plan to participants or beneficiaries during the year (if more than two, enter EINs of the two payors who paid the greatest dollar amounts of benefits):

EIN(s): 75-3182674

Profit-sharing plans, ESOPs, and stock bonus plans, skip line 3.

3 Number of participants (living or deceased) whose benefits were distributed in a single sum, during the plan year ..... | 3 |

Part II Funding Information (If the plan is not subject to the minimum funding requirements of section 412 of the Internal Revenue Code or ERISA section 302, skip this Part.)

4 Is the plan administrator making an election under Code section 412(d)(2) or ERISA section 302(d)(2)? ..... ☐ Yes ☐ No ☐ N/A

If the plan is a defined benefit plan, go to line 8.

5 If a waiver of the minimum funding standard for a prior year is being amortized in this plan year, see instructions and enter the date of the ruling letter granting the waiver. **Date:** Month _____ Day _____ Year _____

If you completed line 5, complete lines 3, 9, and 10 of Schedule MB and do not complete the remainder of this schedule.

6	a	Enter the minimum required contribution for this plan year (include any prior year accumulated funding deficiency not waived)	6a	
	b	Enter the amount contributed by the employer to the plan for this plan year	6b	
	c	Subtract the amount in line 6b from the amount in line 6a. Enter the result (enter a minus sign to the left of a negative amount)	6c	

If you completed line 6c, skip lines 8 and 9.

7 Will the minimum funding amount reported on line 6c be met by the funding deadline? ..... ☐ Yes ☐ No ☐ N/A

8 If a change in actuarial cost method was made for this plan year pursuant to a revenue procedure or other authority providing automatic approval for the change or a class ruling letter, does the plan sponsor or plan administrator agree with the change? ..... ☐ Yes ☐ No ☐ N/A

Part III Amendments

9 If this is a defined benefit pension plan, were any amendments adopted during this plan year that increased or decreased the value of benefits? If yes, check the appropriate box. If no, check the "No" box. ..... ☐ Increase ☐ Decrease ☐ Both ☐ No

Part IV ESOPs (see instructions). If this is not a plan described under section 409(a) or 4975(e)(7) of the Internal Revenue Code, skip this Part.

10 Were unallocated employer securities or proceeds from the sale of unallocated securities used to repay any exempt loan? ..... ☐ Yes ☐ No

11 a Does the ESOP hold any preferred stock? ..... ☐ Yes ☐ No

b If the ESOP has an outstanding exempt loan with the employer as lender, is such loan part of a "back-to-back" loan? (See instructions for definition of "back-to-back" loan.) ..... ☐ Yes ☐ No

12 Does the ESOP hold any stock that is not readily tradable on an established securities market? ..... ☐ Yes ☐ No

Part V Additional Information for Multiemployer Defined Benefit Pension Plans

13 Enter the following information for each employer that (1) contributed more than 5% of total contributions to the plan during the plan year or (2) was one of the top-ten highest contributors (measured in dollars). See instructions. *Complete as many entries as needed to report all applicable employers.*

a Name of contributing employer

b EIN **c** Dollar amount contributed by employer

d Date collective bargaining agreement expires *(If employer contributes under more than one collective bargaining agreement, check box* ☐ *and see instructions regarding required attachment. Otherwise, enter the applicable date.)* Month _____ Day _____ Year _____

e Contribution rate information *(If more than one rate applies, check this box* ☐ *and see instructions regarding required attachment. Otherwise, complete lines 13e(1) and 13e(2).)*
(1) Contribution rate (in dollars and cents) _____
(2) Base unit measure: ☐ Hourly ☐ Weekly ☐ Unit of production ☐ Other (specify):

---

a Name of contributing employer

b EIN **c** Dollar amount contributed by employer

d Date collective bargaining agreement expires *(If employer contributes under more than one collective bargaining agreement, check box* ☐ *and see instructions regarding required attachment. Otherwise, enter the applicable date.)* Month _____ Day _____ Year _____

e Contribution rate information *(If more than one rate applies, check this box* ☐ *and see instructions regarding required attachment. Otherwise, complete lines 13e(1) and 13e(2).)*
(1) Contribution rate (in dollars and cents) _____
(2) Base unit measure: ☐ Hourly ☐ Weekly ☐ Unit of production ☐ Other (specify): _____

---

a Name of contributing employer

b EIN **c** Dollar amount contributed by employer

d Date collective bargaining agreement expires *(If employer contributes under more than one collective bargaining agreement, check box* ☐ *and see instructions regarding required attachment. Otherwise, enter the applicable date.)* Month _____ Day _____ Year _____

e Contribution rate information *(If more than one rate applies, check this box* ☐ *and see instructions regarding required attachment. Otherwise, complete lines 13e(1) and 13e(2).)*
(1) Contribution rate (in dollars and cents) _____
(2) Base unit measure: ☐ Hourly ☐ Weekly ☐ Unit of production ☐ Other (specify): _____

---

a Name of contributing employer

b EIN **c** Dollar amount contributed by employer

d Date collective bargaining agreement expires *(If employer contributes under more than one collective bargaining agreement, check box* ☐ *and see instructions regarding required attachment. Otherwise, enter the applicable date.)* Month _____ Day _____ Year _____

e Contribution rate information *(If more than one rate applies, check this box* ☐ *and see instructions regarding required attachment. Otherwise, complete lines 13e(1) and 13e(2).)*
(1) Contribution rate (in dollars and cents) _____
(2) Base unit measure: ☐ Hourly ☐ Weekly ☐ Unit of production ☐ Other (specify): _____

---

a Name of contributing employer

b EIN **c** Dollar amount contributed by employer

d Date collective bargaining agreement expires *(If employer contributes under more than one collective bargaining agreement, check box* ☐ *and see instructions regarding required attachment. Otherwise, enter the applicable date.)* Month _____ Day _____ Year _____

e Contribution rate information *(If more than one rate applies, check this box* ☐ *and see instructions regarding required attachment. Otherwise, complete lines 13e(1) and 13e(2).)*
(1) Contribution rate (in dollars and cents) _____
(2) Base unit measure: ☐ Hourly ☐ Weekly ☐ Unit of production ☐ Other (specify): _____

---

a Name of contributing employer

b EIN **c** Dollar amount contributed by employer

d Date collective bargaining agreement expires *(If employer contributes under more than one collective bargaining agreement, check box* ☐ *and see instructions regarding required attachment. Otherwise, enter the applicable date.)* Month _____ Day _____ Year _____

e Contribution rate information *(If more than one rate applies, check this box* ☐ *and see instructions regarding required attachment. Otherwise, complete lines 13e(1) and 13e(2).)*
(1) Contribution rate (in dollars and cents) _____
(2) Base unit measure: ☐ Hourly ☐ Weekly ☐ Unit of production ☐ Other (specify): _____

14 Enter the number of deferred vested and retired participants (inactive participants), as of the beginning of the plan year, whose contributing employer is no longer making contributions to the plan for:

a The current plan year. Check the box to indicate the counting method used to determine the number of inactive participants: ☐ last contributing employer ☐ alternative ☐ reasonable approximation (see instructions for required attachment)	**14a**	
b The plan year immediately preceding the current plan year. ☐ Check the box if the number reported is a change from what was previously reported (see instructions for required attachment)	**14b**	
c The second preceding plan year. ☐ Check the box if the number reported is a change from what was previously reported (see instructions for required attachment)	**14c**	

15 Enter the ratio of the number of participants under the plan on whose behalf no employer had an obligation to make an employer contribution during the current plan year to:

a The corresponding number for the plan year immediately preceding the current plan year	**15a**	
b The corresponding number for the second preceding plan year	**15b**	

16 Information with respect to any employers who withdrew from the plan during the preceding plan year:

a Enter the number of employers who withdrew during the preceding plan year	**16a**	
b If line 16a is greater than 0, enter the aggregate amount of withdrawal liability assessed or estimated to be assessed against such withdrawn employers	**16b**	

17 If assets and liabilities from another plan have been transferred to or merged with this plan during the plan year, check box and see instructions regarding supplemental information to be included as an attachment ☐

Part VI Additional Information for Single-Employer and Multiemployer Defined Benefit Pension Plans

18 If any liabilities to participants or their beneficiaries under the plan as of the end of the plan year consist (in whole or in part) of liabilities to such participants and beneficiaries under two or more pension plans as of immediately before such plan year, check box and see instructions regarding supplemental information to be included as an attachment ☐

19 If the total number of participants is 1,000 or more, complete lines (a) and (b):

a Enter the percentage of plan assets held as:
Public Equity: _____% Private Equity: _____% Investment-Grade Debt and Interest Rate Hedging Assets: _____%
High-Yield Debt: _____% Real Assets: _____% Cash or Cash Equivalents: _____% Other: _____%

b Provide the average duration of the Investment-Grade Debt and Interest Rate Hedging Assets:
☐ 0-5 years ☐ 5-10 years ☐ 10-15 years ☐ 15 years or more

20 **PBGC missed contribution reporting requirements.** If this is a multiemployer plan or a single-employer plan that is not covered by PBGC, skip line 20.

a Is the amount of unpaid minimum required contributions for all years from Schedule SB (Form 5500) line 40 greater than zero? ☐ Yes ☐ No

b If line 20a is "Yes," has PBGC been notified as required by ERISA sections 4043(c)(5) and/or 303(k)(4)? Check the applicable box:

☐ Yes.

☐ No. Reporting was waived under 29 CFR 4043.25(c)(2) because contributions equal to or exceeding the unpaid minimum required contribution were made by the 30th day after the due date.

☐ No. The 30-day period referenced in 29 CFR 4043.25(c)(2) has not yet ended, and the sponsor intends to make a contribution equal to or exceeding the unpaid minimum required contribution by the 30th day after the due date.

☐ No. Other. Provide explanation._____

Part VII IRS Compliance Questions

21a Does the plan satisfy the coverage and nondiscrimination tests of Code sections 410(b) and 401(a)(4) by combining this plan with any other plans under the permissive aggregation rules? ☐ Yes ☒ No

21b If this is a Code section 401(k) plan, check all boxes that apply to indicate how the plan is intended to satisfy the nondiscrimination requirements for employee deferrals and employer matching contributions (as applicable) under Code sections 401(k)(3) and 401(m)(2).

☐ Design-based safe harbor method

☐ "Prior year" ADP test

☐ "Current year" ADP test

☒ N/A

22 If the plan sponsor is an adopter of a pre-approved plan that received a favorable IRS Opinion Letter, enter the date of the Opinion Letter 03 / 31 / 2017 (MM/DD/YYYY) and the Opinion Letter serial number J500550A .

ASCENSUS, LLC

System for Providing Defined Contribution Recordkeeping Services, Non-Qualified Recordkeeping Services, Insurance Services, and Trust Activities Provided by Newport Trust

System and Organization Controls (SOC) for Service Organizations Report
for the period of October 1, 2024 to September 30, 2025



Report of Independent Service Auditors issued by
Grant Thornton LLP

Contents

I. Report of Independent Service Auditors 1

II. Ascensus, LLC's Assertion 4

III. Ascensus, LLC's Description of its System and Controls 6

A. Overview of Ascensus, LLC 6

B. Scope of the Description 6

C. Internal Control Framework 7

D. Control Activities 15

E. Controls Related to Information Technology General Controls 33

F. Additional Information about Management's Description 35

G. Subservice Organizations 35

H. Complementary User Entity Controls 49

IV. Description of Ascensus, LLC's Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results 55

A. Types and Descriptions of the Tests of Operating Effectiveness Provided by the Independent Service Auditor 55

B. Control Objectives, Control Activities, Tests of Controls, and Results 57

GRANT THORNTON LLP
1415 Vantage Park Drive, Suite 500
Charlotte, NC 28203

D +1 704 632 3500
F +1 704 334 7701

I. Report of Independent Service Auditors

Board of Directors and Management
Ascensus, LLC

Scope

We have examined Ascensus, LLC's (the "Company") description of its System for Providing Defined Contribution Recordkeeping Services, Non-Qualified Recordkeeping Services, Insurance Services, and Trust Activities Provided by Newport Trust (the "System") titled "Ascensus, LLC's Description of its System and Controls" for processing user entities' transactions ("description") throughout the period October 1, 2024 to September 30, 2025 (the "specified period") and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Ascensus, LLC's Assertion." The controls and control objectives included in the description are those that management of the Company believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The Company uses the subservice organizations listed in Table 1 of Section III of this report to provide services that support the System. The description in Section III of this report includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Company can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities

In Section II of this report, the Company has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Grant Thornton LLP is a U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL and each of its member firms are separate legal entities and are not a worldwide partnership.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the specified period. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- evaluating the overall presentation of the description, the suitability of the control objectives stated in the description, and the suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent limitations
The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion
In our opinion, in all material respects, based on the criteria described in Ascensus, LLC's assertion:

a. The description fairly presents the System for Providing Defined Contribution Recordkeeping Services, Non-Qualified Recordkeeping Services, Insurance Services, and Trust Activities Provided by Newport Trust that was designed and implemented throughout the period October 1, 2024 to September 30, 2025.
b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2024 to September 30, 2025 and subservice organizations and user entities applied the complementary controls assumed in the design of Ascensus, LLC's controls throughout the period October 1, 2024 to September 30, 2025.
c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2024 to September 30, 2025 if complementary subservice organization and user entity controls assumed in the design of Ascensus, LLC's controls operated effectively throughout the period October 1, 2024 to September 30, 2025.

Restricted use
This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of the Company, user entities of the Company's System during some or all of the specified period, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Grant Thornton LLP

Charlotte, North Carolina
December 5, 2025

The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.

II. Ascensus, LLC's Assertion

We have prepared the description of Ascensus, LLC's (the "Company") System for Providing Defined Contribution Recordkeeping Services, Non-Qualified Recordkeeping Services, Insurance Services, and Trust Activities Provided by Newport Trust (the "System") for processing user entities' transactions throughout the period October 1, 2024 to September 30, 2025 (the "specified period"), for user entities of the System during some or all of the specified period and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organizations and user entities of the System themselves, when assessing the risks of material misstatements of the user entities' financial statements.

The Company uses the subservice organizations listed in Table 1 of Section III of this report to provide services that support the System. The description includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Company can be achieved only if the complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

A. The description fairly presents the System made available to user entities of the System during some or all of the specified period for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    1. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:

        a. The types of services provided, including, as appropriate, the classes of transactions processed;

        b. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system;

c. The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

d. How the system captures and addresses significant events and conditions other than transactions;

e. The process used to prepare reports or other information for user entities;

f. Services performed by a subservice organization, if any, including whether the inclusive method or carve-out method has been used in relation to them;

g. The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls; and

h. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

2. Includes relevant details of changes to the service organization's system during the specified period.

3. Does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.

B. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the specified period to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout the specified period. The criteria we used in making this assertion were that:

1. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the Company;

2. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

3. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

III. Ascensus, LLC's Description of its System and Controls

A. Overview of Ascensus, LLC

Ascensus, LLC (the "Company" or "Ascensus"), including Newport Group, is the Retirement Services division. Ascensus has more than 40 years of industry experience providing solutions that help institutional retirement plan providers and selected intermediaries service their plan sponsors and participant clients. Core offerings include administration, recordkeeping, Employee Retirement Income Security Act of 1974 ("ERISA") consulting, compliance and sales support, and multilingual participant education programs, training, and documentation. Ascensus brings knowledgeable in-house resources and "bench strength" to every aspect of retirement plans. We take a collaborative, consultative approach to building retirement plans that can increase engagement, participation and deferrals. The majority of the user entities to which Ascensus provides services are subject to federal laws and regulations pursuant to ERISA.

Ascensus provides participant recordkeeping, plan administration, marketing support services and supplemental solutions for 401(k), non-qualified deferred compensation, compensation and benefits consulting and other types of retirement plans. Through relationships with various mutual fund companies, insurance companies, banks, credit unions, third-party administrators (TPAs), and broker-dealer firms, Ascensus Retirement currently services clients across the United States.

B. Scope of the Description

This report describes the control structure of Ascensus' System for Providing Defined Contribution Recordkeeping Services, Non-Qualified Recordkeeping Services, Insurance Services, and Trust Activities Provided by Newport Trust for the period of October 1, 2024 to September 30, 2025 (the "specified period").

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of the Companies, user entities of the Companies' System during some or all of the specified period, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting (ICFR) and have a sufficient understanding to consider it, along with other information, including information about the controls implemented by user entities themselves, when assessing the risks of a material misstatement to the user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

The AICPA's Auditing Standards Board (ASB) issued SSAE No. 18, Attestation Standards: Clarification and Recodification. The attestation standards are developed and issued in the form of SSAEs and are codified into sections. The identifier "AT-C" is used to differentiate the sections of the clarified attestation standards ("AT-C") sections from the sections of the attestation standards which are superseded by SSAE No. 18. This report is issued under AT-C sections 105, 205, and 320. These reports are commonly referred to as SOC 1® reports. The scope of this report is limited to the Company's

Retirement Services and the systems, including the website (www.newportgroup.com), covered in this report. User entities and their auditors are responsible for determining if the services provided to them by the Company are in the scope of this report.

Once plan sponsors log into the website, they have full access to the participant accounts and participant and plan level details.

C. Internal Control Framework

The control environment sets the tone of an organization, influencing the control awareness of the organization. The control environment is embodied by the organization's awareness of the need for controls and the emphasis given to the appropriate controls through management's actions supported by its policies, procedures, and organizational structure.

Senior leadership recognizes its responsibility for directing and controlling operations, for promoting a culture of ethical behavior and accountability and implementing a framework of effective controls. This framework is the foundation for all other components of our internal control structure.

a. The following are the primary elements of the service organization's control environment:

b. Commitment to integrity and ethical values

c. Oversight responsibility of Senior Management

d. Assignment of authority and responsibility

e. Commitment to competence

f. Accountability

Ascensus, LLC Organization Structure

Ascensus is comprised of the following major business groups and divisions:

- Retirement Services
  - Client Service
  - Retirement Operations
  - Retirement Administration
  - Ascensus Trust**
  - Provident Trust Group**
  - FuturePlan**
  - Plan Services Sales*
  - Business Development*
  - Retirement Products & Solutions (RPS)**
    - Total Benefit Communications, LLC (TBC)*
    - Wrangle*
- Newport Group
  - Non-Qualified Plans

- Bank Owned Life Insurance (BOLI)*, Company Owned Life Insurance (COLI) and Insurance Company Owned Life Insurance (ICOLI)
- Newport Trust - Institutional Trustee and Independent Fiduciary Services (NDS & SFS)

- Information Technology
- Corporate
  - Legal, Risk Management and Compliance (LRC)
  - Human Resources (HR)
  - Corporate Finance*
  - Corporate Development and Mergers & Acquisitions (M&A)*
  - Strategic Business Support Services*

Each division is led by a Vice President or an Executive Vice President who reports to the President of Ascensus's Retirement Services.

---

* Indicates groups that are not included in the scope of this report.
** Indicates divisions that are not included in the scope of this report.

Organizational and Management Controls

A primary responsibility of management is the establishment of an appropriate control environment to help achieve specified business objectives.

Ascensus's organizational structure is designed to provide adequate segregation of duties, as well as clearly defined areas of functional responsibility over the processing areas. Organizational charts for the IT team are reviewed and updated on an annual basis and whenever and organizational change occurs that warrants an organizational chart update to help ensure that Ascensus meets its commitments and requirements as they relate to security. In addition, roles and responsibilities for designing, developing, implementing, operating, monitoring, and maintaining the systems are defined within job descriptions, policies, and procedures.

Human Resources Policies

Ascensus has established hiring policies and guidelines designed to assist managers in selecting appropriate applicants for available positions. Ascensus hiring policy requires the following: a minimum level of education and experience as fits the position, completion of relevant application forms, execution of confidentiality statements and successful completion of the background investigation, which includes criminal, financial, education, and employment verification, as well as professional references.

Ascensus conducts a continuous, dialogue-based performance management review process that includes associates' feedback and recognition. The process evaluates an associate's performance against their established goals, as well as their core competencies. The competency assessment ensures alignment with the four cornerstones of Ascensus's products and client service: (1) Client, (2) Associate, (3) Policy and Process, and (4) Fiscal Responsibility. This focus, combined with Ascensus's Core Values of People Matter, Quality First and Integrity Always, promotes a professional working environment for associates.

To encourage staff continuity, supervisory personnel are eligible to receive an annual bonus that is directly tied to client retention and client satisfaction, associate satisfaction, and the achievement of agreed-upon performance standards.

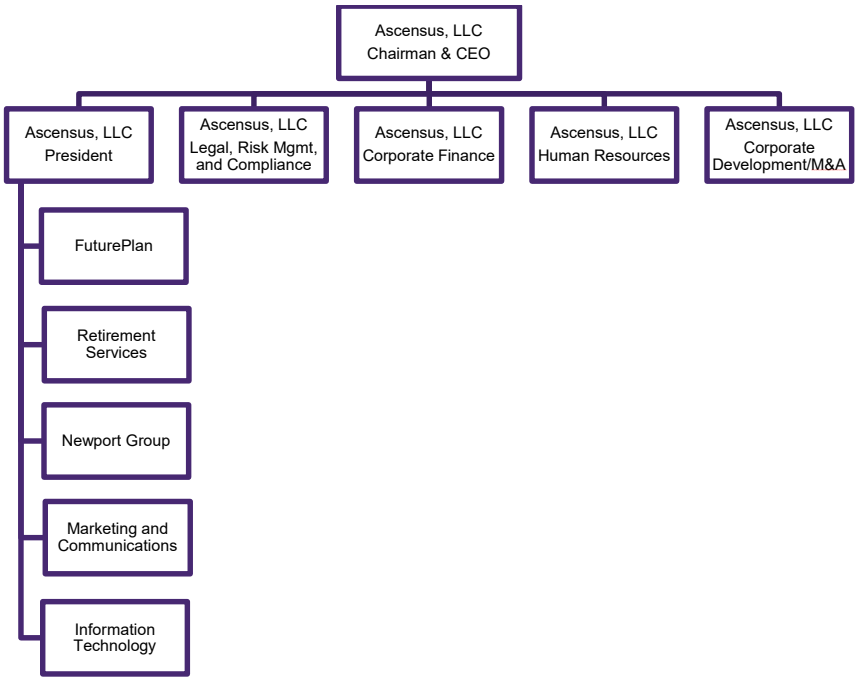
Ascensus recognizes the dignity of each of its associates and believes in the importance of cultivating a diverse and inclusive working environment. The organization embraces, respects, and appreciates the contributions of all associates. Through programs and practices, Ascensus is committed to fostering inclusion and tolerance, promoting an appreciation of differences and creating a culture where there is mutual respect among all associates. Ascensus's diversity mission statement defines a core component of the core value that "People Matter."

Learning and Development

Associates receive training through in-house classroom and self-paced training courses, supervised on-the-job training, formal coaching programs, and external seminars and education programs. Content for in-house classroom and self-paced training courses is reviewed and updated annually or when there are regulatory updates. This review and update are performed by Learning and Development and by Subject Matter Experts (SMEs) from various business units. New associates attend an onboarding training program to ensure they understand their job functions and how their responsibilities fit into overall business objectives. All associates are required to complete annual training on data security concepts to ensure that confidential information is properly protected at all times.

The following organization chart illustrates the structure of the groups and divisions at Ascensus as of September 30, 2025:

Ascensus, LLC Retirement Services Corporate Structure



The Ascensus groups that are in scope for this report are described below:

Client Services

Client Services is responsible for day-to-day financial advisor, plan sponsor, and participant service delivery, partner relationships, transaction services, growth/business development, and institutional project management. The Client Services department is comprised of the following:

- **The Plan Sponsor Service Center** is responsible for addressing the day-to-day servicing needs of the businesses sponsoring retirement plans and their Financial Advisors and TPAs. The team has developed the following service models/products to meet an employer's needs:
    - The "Individual(k)" product is targeted for individual business owners who need a comprehensive but simplified retirement plan to fulfill their retirement planning objectives.
    - The Unbundled Service product coordinates the TPA function with the services of a Financial Advisor. Ascensus's primary role is to facilitate the ministerial recordkeeping and transaction processing of plan administration while the TPA provides the plan document, plan design and plan compliance services in conjunction with a Financial Advisor who provides investment services.
    - The Full-Service product coordinates services to the small business enterprises and professional firms that comprise the largest percentage of Ascensus's clients, Financial Advisors and financial partners. The Full-Service Plan Sponsor Services teams help clients manage their plans by leveraging straight-through processing, ensuring Retirement Services Consultant availability through Ascensus's service delivery model, and providing tools to simplify the overall administration of their plans. As part of the Full-Service platform, Ascensus has a Premier service model that addresses the unique service requirements of larger clients, their Financial Advisors and Ascensus's financial partners.

- **Participant Services** assists participants through contact channels that include the Integrated Voice Response System (IVR) and web, and through telephone interaction with Participant Services associates.

Retirement Operations

Retirement Operations is responsible for transaction processing, account reconciliation, and reporting. Each team within Retirement Operations is described below:

- The **Transaction Processing** team supports the processing of plan contributions, investments, distributions and loans on the Ascensus Recordkeeping System (ARS or ARK).
- The **Reconciliation** team is responsible for balancing transfer agency activity and fund positions with ARS, and for producing quarterly participant statements and plan administration reports.

Retirement Administration

Retirement Administration is responsible for the installation and startup of new plans, ensuring that plans are processed in accordance with the regulations that govern their administration and the trading of assets. Each group within Retirement Administration is described below:

- The **Year-End Services** team coordinates the completion and delivery of ERISA compliance services, compliance testing, Form 5500 reports, and year-end audit reporting to clients.
- The **Transition Services** team installs startup and conversion plans in ARS. This includes establishing and auditing plan and participant data on ARS.
- The **Trade Group** is responsible for trading, settlement and other functions related to the money movement that supports the transactions processed on a daily basis.

Information Technology

IT is comprised of the following teams:

- The **Infrastructure** team is responsible for the IT environment, e.g., systems, telephony, network and desktop.
- The **Application Development** team is responsible for developing and delivering modifications to existing applications and creating new applications in accordance with business requirements. These applications include ARS and supporting applications used at Ascensus.
- The **Production Support** team manages the daily processing, monitors and implements production code, and verifies that system changes are tested prior to implementation into production.
- The **IT Project Management** team documents the business requirements for IT initiatives and manages the components needed to facilitate a successful implementation of code.
- The **Quality Control (QC)** team tests system changes to verify that systems are functioning as requested and the introduction of the code into production will not negatively impact current applications or performance.
- The **Information Security** team is responsible for the security of Ascensus's systems and for monitoring the tools that detect potential situations that may compromise system security.

In addition to the groups described above, Ascensus' Qualified Plan Retirement division utilizes offshore resources in Chennai and Trivandrum, India, which provides Ascensus with a discrete operating unit dedicated to Ascensus and only for use by Ascensus and its affiliates. These teams follow procedures defined by Ascensus to provide services related to data entry, review, report generation, administrative support and monitoring and resolution of fund position variances. This is provided by a combination of

Ascensus' own offshore facility and separate services provided by RR Donnelley Global Outsourcing (RRD). See the "Subservice Organizations and Complementary Subservice Organization Controls" section for additional information about RRD.

Risk Assessment Process

Ascensus has a risk assessment process in place to identify and manage risks that could affect the company's ability to provide contractual services to its clients or could expose the company to business risks from regulatory, monetary or reputational perspectives. This process requires all managers to identify significant risks in their areas of responsibility and implement appropriate measures to address those risks. Identified operational and strategic risks are reported to the Ascensus Risk Management Committee, which prioritizes both operational and strategic risk items. The committee meets quarterly, and the participants include senior management from Operations, Client Services and IT. Topics for discussion include service offerings, high margin/high dollar client impact of revenue, and service loss and operational gaps or procedural deficiencies that have been identified.

Monitoring Activities

Each of Ascensus's divisional management teams monitors the quality of its operational activities, including the internal control environment, as a routine part of their daily activities. Management reports are used for each significant function and are monitored at established intervals. The Executive Steering Committee, which includes senior management and IT representatives, meets bi-weekly to discuss the status of current and proposed projects.

Ascensus's leadership teams have developed and implemented processes to provide assurance that system controls are adequately designed to address identified risks relevant to the operation of the systems and that those controls operate in an effective manner. These processes include a risk identification and assessment process to review any existing or new risks that could threaten the operation of the systems. Controls are implemented to mitigate known risks. This information serves as a basis for the assertion Ascensus management makes in Section II of this report.

A comprehensive vendor management framework exists to ensure appropriate due diligence is performed before Ascensus enters into third-party relationships. Provisions are made for effective oversight after the relationship has been established, including periodic reassessments of each vendor against established due diligence standards. The framework also provides guidance for procurement efforts, including sourcing needs assessment, vendor selection, contract management and ongoing monitoring. A fundamental component of the framework is a structured vendor risk management program that classifies vendors based on risk potential, requires greater scrutiny of vendors identified with higher risk potential and ensures appropriate monitoring and mitigation of identified risks.

Vendor performance is monitored by an assigned vendor owner within the primary line of business that utilizes the services of each subservice organization. As applicable, vendor owners solicit input and feedback from the business areas that use each vendor's services to ensure a comprehensive view of vendor performance. The monitoring and oversight performed by the vendor owners are done at a level of detail commensurate with the business relationship and criticality of the vendor.

When available, Ascensus's management obtains and reviews SOC 1 and/or SOC 2 reports from subservice organizations to verify that adequate controls relevant to Ascensus's control environment are in place and operating effectively. Details on governance programs, including Business Continuity and Vendor Management programs are also collected from vendors for Ascensus' review.

Regulatory Supervision

Newport is required to develop and maintain formal policies and procedures by the New Hampshire State Banking Department (the "Department"). Further, Newport is required to periodically report on its financial condition to the Department. The Department periodically reviews these policies, procedures and financial reports to confirm Newport's compliance with the law and continued financial viability.

Information and Communication

Ascensus employs various methods of communication to ensure that associates understand their individual roles and responsibilities and to ensure that significant events are communicated in a timely and secure manner. These methods include orientation and training programs for newly hired employees, internal communications that summarize significant events and changes, and the use of email messages to communicate time-sensitive, legislative and regulatory messages and information. Executive management and corporate leadership hold periodic meetings to provide insight into strategic direction, key decisions, and company performance summaries. Managers also hold periodic staff meetings as appropriate to disseminate the time-sensitive, legislative, regulatory, and corporate messages and initiatives.

IT employs various methods to communicate initiatives, performance, and IT security effectiveness to leadership members to ensure that SLAs and security obligations are sustained. Key IT initiatives are presented to senior leadership to ensure timely progress and the proper prioritization of upcoming projects. Ascensus IT monitors network performance and provides a summary to IT leadership. Ascensus IT also performs network scans and regularly scheduled external scans to validate these results. Summaries regarding infrastructure performance, security scan results, and enhancement initiatives are communicated to Ascensus IT leadership.

The table below summarizes the technical information for systems supporting transaction processing. See the following sections, “D. Control Related to Qualified Retirement Plans, Non-Qualified Retirement Plans, Institutional Trustee and Independent Fiduciary Services (Nondiscretionary Services and Special Fiduciary Services)” and “E. Controls Related to Information Technology General Controls” for additional detail on how information is used and communicated to external and internal parties, as necessary.

Application	Purpose	Applicable Business Line
Ascensus Recordkeeping System (“ARS”)	System used for processing plan transactions, including contributions, investments, distributions and loans.	Qualified Retirement Plans
HUB+	System provided by Vertical Management Systems (VMS) that is used for direct trading of mutual funds with the National Securities Clearing Corporation (NSCC).	Qualified Retirement Plans
Non-Qualified (“NQ”) Services – Case Tracking System & NASA Application	The Case Tracking System is a tool utilized to verify that enrollments and re-enrollments are completed prior to the pre-defined payroll deadline, if required by client agreement. The Newport Accounting Services Application (NASA) is a proprietary reporting application tied to the NQServices SQL Server database and is utilized to generate the monthly Corporate Reporting.	Non-Qualified Retirement Plans
Electronic Database Tool ("EDB”)	Detailed plan and participant information maintained in the Transaction System is used in the Electronic Database Tool daily and participant information is available online through the Company’s website.	Non-Qualified Retirement Plans

Application	Purpose	Applicable Business Line
BOSS Application ("BOSS")	BOSS is a proprietary application that consists of various operational modules developed to complement business processes and reporting.	Non-Qualified Retirement Plans
McCamish Application ("McCamish")	McCamish is an application the Company uses to administer the daily transaction calculation and balance calculations for non-qualified retirement plan participants' accounts. Transactional information from the McCamish application is then transmitted to the EDB to provide participants\sponsors with non-qualified retirement plan account balances.	Non-Qualified Retirement Plans
Trust 3000 Application	This system is supplied and supported by SEI and is used as a trust accounting, processing, and custody system by Newport to maintain plan sponsor accounts, move cash and securities, produce plan sponsor statements, and make distribution payments.	Institutional Trustee and Independent Fiduciary Services (SFS)
Retirement Benefit Plan System ("RBPS")	This system is supplied and supported by SEI and is designed to generate participant level distribution payments. RBPS transmits participant distribution data to the Trust 3000 application.	Institutional Trustee and Independent Fiduciary Services (SFS)
Customer Strata Station Browser ("CSS")	This application is supplied and supported by SEI and is a cash transaction processing system that provides real-time access to Trust 3000 account record information via an extranet connection. Newport users can view account information, add accounts, manage contacts, create notes and activities, and create, approve, and post transactions to Trust 3000 application records.	Institutional Trustee and Independent Fiduciary Services (SFS)
Cconnect	This application is supplied and supported by SEI and is designed to provide SEI customers and clients with the ability to access certain account information via the internet. The product is designed to enable customers to retrieve real-time account holdings, market values, tax lot information, cash information, transactions, position details, asset summaries, available funds, balance summaries, pending trades, and monthly/ quarterly/ annual statements. Access is assigned by SEI and users have read-only access.	Institutional Trustee and Independent Fiduciary Services (SFS)
Websites & Webservers	Plan Sponsor and Participant account inquiry and transaction initiation.	All

D. Control Activities

1. Qualified Retirement Plans

Transition Services

Both new and conversion plan relationships are typically established between a client and Ascensus via an intermediary, either an individual financial advisor or one of Ascensus's institutional partners. In the Transition Services process, Ascensus works with a client to transition their plan into the environment. This process follows a defined policy. Once a plan sponsor, institutional partner or financial advisor has chosen to administer their plan through Ascensus, the Transition Services team and required parties, including prior recordkeepers and the plan sponsor, set up the plan and determine a timeline of events. This process includes completing a paper or digital Plan Establishment Kit (PEK) that guides the client through each step of the installation.

For conversion plans, Ascensus works with the plan's prior recordkeeper to acquire participants' indicative and financial information for upload to ARS. For new plans, Ascensus obtains similar information directly from the plan sponsor. Each step in the conversion has built-in QC procedures, which include checklists that validate each step in the data acquisition and loading process. Ascensus management regularly reviews the status of plans in conversion to help ensure that timelines are being maintained and any potential issues are escalated promptly and appropriately.

New and Converted Plan Setup

Ascensus has established installation policies and procedures to help ensure the accurate and timely installation of new and converted retirement plans. These procedures are documented and accessible via the company's intranet, providing guidance to associates involved in the setup process. Each plan installation is tracked using an installation timeline, which helps monitor progress and ensure that key milestones are met.

As part of the quality assurance process, a detailed review of plan parameters—such as vesting calculations—is conducted within the ARS system. This review is documented through a signed Plan Rules Audit Memo, which serves as evidence that the plan setup has been verified before the client receives the final go-live confirmation. Additionally, the Business Projections Report is reviewed daily to monitor the status of all plans in the pipeline. Any plans that have not yet been installed are flagged, and their progress is tracked to ensure timely resolution.

Ongoing Enrollments

The enrollment process for new participants entering a live plan is designed to simplify the enrollment process. Each new participant receives welcome information that describes the parameters and investment offerings of the plan, as well as comprehensive enrollment instructions. Enrollment can be completed online or via a hard copy form at the plan sponsor's discretion. New enrollee data that has been entered in (ARS) is verified to confirm that it accurately reflects the new participant's selections. Ascensus verifies the eligibility of each new participant prior to activating their account and enters them into the plan on the appropriate entry date, as defined by the plan's rules.

Transaction Processing

Plan participants have the option, based on plan-specific parameters, of executing transactions within their accounts, including enrollments, distribution requests, loan requests, fund transfers, life event changes and changes to beneficiaries. These methods are described below. Each method employs authentication and privacy controls to verify the security of participants' information and the confidentiality of their requests.

- *Mail/Fax* – Hard copy documents received by Ascensus are immediately scanned into the Business Process Management (BMS) system. The BMS is monitored via queues in the system, and includes automated edits (i.e., checking for completed fields) and system reporting. Ascensus associates use this functionality to help ensure that transaction forms are flowing promptly and correctly to the Transaction Processing team.

- *Phone* – Ascensus's Participant Services can accept transaction requests directly from participants over a recorded telephone line. In order to initiate a transaction, a participant must first authenticate their identity based upon rules agreed to with the applicable partner. Requests on the recorded line must be repeated back to the participant to verify the request has been accurately recorded by the Participant Services associate. Trade transactions in accounts with balances over $100,000 are automatically routed for a second quality review by a member of Participant Services, independent of transaction entry, to re-verify the accuracy of the record in ARS.

- *IVR* – Ascensus maintains an automated phone system for transaction requests. As with the live phone option, this system requires a participant or plan sponsor to first authenticate their identity, including the use of an IVR-specific personal identification number. The IVR is fully integrated with ARS and programmed to access ARS and validate transactional requests and replicate the ability of a live associate to inform participants of the specific plan parameters that may govern their transaction options. The IVR also allows a participant to cancel a transaction if the day's trading cut-off time has not yet been reached. The IVR repeats back all requests to the participants before concluding the phone call to verify the participant's request has been captured accurately.

- *Internet* – Ascensus maintains a secure web portal that allows participants to request transactions, review their accounts, and access plan-related information such as fund prospectuses. Similar to the other transaction request methodologies, the participant or plan administrator must authenticate their identity to begin using the website. In this case, authentication is established using a unique user ID and password. As with the IVR, the website is fully integrated with ARS to verify that any transaction request is consistent with the plan's setup parameters. Transaction requests must be verified and confirmed before they are placed to verify that the system has recorded the transaction accurately. To verify all activity has been properly recorded and to prepare it for processing by the system, each internet-requested transaction is recorded in a database that is accessed during nightly processing.

Regardless of the method used to submit transactions, the same controls are used to verify transaction requests are processed completely and accurately, including the reconciliation and QC controls described in Section IV of this report, "Description of Ascensus, LLC's Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results."

Distribution Processing

When a plan participant terminates employment with the employer, they have the option to withdraw their vested account balance from the plan. If a participant's balance exceeds $5,000, they may choose to leave the balance in the plan; otherwise, leaving the money in the plan is at the sponsor's discretion. Those participants electing a distribution may either take a lump sum or roll their monies into another qualified plan or IRA. The initial step in this process is the participant's submission of a distribution form to the plan sponsor for the sponsor's authorization either via the participant web portal or via hardcopy. The authorized form is then forwarded via signed hard copy to Ascensus for processing. Some plans also allow participants to take in-service partial withdrawals or hardship withdrawals. In these cases, the participant must first submit a completed distribution form to the plan sponsor, and once this has been approved, it is forwarded to Ascensus. Distribution requests are reviewed prior to processing to help ensure the proper authorizing signature is in place. Individuals at the plan sponsor who are authorized to approve

distributions are determined during the initial plan setup stage. The list of individuals authorized to approve distributions is updated as needed based on instructions from the plan sponsor.

The timing of the processing of a distribution depends on both the plan's provisions and the receipt of all required information. All disbursement transactions are first reviewed by Ascensus to help ensure that none of the transactions violates the plan's vesting and other provisions. Ascensus then enters the distribution information in ARS, which in turn initiates the trades to fund the transaction. ARS executes automated edit checks over the entered information to help ensure that required data fields have been populated. This allows Ascensus to create required distribution and tax reporting documentation. Any issues that result from these edit checks are recorded and tracked to resolution so that the transaction can be completed as soon as possible. Distributions are subject to a verification process that includes a check to confirm that the transaction has been properly entered into the system and that QC checklists have been completed. This helps ensure that disbursement processing is in accordance with participant and plan sponsor directives. QC associates review financial transactions for accuracy, completeness and timeliness after data entry and evidence their review by signing off on the corresponding transmittal form or via electronic sign-off in the BPM system. Any issues identified are resolved prior to sign-off.

Activity that is entered and verified in ARS prior to the cut-off time is submitted for trading that day; otherwise, the trades are pended until the next available trading day. When all required funds have been received, information is forwarded to the plan's trust entity for the creation of checks, processing of appropriate withholdings, and mailing. Ascensus reconciles monies held in the distribution processing account on a daily basis to verify that funds are being used to fund payments and no remaining balances are in that account.

To help ensure that plan sponsors have a record of all activity processed in their plans for their own recordkeeping and auditing purposes, Ascensus supplies a monthly summary, the Monthly Plan Confirmation (MPC), to each plan sponsor. Activity shown on the MPC includes distributions and fund exchange and allocation change transactions.

In order to comply with tax reporting regulations, Ascensus calculates required tax withholdings from distribution payments, and also creates and forwards a 1099R tax form to participants who received a distribution payment for assistance in preparation of their annual income tax returns. Before these tax forms are provided to participants and the IRS, automated verifications are executed against the accumulated tax records to verify all required codes are present.

Loan Processing

Some plans permit their participants to take loans against a portion of the participant's vested account balance depending on the parameters of their plan. ARS stores each plan's loan parameters, which define the amounts eligible to be loaned and the loan terms. The transaction begins with the participant completing a loan request, which is available on the website. The request is then validated against the plan's loan rules, and if it is deemed to be within those rules, Ascensus creates the trades to fund the loan and creates the amortization schedule. Loan initiation requests that are received prior to the cut-off time are submitted for trading that day; others are held for trading on the next available trading day.

Loan repayments are received each pay period along with contribution information. Loan repayments are split according to principal and interest in accordance with the amortization schedule, and the outstanding loan principal will be reduced by the principal portion of the repayment.

Variances between a plan's contribution amount at the trust company and the cash position in ARS are identified on daily variance reports, which are monitored throughout the day by Ascensus associates until corrected. Vesting amounts are automatically calculated based on the vesting schedules configured during plan setup. Unvested employer contributions are credited to a forfeiture account.

Fund Transfer

Participants can request to reallocate their money via direct contact with the call center, through IVR, or via entry into the secure internet site (described under "Transaction Processing" in this section).

Each method of receiving transfers has QC processes built in to help ensure timeliness and accuracy, including common industry methods of authenticating participants prior to accepting transactions. These methods are integrated into the overall Identity Protection Program. The QC processes differ based on the submission method used; these processes are described in "Transaction Processing" in this section.

Regardless of the method by which they are received, transfers are entered in ARS for processing. ARS calculates the trades required to execute the transfer and updates participant accounts to reflect their new allocation. As with other transactions, any transfer requests received prior to the cut-off time are submitted for trading that trading day; otherwise, they are held until the next available trading day. Ascensus also periodically rebalances participant accounts, if the plan rules dictate such, by automatically creating transfer transactions to bring the account back to the intended alignment. These transactions are created by Ascensus, in accordance with a plan's rebalance schedule, but otherwise are processed and traded in the same manner as a participant-initiated fund transfer.

Contribution Processing

At the conclusion of each pay period, the sponsor submits the following information electronically to Ascensus:

- Updated participant-indicative information
- Compensation and plan contributions
- Hours worked
- Loan repayments

The data undergoes verification and review processes to help ensure relevant information has been submitted and has been accurately downloaded to Ascensus's systems. Edit checks are run immediately to verify that the totals on the file equal the participant-level submissions and that all participants on the file have records in Ascensus's systems. Any issues during the processing of the contribution file are recorded and escalated to management. This escalation helps ensures that contribution issues are researched immediately so that participant contributions can be invested in as timely a manner as possible.

Ascensus maintains records for each contributing participant that indicates how Ascensus should split the contribution among the plan's available funds. This allows each contribution to be immediately invested per the participant's stated directives.

Data is submitted before contribution or loan repayment dollars are forwarded so that Ascensus can verify that the data conforms to plan requirements and any required changes are reviewed with plan sponsors. This allows Ascensus to establish that the proper dollar amounts are submitted (a "data before dollars" arrangement). Cash received is reconciled and invested according to the participant's directions.

Each period, Ascensus uses the indicative information portion of the submission to verify and update contact information for each person on file, as necessary, and uses employment hours and compensation to update vesting and contribution amounts.

Trading Process and Account Reconciliation

As transactional activity is received, Ascensus prepares trades for placement at the end of the business day. Trades are collected at the plan and fund levels for execution. ARS sends a message to the trading system any time a new transaction has been received that requires a trade. These messages are assembled throughout the day until the trading deadline when the assembled trades are submitted for execution. Ascensus is occasionally required to place trades manually with the fund company, outside of the automated trade gathering methodology. A series of procedures are in place to address this need, whereby trades are reviewed for accuracy by an individual other than the one who entered the transaction. Receipt of the trade by the fund company is also verified.

While Ascensus maintains accounts for each individual participant in ARS, all trading is performed at the plan and CUSIP level. This requires a reconciliation process to verify that the total balances of all participants in ARS match the single balance held at the fund. This is necessary to verify that actual shares exist to support every share allocated to participants within ARS. Before beginning the reconciliation process, the trading system verifies that all activity has been placed, all earnings have been posted and any issues with trade placement are promptly researched. Once all trades have been placed, Ascensus facilitates the settlement process with the applicable trust company by reviewing a daily report of trades that require settlement and forwarding a report listing these required money movements.

The reconciliation process begins each day when Ascensus receives updated pricing information, confirmations of the prior day's trades, and updated positions from the fund companies. Data elements are received electronically via the trading interface, which verifies data received and creates alerts if data is delayed. Missing prices are identified via reporting that scans the database for trades with missing pricing data. The ability to enter or update prices is restricted to appropriate personnel who require the access to perform their job responsibilities. Alerts are investigated to verify accuracy in the trading, posting and reconciliation processes.

Once Ascensus has received updated fund positions, the positions are compared to the current positions generated by ARS, which is the summation of all participant accounts after the prior day's activity has been posted. This is performed via a system-generated Daily Variance Report that highlights inconsistencies. Inconsistencies can result from dividend postings, use of different prices between the two systems, or rejected trades. Differences between these two sets of positions are isolated and reviewed by the Reconciliation team. Once the root cause has been determined, Ascensus works with the appropriate fund companies or internal transaction processing teams to resolve the identified breaks. Any items that are not resolved within two business days are tracked and escalated for resolution.

As each plan maintains only one account at a fund company, it is the role of Ascensus to determine how dividends paid into a single account should be allocated between those participating in the fund at the plan level. To help ensure that Ascensus allocates the total dividend at the proper time, ARS automatically posts the shares to the individual participant accounts on the pay date to participants with a balance in the fund as of the declared record date. These allocations are verified daily by the reconciliation processes.

Statements and Reporting

Once activity has been verified and fund positions agreed with the fund company positions, Ascensus produces participant statements and standard employer reports. These are produced on a quarterly basis within 15 calendar-days following the end of the reporting period and delivered either electronically or via hard copy mail. In addition to the standard quarterly reporting, annual summarization reports are also produced for the Plan sponsor to assist with plan auditing and account tracking. Each plan is put through a series of statement processing edits designed to confirm accuracy prior to production. These edits help ensure that participant-level records are consistent with the plan, that prior period information carries over properly as the starting value of the current period, and that loan tracking is in line with financial balance tracking. Although

investment inconsistencies are addressed as these processing edits are executed, there are other items reported on statements that need to be verified for accuracy.

As the participant statements and other plan reports are key tools in plan auditing and plan reviews, Ascensus employs additional access-rights security to help ensure that reports are not released until all issues identified have been resolved, even those that do not impact participant balances. Thus, the ability to override the process's edit parameters and to release reports is restricted to senior level associates so that documents are not released without the proper supervisory reviews. This includes detailed reviews of a sample of statements to verify that no errors exist. Additionally, the Vice President of Risk Management performs a review of associates with the ability to override the process's edit parameters and to release reports on a semiannual basis.

In addition to the participants' statements, Ascensus produces other administration reports that assist plan sponsors and auditors in completing their required tasks. To assist with plan filings and audits, a complete package of reports is produced and delivered via the Plan Sponsor Web portal on an annual basis.

Compliance - Annual Deferral Percentage/Annual Contribution Percentage

Ascensus provides clients with testing, plan parameter review and compliance consultation to verify that plans remain in good standing. Specifically, through the compliance review process, required testing is completed and the results are interpreted or acted upon. The Year-End Services team works with the ERISA Legal team to keep ARS updated with the latest testing parameters, and to verify that the basic parameters required to execute the testing procedures are properly updated. Further, only authorized associates are able to update testing-related data tables.

Ascensus works with plan sponsors to verify the accuracy of data that impacts testing. Data inconsistencies are immediately shared with plan sponsors so that corrections can be made timely. Annual discrimination testing (mandated testing to help ensure that plan participants are benefiting from the plan) is completed within required parameters and the results are delivered electronically to plan sponsors via their secure website. Ascensus works with clients to perform corrections or refunds as required to return a plan to compliance, and to process the transactions within the designated parameters.

Ascensus monitors the status of each plan in the testing cycle and produces detailed testing summary reports so that Ascensus and the management and user entities are notified of issues and can address them as necessary.

2. Non-Qualified Retirement Plans

Plan Enrollment Kit

Installation of Non-Qualified deferred compensation plans by Ascensus may require the creation of a Plan Enrollment Kit. The Relationship Manager reviews enrollment requests to ensure that a Plan Enrollment Kit is created in accordance with client provisions. completes a Materials Request Form that details required documentation for the creation of Plan Enrollment Kits in accordance with client provisions included in the Plan Administration Manual.

Forms, such as cover letters, are customized to each sponsor's Plan Enrollment Kit. A review of enrollment requests is performed by the Relationship Manager to verify that a Plan Enrollment Kit was created in accordance with client provisions included in the Plan Information Guide. Required changes are made to the document and communicated to the third-party fulfillment vendor responsible for printing and mailing, if applicable, before the Plan Enrollment Kit is finalized. A final review of the Plan Enrollment Kits is performed by the Non-Qualified Conversion Team and Client Services and provided to the Communications Department, along with the materials request form. The Communications Department sends an e-mail to the third-party fulfillment company authorizing them to generate and mail the Plan Enrollment Kits to participants if applicable. This report does not include control activities surrounding the generation and mailing of the Plan Enrollment Kits by the third-party fulfillment vendor.

While the Plan Enrollment Kits are being created, the sponsor submits a census file to Ascensus that contains all eligible participants and information required to set up these participants in the plan (i.e., name, address, social security number, hire date, etc.). Upon receipt of the census file, Operations loads eligible participants and applicable information into the Transaction System. The Implementation Project Manager (new plans) or Plan Administrator (existing plans) puts the census file through the plan's census analyzer to compare various data elements and update the Transaction System. Additionally, for new clients with enrollments, a member of the Product Support Team compares the number of records provided in the census file to the enrollment system to confirm that the number of records provided match those loaded. Any discrepancies are researched and resolved.

a. Online Enrollment

Participants may elect to enroll in their plan by accessing online enrollment screens through our website. Enrollment periods are defined during annual planning with the client and are usually two weeks in length. These online enrollment screens are based on enrollment parameters defined in the sponsor's plan document and information contained in the enrollment kit. A review and approval of the online enrollment test scripts is completed by the Implementation Project Manager or the Relationship Manager to verify that website screen errors are identified and corrected prior to activation. Further, they verify that the online enrollment website screens are created in accordance with client provisions. In addition, the plan sponsor is provided with the opportunity to review the website prior to the commencement of the open enrollment date which is facilitated by the Relationship Manager. Once testing has been successfully completed and the plan sponsor has been provided with the opportunity to review the website, the Implementation Project Manager or the Relationship Manager authorizes activation of the plan's online enrollment screens. Approvals are evidenced by a signature or sign-off within the Tracking System.

As eligible participants complete the online enrollment process, an e-mail is generated and sent to the participant, with a copy sent to the e-Confirm mailbox. This e-mail confirmation details the participant's enrollment elections. These e-mails are retained to determine that data was captured and updated in the Company's administrative systems.

Enrollment Results reports are generated that detail each eligible participant and whether they have accessed enrollment, enrolled, declined as well as detailing their deferral elections, account allocations, distribution elections, and investment choices. The reports are reviewed by the Implementation Project Manager or Plan Administrator to monitor the enrollment process. A final report detailing the results is prepared by the Conversion Project Manager (new plans) or Relationship Manager (existing plans) and provided to the client. These reports are also used toward the end of the enrollment process in order for the sponsor or the Company to contact eligible participants who have not enrolled or have not completed their enrollment to determine their intent. A separate deferral election report is delivered to the Plan Sponsor/payroll contact by the pre-defined payroll deadline so that deferral deductions scheduled for the following year are coded into the client's payroll system.

b. Enrollment Forms

For eligible participants who enroll through the use of paper enrollment forms, the Plan Administrator, Conversion Project Manager, or plan sponsor enters the eligible participant's data directly into the enrollment system. The Conversion Project Manager, Plan Administrator, or plan sponsor compares the information on the eligible participant's enrollment form to the information that was entered into enrollment system. Discrepancies are corrected in the enrollment system.

c. Evergreen Elections

Certain plan provisions allow participants to carry over elections from year to year, often referred to as “passive elections.” If a participant does not actively re-enroll, their elections from the previous year will automatically carry forward to the current year’s plan in the Transaction System. Following the end of the enrollment period, Client Services generates Enrollment Confirmations and provides these Confirmations and distributes them to participants for their review.

d. Enrollment Reports

The online Enrollment website is programmed to deactivate based on the enrollment period end date. Once the enrollment information is uploaded to the Transaction System, an exception report is generated to verify that all enrollment information was uploaded completely and accurately. The Plan Administrator reviews this report to verify that all enrollment information was uploaded completely and accurately. Any exceptions are researched and resolved.

At the end of the enrollment period, an Enrollment Summary report and an Enrollment Results report are generated and provided to the sponsor. The Enrollment Summary details overall results of the enrollment process such as participation rate, average salary deferral, aggregate investment elections, model portfolio results, and investment allocation. The Enrollment Results details participants who enrolled, along with their deferral elections for each deferral source, account allocations, distribution date, and distribution method. Correspondence sent to the sponsor is retained in the plan’s file at the Company.

All steps involved in the enrollment process, including constructing and updating the enrollment kit and building the online enrollment website, are tracked using the Case Tracking Database. The Client Service teams are responsible for updating the status of these tasks on a daily basis. Further, Client Services reconciles enrollment elections and participant data from enrollment results reports (deferral elections, account allocations, investment elections, and beneficiary information when applicable) generated from the online enrollment site compared to the enrollment specifications in the Client Agreement to verify that all data was captured and updated completely and accurately in the Transaction System. The Plan Administrator monitors the Case Tracking System to verify that enrollments and re-enrollments are completed prior to the pre-defined payroll deadline, if required by client agreement. Further, the Plan Administrator reviews the Case Tracking System to help ensure that at the end of the enrollment period a Deferral Election Report is provided to the plan sponsor prior to their pre-defined payroll deadline, if required by the client agreement.

Re-enrollment

a. Enrollment Materials

Before a plan’s anniversary date, re-enrollment materials are created and mailed to eligible participants that are defined by the sponsor. A review is completed by the Implementation Manager or Plan Administrator of the pre-populated data for re-enrollments to verify that all elections were carried forward from the prior period to help ensure the completeness of the re-enrollment data loaded into the enrollment system. Any discrepancies are researched and resolved. The same enrollment procedures and controls described above are followed for the re-enrollment process.

b. Updating the Transaction System

At the end of the enrollment period, participant elections are loaded into the Transaction System by the Product Support Enrollment Team. Once the enrollment information is uploaded to the Transaction System, an exception report is generated to verify that all enrollment information was uploaded accurately. Discrepancies are researched and corrected.

New and Converted Plan Setup

A Plan Administration Manual is created as an addendum to the client contract to detail the plan information such as the last day of the plan year, plan type, effective date, anniversary date, investment types, account types, money types, distribution types, and vesting schedules. The Plan Administration Manual is signed by the client/sponsor indicating that they have reviewed and approved the plan setup.

For converted plans, a plan and investment level reconciliation are performed to verify that the converted plan's liability records agree to the prior Recordkeeper's data. This reconciliation is provided to the plan sponsor for review and approval.

The Implementation Project Manager completes the Implementation and Conversion "Go Live" checklist verifying that the Plan Administration Manual is consistent with source documents including contract provisions and that the plan is set up within the Transaction System in accordance with contract provisions as detailed within the Plan Administration Manual.

Transaction Processing

a. Participant and Sponsor Contributions

At the end of each pay period, the sponsor electronically submits a worksheet file to the Company which contains employee deferral amounts and company contributions. A central e-mail box at the Company is used to collect this data. The Conversion Project Manager (new plans) or the Plan Administrator (existing plans) performs the following verifications to identify major discrepancies in the worksheet file:

- Evaluates the effective date and formatting of the file for automated processing.
- Evaluates the file for any negative contributions in order to strip those from the file to discuss with the Sponsor.

The original e-mail received from the plan sponsor is saved to the network by the Conversion Project Manager or Plan Administrator. The Operations Team performs a reconciliation of the payroll information received from the plan sponsor to the payroll information input into the Transaction System. Any identified discrepancies are communicated to the plan sponsor. The worksheet file is reformatted (if required) and uploaded to the Transaction System. During the nightly batch cycle, the Transaction System is programmed to process the information in the contributions file accurately based on selected investment elections, allocation percentages, and the funds' prices. The final upload of this information into the Transaction System during the nightly batch is also dependent on the receipt of the pricing files which is submitted to the Transaction System by a third-party mutual fund/insurance provider.

The Operations Team reviews the payroll batch process to help ensure that there are no event sequence errors in the batch process. Any identified event sequence errors are researched and resolved. Client Services maintains a payroll processing log to verify that payroll, deferral, and plan sponsor contribution information received from the plan sponsor and is processed after receiving all the necessary data at the Company.

Detailed plan and participant information maintained in the Transaction System is downloaded into the Enterprise Database Tool (EDB) on a daily basis and participant information is available online through the Company's website.

b. Disbursements

The plan sponsor is responsible for notifying the Plan Administrator when a disbursement needs to be processed for non-scheduled separation of service. Scheduled disbursements, elected by participants during each enrollment or by individual distribution modification requests, are managed by the Plan Administrator.

Event triggered disbursements are processed only after the plan sponsor notifies the Plan Administrator or Client Service Manager of a participant's separation of service. For the participant receiving a disbursement, the Plan Administrator verifies that the data in the Transaction System for that participant reflects all payroll contributions and realized earnings. Based on the calculation method defined in the plan document and the valuation date, the Plan Administrator or Client Service Manager calculates the participant's disbursement amount (including any forfeited amounts) and processes it in the Transaction System. The disbursement amount is then sent to the plan sponsor or the paying agent.

For periodic installment payments, the Plan Administrator tracks future scheduled disbursements. Based on disbursement information supplied by the Company, the plan sponsor is responsible for generating the disbursement check and delivering this check to the participant.

c. Fund Transfers / Allocation Changes / Client-Initiated Rebalancing

Based on the plan setup, participants can perform fund transfers, investment allocations, and rebalances online through the Company's website, by submission of a hardcopy form to Client Services or over the phone with Client Services. Information entered on the website is configured to only accept valid inputs. The www.newportgroup.com website edit controls require that future allocations, rebalances, and fund transfers entered by the participant must each total 100%. Entries not totaling 100% are rejected by the website. The participant is responsible for reviewing the fund transfer and/or allocation changes prior to releasing the transaction for processing.

Each business day, the fund transfers requests, allocation changes, and rebalances entered by the participant via the www.newportgroup.com website are stored in the Electronic Database Tool and automatically generate a load file that is used to update the data in the Transaction System. During the nightly batch process, fund transfers, allocation changes, and rebalances entered via the website are automatically uploaded and set as pending in the Transaction System. These pending transactions are automatically released for processing on the effective date which is programmed into the Transaction System during the plan design phase. A Pending Transaction Report, detailing information about the requested transaction, is sent daily via e-mail by the EDB to the Conversion Project Manager, Information Technology and Support, Operations, Client Services, and Asset & Liability Management personnel for review.

Confirmations for fund transfers, allocation changes, and rebalances are auto delivered to participants via the website (www.newportgroup.com).

Detailed plan and participant information maintained in the Transaction System is downloaded into MRS/EDB each business day. Participant information is available online through the Company's website.

Wire Transfers/Premium Invoices

Once a client wire has been deemed necessary (either through their request or through the rebalancing process), the system is programmed to require that wire transfer instructions, including client name and account information, are reviewed for accuracy and approved by an appropriate member of the Asset & Liability Management Team prior to the first wire transfer template being processed. The wire is then activated by Management of the Asset & Liability Management team. Wire transfers must be reviewed for accuracy and approved by a secondary individual prior to the wire transfer being initiated. After requests are received, wire transfers are initiated within two business days or as otherwise required by client agreement. A wire transfer confirmation is sent to the client detailing the total dollar amount transferred and the account(s) to which it was applied.

A premium invoice detailing the wire transfer information including the Premium Roster detailing instructions for payment allocation, is reviewed for accuracy and approved by the Investment Analyst or designated approved and sent to the Insurance Carrier. Wire transfers for insurance premium payments are initiated within two business days from the date of the premium invoice. Before it is sent to the insurance carrier, a systematically generated roster detailing instructions for payment allocation is reviewed for accuracy and approved by the Investment Analyst or by a designated approver prior to being sent to the Insurance Carrier. The Non-Qualified Asset & Liability Management group reconciles the data from the Insurance Carrier confirmation to the allocation instructions for each wire payment related to a premium invoice. Discrepancies are researched and resolved.

Plan Rebalances

The Company's Non-Qualified deferred compensation rebalancing process is designed to:

- Neutralize the effect on earnings of changes in plan assets and liabilities,
- Invest assets on a basis that correlates with the aggregate investment allocation selected by plan participants,
- Maintain the "unfunded" status of the plan and minimize expenses and taxes at the plan sponsor level.

The Asset & Liability Management team compares either the final fund allocation or the individual trade transactions from the trade confirmation to the original trade instructions to verify that all trades were performed and that the trades were performed accurately and completely within the Transaction System. The Event Tracking system is monitored by the Non-Qualified Asset & Liability Management team to verify that trade confirmations are sent to the client for their review for accuracy and completeness as required. Required rebalances are flagged as completed once confirmations have been sent to the client.

Investing and Pricing

Pricing files, submitted electronically by mutual fund and insurance providers, are uploaded into the McCamish calculation module. The Transaction System is programmed to reject and not process transactions, if prices are not detected, and reports these unprocessed "pending" transactions in a log. The "pending" transactions are still held in a "pending status" within the Recordkeeping system. Prior to uploading new fund prices, Operations settles any prior day's pending transactions residing in the Transaction System. The recording system ensures that the new date's transactions are processed using the correct day's pricing. During the resolution of pending transactions, a batch log is generated which includes any errors that have been detected. On a daily basis, the Processing Specialist resolves all errors on the daily transaction load log and reviews an exception report that details if the fund's price is valued at zero or if there is a major fluctuation in the fund's price in order to process requested participants' elections. An independent QC review is performed to help ensure that all errors were addressed, and fund price updated were processed completely and accurately. Operations completes a daily pricing checklist to confirm that each business morning the pricing files are uploaded into the Transaction System accurately and completely.

On a daily basis, price files from numerous providers, such as Bloomberg, Vertical Management Systems, NSCC, and mutual fund/insurance providers are uploaded into the BOSS Pricing and Unitization module. A report from the BOSS Pricing and Unitization system identifies the Operations team when a fund's price is zero or if there was a fluctuation over 5% from the prior business day's price. To help ensure that the upload is complete and accurate, an exception report is reviewed daily by Operations that details if a fund's price is valued at zero or if there is a major fluctuation in the fund's price. Any issues are researched and resolved by Operations.

In the event that an incorrect price for a fund was uploaded into the Transaction System, the system can back out all financial transactions effected by the incorrect price, based on a range of entered dates, and reprocess all these transactions based on the fund's correct price. All

retroactive price corrections are reviewed for accuracy by the Operations Supervisor, Director of NQ Operations, Manager of NQ operations, or client prior to being executed within the Transaction System.

The BOSS pricing system provides the end user with a report that outlines the plans and models affected by any price change and the necessary process that must happen to make the corrections. The ability to update pricing is limited to Operations and Implementations personnel assigned access to the BOSS pricing module. All price changes are reviewed for accuracy by the Operations Manager, Operations Supervisor, Director of NQ Operations, or client prior to being executed within the Transaction System.

Trading Cut-off

Trades submitted prior to 4:00 PM Eastern Time (ET) are compiled, reviewed, and processed using that day's fund prices. The Transaction System is programmed to process and trade participant trading instructions received prior to 4:00 PM ET the same day. Participant requests received after 4:00 PM ET are processed and traded the following business or trading day. Trades made prior to market close are processed using the effective day's closing prices. These trading instructions are placed in a pending status and processed the following business day using the following business day's fund prices (or in accordance with plan guidelines with the effective day's closing prices). Exceptions to this rule are that some plan designs pend transaction data on monthly or quarterly release cycles.

Participant and Plan Reporting

a. Liability Reporting

On a daily basis, the Operations group processes client-received payrolls into the Transaction System. As part of the daily import process, the Transaction System information is imported into EDB. At period-end, Accounting Services generates Participant Account Activity Statements ("PAAS") from EDB and imports this information into NASA. At least quarterly, Accounting Services then performs the following:

- Compares the PAAS beginning balances to the ending balances of the prior month's PAAS,
- Reviews the reported gains and losses for reasonableness,
- Researches and resolves any discrepancies.

Accounting Services sends corrections for any discrepancies and errors to Client Services for entry into the Transaction System. Accounting Services re-imports a corrected PAAS into NASA which in turn generates a report that is sent to the client as part of the monthly Corporate Reporting Package, when applicable.

Accounting Services also generates a "Liabilities by Fund" report from the Transaction System which provides details of the ending liability balances by fund. As part of the periodic extract process into EDB, an internal Benefit Liability Report (BLR) is generated which is used to reallocate model portfolios investments across individual funds. The internal BLR is reviewed by Accounting Services to verify that liability balances contained in the model portfolio have been fully allocated to funds. When applicable, the Internal Benefit Liability Report is agreed to the Liabilities by Fund Report by Accounting Services and reviewed to help ensure that the allocations from the model portfolio investments were zeroed out. To help ensure that the amounts reported to the client are accurate, Accounting Services reconciles the ending liability balances from the following systems: EDB, and NASA. Any identified discrepancies are researched and resolved.

The reconciled Internal Benefit Liability Report is then imported into NASA which in turn generates an External Benefit Liability Report. The External Benefit Liability Report provides liability balances as of the valuation date, as well as the transaction summary for the period. This report is sent to the client as part of the monthly Corporate Reporting Package.

b. Plan Asset Reporting

Utilizing asset information that is already imported and accumulated as part of the rebalance process, Accounting Services generates an Asset Value Report through NASA on a monthly reporting basis. The Asset Value Report provides asset balances as of the valuation date, along with a transaction summary for the period. Accounting Services also receives asset transaction statements from mutual fund/insurance providers on a monthly basis. Details from these external asset transaction statements is manually entered into NASA. NASA compiles this detail into the transaction summary reflected on the Asset Value Report. At least quarterly, Accounting Services performs the following functions:

- Compares the Asset Value Report from NASA to the mutual fund and insurance carrier reports to verify that composite totals and transaction information is accurate,
- Compares beginning balances of the Asset Value Reports to the ending balances of the prior month's Asset Value Reports; and
- Reviews gains and losses for reasonableness based on the client's rebalance protocol, funding status, timing of transactions, and other account factors.

Discrepancies identified during the above operations are researched and resolved. The final Asset Value Report is included in the Corporate Reporting Package that is submitted to the sponsor on a periodic basis. Based on information contained in the Corporate Reporting Package, a Journal Entry report is generated to assist clients with recording the current month's transactions. The Journal Entry report listing journal entries generated relative to the deferred compensation program for the period is reviewed by Accounting Services to help ensure that the journal entries reported to the client are accurate based on the AVR's and Benefit Liability Report's ending balances. The journal entries are segregated by entries requiring manual postings, and entries that have already been posted by the sponsor's accounting system.

A checklist is completed by the Accounting Services staff to verify that the requisite preparation steps have been followed and documented for the Corporate Reporting Package (including the Assets Value Report, Benefits Liability Report, PAAS, and Journal Entry reports, when applicable). Also, Accounting Services verifies that the ending balances on the Asset Value Report and the Benefit Liability Report reconcile to the Deferred Compensation Journal Entry Report. Any discrepancies are researched and resolved. A sign-off by the Accounting Services staff on the checklist is used to document the reviews performed. The sponsor is responsible for reviewing the period- end reports and communicating with the Company if any discrepancies are detected.

Participant Statements

On a quarterly basis, the Plan Administrator reviews and reconciles the following exception reports that identify discrepancies between the Transaction System, the printed statements, and the website (www.newportgroup.com) to be sure that all areas are properly reflected in the following:

- The NQ Statement Balance/Units Audit Report,
- The Header Audit Report,
- The Deferral Audit Report,
- The Distribution Audit Report.

The Plan Administrator reviews quarterly participants' statements and selects a sample to verify the following for accuracy:

- Financial transactions to source documents,
- Distribution elections,
- Deferral elections.

The Non-Qualified Client Services Team monitors Case Tracking to verify that Participant Statements are made available to participants either by quarterly mailings or online through Statement on Demand. For newly implemented plans, the delivery date of the first statement delivered via quarterly mailings or posting to the online archive is negotiated in advance with the client. Statements delivered via quarterly mailings or posting to the online archive are made available to the participants by the 30th business day of the month following the close of each calendar quarter.

Non-Broad-Based COLI Billings

The COLI Insurance Services Administrator prepares the premium billing package. The package is reviewed by the Financial Analyst, Relationship Manager, Account Manager, Director of Financial Services, Senior Consultant, and/or Policy Administrator to determine the amount to be invoiced and how it is to be paid. If the policy has a flexible premium, the policy allocation is obtained from a member of Insurance Services, Client Services, or Financial Services.

With respect to the preparation of the billing packages for Non-Broad-based COLI, the CIS Administrator prepares the premium billing package. The package is reviewed by the Financial Analyst, Relationship Manager, Account Manager, Director of Financial Services, Senior Consultant, and/or Policy Administrator for reasonableness and consistency with the current Premium Payment Strategy prior to client distribution.

The Insurance Operations Team monitors the Premium Billings Deliverables Tracking spreadsheet to determine that the CIS Administrator, Relationship Manager, or Account Manager transmits the Premium Billing Package to the client with the payment amount and wiring instructions.

Once the transaction date is confirmed, COLI Insurance Services verifies that the movement of money from one location to the other was performed accurately, provides the insurance carrier with a roster of how to correctly apply the premium, and obtains verification from the insurance carrier that the premium was applied in accordance with the provided roster.

Imputed Income Reporting

For each report, the Insurance Services Policy Administrator, Account Manager, Financial Analyst, Relationship Manager, or Department Supervisor updates the prior year's rate table to the current year's rate table to verify the accuracy of all insurance carriers' one-year term insurance rate tables.

The Imputed Income Report is audited by the Policy Administrator, Account Manager, Financial Analyst, Relationship Manager or Department Supervisor to verify that the name, the policy number (or policy ID), and the imputed income (or economic benefit) amount are reported accurately. The Plan Administrator, Account Manager, Financial Analyst, Relationship Manager, or Department Supervisor monitors the Imputed Income Tracking Sheet to verify that the Imputed Income Report is sent to the client on or before the client deadline.

Insurance Benefit Participant Statements

Insurance Benefit Participant Statements are reconciled to the source data from the Client and Currency Policy values and reviewed by a member of Insurance Services, Client Services or Financial Services for accuracy.

The Benefit Plan Administrator monitors the Benefit Statement Tracking Document to verify that Insurance Benefit Participant Statements are mailed to the participants or the clients for distribution per the scheduled client due date as required by the Client Agreement.

COLI Best Practices Act

The CIS Administrator completes and monitors the tracking spreadsheet, evidencing preparation of the 101j Supporting Documentation and the 101j cover letters using policy values, census information, and data stored in LIAM for each client to determine that the tax year end deadlines are met.

The COLI Best Practice Audit Checklist is completed by the CIS Administrator for every 101j reporting package to verify the following critical items are accurate:

- Accurate policy numbers,
- Accurate number of insured individuals,
- Multiple individual policy identification, and
- Policy owner and tax information (TIN).

The 101j reporting package and corresponding COLI Best Practice Audit Checklist are reviewed by the Account Manager, Relationship Manager, or a peer CIS Administrator to verify that all fields are complete and accurate.

The Relationship Manager, Account Manager, or Policy Administrator verifies that 101j reporting packages are provided to the client no later than 45 business days after the client's tax year.

Death Claim Processing

The Company provides periodic reporting to COLI clients including recently reported deaths, Distribution of Proceeds, and Death Claims Status reports.

On a monthly basis, the Claims Administrator collects and forwards the new insured's personal information (e.g., social security numbers) through a secured file to a sweep vendor, a third-party service provider (not included in the scope of this report), to conduct weekly sweeps in an effort to identify deceased individuals. PBIS returns the file and provides a hard copy report with flags indicating deaths, location of deaths, and the date of deaths. The file is loaded into BOSS from which a report is generated. The BOSS report is then compared to the hard copy report from PBIS to verify that all deaths reported by PBIS have been loaded into BOSS correctly. The Claims Administrator reconciles the identified deceased insured individuals documented within the internal policy database to the file received by the sweep vendor to help ensure accuracy.

An audit is performed on the data returned by PBIS to identify policy lapses, previously reported deaths, and discrepancies. Any new claims uncovered by the Social Security sweep are then communicated to the client as well as the respective carriers. Research is conducted to determine the municipality or country (if outside the U.S.) in which the death occurred to order a valid death certificate. Approved death claim carrier forms are obtained from the client and are submitted along with the required documentation to the carrier for payment.

A Death Claim worksheet is received from the carrier with the details of the amount to be distributed to settle the claim. The worksheet is compared for reasonableness to the census or annual billing previously provided to the client. A proceeds report is created based upon the payment made by the carrier. The report is reviewed to help ensure the accuracy of the payment received from the carrier.

3. Institutional Trustee and Independent Fiduciary Services - Nondiscretionary Services ("NDS")

Newport provides trust and custodial services through a wholly owned subsidiary chartered by the New Hampshire State Banking Department. Newport serves as discretionary and non-discretionary trustee and custodian for qualified and non-qualified employee benefit plans, including defined benefit pension plans, voluntary employee beneficiary association plans, employee stock ownership plans, 401(k) plans, profit sharing plans and rabbi trusts.

Account Acceptance and Set-up

Newport plans originate from three different sources; sales ("New Accounts"), custodians entering a sub-custodial agreement with Newport ("Assigned Plans"), and from existing clients of Newport adding trust/custodial services ("Migrations").

Before accepting an account, an initial due diligence is conducted. In this review, the Company considers its ability to properly administer the account, including whether:

- The Company has the expertise and systems necessary to properly manage the account;
- The account meets the Company's risk standard;
- The type of account and the services to be provided by the Company;
- The existence of, or potential for, administrative problems.

In accordance with the Company's policies, certain due diligence procedures are conducted to ensure compliance with the Company's Bank Secrecy Act/Anti-Money Laundering (BSA/AML) policies including Office of Foreign Asset Control (OFAC) checks and Customer Identification Program (CIP) requirements.

Prospective plans are presented to a board appointed committee or a designated sub-committee (the "NDS Sub-Committee") for review to determine whether the account type requires special or unique skills to administer the assets, such as closely held assets, and to confirm that they are deemed acceptable assets under the Company's policy. The NDS Sub-Committee pre-approves the assets before the Company will proceed with the relationship. All pre-approvals are documented through the NDS Sub-Committee meeting minutes.

Once the governing documents have been executed and returned, the account is presented to the NDS Sub-Committee for final approval. The NDS Sub-Committee reviews the documentation, and if in good order, provides final approval. For New and Migrated accounts, final approval is given prior to the Company accepting responsibility for the account. For Assigned accounts final review of governing documents occurs upon receipt which may be some time after the account has been made active (the "Assignment Date").

A Checklist is completed by a member of the NDS Sub-Committee to verify that the appropriate documents were received and reviewed for completeness. The approval by the NDS Sub-Committee is documented in the checklist and/or meeting minutes.

Annual Administrative Reviews

Each account administered by the Company will be reviewed for proper administration annually to help ensure the completeness and accuracy of the account's governing instruments, Bank Secrecy Act procedures, transaction records, account reporting, fees, and risk assessment. The Company utilizes a "due-diligence" approach to the review process which utilizes a combination of internal audits, tickler systems, vendor reviews, checks and balances and other procedures to verify that, over the course of the year, all accounts are properly administered. The NDS Sub-Committee confirms or verifies, as appropriate, internal audit reports and other account level checks and balances are reviewed at least annually. The reviews, and details of any decisions made concerning the account, will be documented in the NDS Sub-Committee's minutes.

Account Terminations

The Sub-Committee reviews all terminating accounts to help ensure that all closing requirements have been discharged. For an account to be closed, all checks must have cleared, and no remaining balance may exist in the account.

The Deconversion Team processes the account closure and:

- Verifies that written notification is from an authorized party,
- Verifies that the account balances are zero,
- Verifies that all checks have been paid,
- Provides an Account Deconversion/Termination Notice or an executed Deconversion Authorization Form.

The NDS Sub-Committee reviews the account closure documentation during a NDS Sub-Committee meeting to help ensure the above noted items are on file and to acknowledge the account termination. Two members of the NDS Sub-Committee sign the Account Closing Checklist and document the review in the meeting minutes to evidence the review performed.

4. Institutional Trustee and Independent Fiduciary Services - Special Fiduciary Services ("SFS")

Account Acceptance and Set-up

Within 90 days of account setup in the Trust Application, a Relationship Manager performs a post-acceptance review to assess whether or not the Company has the authority to maintain the account and the results of the review are provided to the SFC.

For discretionary accounts: On an annual basis, the SFC performs a review of all individual accounts for which the Company has investment discretion to evaluate the suitability of the securities comprising the account.

Annual Administrative Reviews

On an annual basis, the Special Fiduciary Services Sub-Committee performs a review of all individual accounts for which the Company has investment discretion to evaluate the suitability of the securities comprising the account.

Account Terminations

The Sub-Committee reviews all terminating accounts to help ensure that all closing requirements have been discharged. For an account to be closed, all checks must have cleared, and no remaining balance may exist in the account. A review of the checklist by a responsible party is performed to help ensure that the supporting documentation is on file and authorized by the Plan Sponsor.

Transaction Processing

<u>New Security Setup</u>

Relationship Managers and Administrators verify that requests for new securities are submitted by authorized plan sponsor representatives. Upon receiving an e-mail confirmation from the third-party processor noting successful processing of the new security, the Company reconciles the new security setup to the Trust application against the instruction from the plan sponsor to help ensure complete and accurate processing by the third-party processor. Any discrepancies are researched and resolved.

Money Movement

Middle Office team members receive e-mail alerts when plan sponsor funds are received into the Company's Demand Deposit account ("DDA"). After funds and the associated plan sponsor instructions are received, an Account Administrator or Relationship Managers (RM) processes the transaction in the Trust Application, a Relationship Manager other than the processor reviews and approves the transaction in the Trust Application to help ensure the completeness and accuracy of processing. Access to process cash receipts in the Trust Application is restricted to appropriate Relationship Managers and Administrators. Access to set up outgoing wire transfers in the Trust Application is limited to Administrators and Relationship Managers. Wire transfers must be reviewed for accuracy and approved by a secondary individual prior to the wire transfer being initiated.

Lump Sum Payments

Prior to processing a distribution request, the RMs review the Plan Sponsor distribution requests to verify that the request is authorized. An Administrator and/or a Relationship Manager reviews the distribution request for completeness and confirms that adequate funds are available prior to approving and processing the payment in the Trust Application. For periodic payments, SFS reviews the Monthly Pension Check Register which details scheduled transaction payments entered to help ensure that funds will be available the day payments are due to post prior to month end (for monthly and quarterly payments).

Stock Distributions

For plan sponsor requested stock distributions, Relationship Managers and/or Administrators verify that the request was submitted by the authorized plan sponsor representatives. Authorized requests are submitted to the third-party processor for processing. The Relationship Manager and/or Administrator reviews the Trust Application for posting by the third-party processor.

Directed Accounts

Before processing trades requested by the plan sponsor, the Relationship Manager verifies that the request is properly authorized. The Relationship Manager or Administrator review the trade instructions entered into the Trust Application for accuracy.

Discretionary Accounts

Before processing trades, the Administrator or Relationship Manager verify that the request is properly authorized prior to entering the transaction into the Trust Application. The Relationship Manager or Administrator review the trade instructions entered into the Trust Application for accuracy.

Outside Managed Accounts

On a daily basis, the Operations Manager or designee performs an online review of DTC affirmed trades that are not pending in the Trust Application. Any DTC affirmed trades that are not pending in the Trust Application are researched and resolved.

Asset Reconciliation

On a daily basis, Administrators or Relationship Managers review the Daily Nightwork Batch Reports to monitor the previous day's activity. Any discrepancies are researched and resolved.

For discretionary accounts, the Un-invested Cash Report and Sweep Fund Balance report, which list un-invested cash broken out by discretionary accounts versus directed accounts and Custodian invested sweep fund balances, are submitted to the Special Fiduciary Services Sub-Committee ("SFC") for review annually.

Upon receiving an e-mail confirmation from the third-party processor noting successful processing of the new security, the Company reconciles the new security setup to the Trust application against the instruction from the Plan Sponsor to help ensure complete and accurate processing by the third-party processor. Any discrepancies are researched and resolved.

Daily, a Middle Office team member performs a reconciliation between the Trust Application and the Demand Deposit account ("DDA") to help ensure that all cash transactions are processed completely and accurately. Any differences are investigated and resolved. Monthly, the Middle Office team members review the Asset/Position Report and the Mutual Fund Reconciliation Report which provide an explanation of position breaks between the Trust Application and the custodian. Any unresolved position breaks are followed up on by the Middle Office team.

Valuations

The Company's management and Special Fiduciary Services Sub-Committee ("SFC") review the final valuations provided by the independent Financial Advisors for privately held stock. Any issues or concerns are raised to the Trust Committee for handling.

For securities that are not publicly traded (e.g., closely held equities, insurance contract, limited partnership), Relationship Managers and/or Administrators submit the reviewed prices to the third-party processor for processing. Relationship Managers and/or Administrators reconcile the pricing entries in the Trust Application to the updates provided by the pricing source to verify that pricing of non-publicly traded securities were entered accurately into the Trust Application.

E. Controls Related to Information Technology General Controls

1. Physical Security

Ascensus contracts with Data Center vendors and mandates that they maintain a security environment that includes physical access security controls including zoned keycard access, CCTV, and biometric entry controls as a Multi-Factor Authentication parameter for entry. All individuals visiting the Ascensus dedicated area (cage) must sign-in with a government issued identification and be escorted at all times. Ascensus manages access to the dedicated area and all access is regularly reviewed, with access immediately removed upon termination or a change in job responsibilities that no longer would require access. Data Center vendors continued adherence to those contractual mandates is overseen by the Ascensus Vendor Compliance program, which assesses all vendors on at least an annual basis via detailed questionnaires and on-site reviews.

Ascensus leverages the offshore services of RR Donnelley to support some business operations. Ascensus monitors access controls at the RRD offshore facilities monthly.

2. Backup

To help ensure that Ascensus can effectively recover operations as quickly as possible in the event of a system interruption or unintended loss of data, backup records for the systems are produced each business day and stored at a secure off-site location. Ascensus has protocols in place to create these backups, and has secure methods to track and retrieve them, when needed. Only authorized associates can execute the backup creation process or modify the backup schedule. Issues with backup creation are reported on the Tivoli Storage Management® (TSM) Monitor Report and the VMware® backup report, are escalated to the backup manager and are resolved to help ensure that the off-site records are properly maintained. Additionally, to facilitate disaster recovery, data is replicated to Ascensus-owned equipment securely stored at an off-site data center that is more than 2,400 miles from the primary data center.

Backups are tested in conjunction with the testing of disaster recovery procedures to ensure that, in the event of an incident or data loss, Ascensus is prepared to resume operations and/or recover data as quickly as possible. During the disaster recovery testing, backups are used to bring the systems up remotely and business users mimic live production processing using the backups.

3. Logical Access

Access to Ascensus's systems that store client data is monitored. Before a new user is added or additional access is granted to an existing user, management authorization is required. Requests for new or modified access are submitted via the ticketing system and are reviewed to help ensure that only those with a business need for the access are approved by management before the access is granted. To help ensure that access is closely tied with job functions, users are granted access based on profiles defined by business group management.

All passwords must conform to corporate requirements for complexity, and users are required to periodically change their passwords. Individuals who terminate employment with Ascensus will have their access to Ascensus's systems revoked within two business days; this process is coordinated through the HR team.

Access to the UNIX system's "root password" and the Windows System Administrator is password restricted to authorized Ascensus employees. The list of those granted this authorization is regularly reviewed.

Client data is not housed off-shore at any time; rather, off-shore associates supporting the qualified plan business line access data via secure connections to the on-shore Ascensus data center. Offshore associates have no ability to save data to local drives and their ability to print hard copy materials is limited, and does not include the ability to print client data. These rights are directly and controlled by onshore Ascensus IT personnel.

4. Change Management

Changes to Ascensus's systems are tested and approved before they are moved into a "live" production environment to validate that the new code works as intended and can run within the required time constraints. The change process begins with a request from the business team for new or altered functionality and requires a review from impacted business teams to verify that the proposed approach will meet their needs. Once a project has been approved by business users, it is reviewed to determine whether the project is appropriate. Once requests have been approved, they are prioritized based on the criticality of the requested change. The status of projects and their associated priorities are reviewed and managed by IT management so that executive-level management is aware of the status of IT requests. Development work is performed in a segregated development environment. New functionality cannot be moved into the production environment without successful completion of testing (described below) and the approval of IT management. Only authorized individuals can implement new functionality into production.

New functionality is tested, and the testing is tracked via checklists that require sign-off by developers. Once new functionality is ready to be implemented, changes are released via a prescribed schedule. Business team management is notified of new functionality and its scheduled release so that management can inform associates impacted by the change prior to the release. Any functionality that is critically required and cannot wait until the next scheduled release must be approved for an emergency release by a member of the senior management team. Similarly, security patches or updates that are provided by vendors must first be loaded to the development environment and tested to assess impact on systems before they are implemented in the production environment.

Addition of new hardware or operating systems must be approved by senior leadership and the impact is assessed in the development environment prior to rollout to production regions. New servers within Ascensus's production environment are requested and deployed using a virtual server workflow and provisioning tool. Once a request has been approved, a server is systematically built based on an image configured according to defined standards.

5. Computer Operations

Automated jobs are scheduled and executed throughout the day to update participant accounts. Each of these jobs is monitored to help ensure that they execute timely and run to completion. This monitoring is accomplished (i) via detailed run sheets that outline each step to be executed and require signed confirmation that each step has been completed, or (ii) via automated monitoring using the batch scheduler, which verifies completion of automated jobs. Logs of completed run sheets are maintained for management review and issues encountered during job execution are noted in the logs. The logs also serve to alert associates during shift turnovers of any issues carrying over into their shifts.

Daily meetings, attended by IT and business associates, are held to discuss issues across the organization and their potential impact. Escalation procedures for system issues are maintained and are accessible to associates to facilitate prompt resolution of issues and minimize the impact on the business.

Ascensus maintains an Escalation and Incident Response Policy. Security incidents resulting in unauthorized access to, or misuse of, data are subjected to documented procedures, including notification of affected parties per operational agreements, contractual commitments, and statutory requirements.

F. Additional Information about Management's Description

The Company has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives and related controls are presented within Section IV of this report, "Description of Ascensus, LLC's Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results," and are an integral component of the Company's description of its system as described within this section.

G. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve specific control objectives, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control over financial reporting must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Table 1

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Csquare	All Business Lines	Csquare is the primary site for third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable control objective: • Controls around the physical security of the Data Center ensuring that physical access to the system resources is restricted to authorized individuals, and the physical environment is monitored and protected from disruptive events. In addition, the Company has identified the following controls to help monitor the subservice organization. • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objectives 1 - 39

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Switch	All Business Lines	Switch is the backup site for third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable control objective: • Controls around the physical security of the Data Center ensuring that physical access to the system resources is restricted to authorized individuals, and the physical environment is monitored and protected from disruptive events. In addition, the Company has identified the following controls to help monitor the subservice organization. • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objectives 1 - 39

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Infosys McCamish Systems, LLC ("McCamish")	Non-Qualified Plans	Infosys McCamish Systems, LLC develops and hosts the McCamish Application including the calculation module portion of the Transaction System. The following control area is critical to achieving the applicable control objectives: • Controls around ensuring the accuracy of calculations (i.e., payroll, deferral, client/Plan Sponsor contribution information, scheduled and non-scheduled disbursement information, participant fund transfers, allocation charges, and rebalances) of the transaction module. • Controls around ensuring changes to McCamish Application are tested and approved prior to implementation into production. • Controls around limiting physical access to the system resources to authorized individuals, and the monitoring and protection of the physical environment from disruptive events. • Controls around limiting logical access to programs and data to properly authorized individuals. • Controls around backup and restoration procedures. • Controls around the monitoring of computer operations.	Control Objective 15 Control Objective 17 Control Objective 19 Control Objective 35 Control Objective 36 Control Objective 37 Control Objective 38 Control Objective 39

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
		In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	
SEI Private Trust Company (SEI)	Non-Qualified Plans & Institutional Trustee and Independent Fiduciary Services	SEI Private Trust Company provides change management, logical security, and computer operations for the Trust 3000, DepLink, RBPS, CSS, and Cconnect applications. The following control areas are critical to achieving the applicable control objectives: • SEI is responsible for providing account opening, account maintenance, and account closing services recorded within Trust 3000 application. • SEI is responsible for providing Trust 3000 application Asset/ Position, Cash and Mutual Fund reconciliation reporting services. • SEI is responsible for providing securities setup and change assets services recorded within Trust 3000 application. • SEI is responsible for providing securities transactions processing, settlement, and recordkeeping services utilizing the Customer Strata Station Browser (“CSS”) and Trust 3000 applications.	Control Objective 29 Control Objective 30 Control Objective 31 Control Objective 32 Control Objective 33 Control Objective 34 Control Objective 36 Control Objective 37

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
		• SEI is responsible for providing contributions and disbursement processing services utilizing the Retirement Benefit Plan System ("RBPS"), Customer Strata Station Browser ("CSS"), and Trust 3000 application. • SEI is responsible for providing the monitoring of trades and trade processing services recorded within the Trust 3000 application. • SEI is responsible for providing corporate action identification, processing, and settlement and recordkeeping services recorded within Trust 3000 application. • SEI is responsible for providing processing for closely held securities and pricing services recorded within the Trust 3000 application. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
RR Donnelley ("RRD") Global Outsourcing	Qualified Plans	The Company uses RRD for completion of data entry and quality reviews of participant demographic and distribution data, data entry and quality reviews of plan-level exceptions related to payroll submitted to Ascensus for processing, monitoring of identified fund position variances between Ascensus and the transfer agent for timely resolution, and review of plan and participant reports, including quality review of quarterly participant statements. The following control area is critical to achieving the applicable control objectives: • Controls around data entry and quality reviews of participant demographic and distribution data. • Controls around data entry and quality reviews of plan-level exceptions related to payroll submitted to Ascensus for processing. • Controls around monitoring of identified fund position variances between Ascensus and the transfer agent for timely resolution. • Controls around review of plan and participant reports, including quality review of quarterly participant statements. • Controls around physical access at RRD facilities controlled by cardkeys. • Controls around the distribution of cardkeys is managed by offshore leadership. • Controls around timely removal of physical access to RRD facilities for terminated employees.	Control Objective 3 Control Objective 7 Control Objective 8 Control Objective 9 Control Objective 10 Control Objective 11 Control Objective 12 Control Objective 36

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
		In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Pension Benefit Information Services ("PBIS"), LexisNexis and LifeStatus360	Non-Qualified Plans	PBIS, LexisNexis and LifeStatus360 are provider of death index data used to determine when plan participants have passed away generating claims and benefit payouts. The following control area is critical to achieving the applicable control objectives: • Controls provide reasonable assurance that death index data is complete and accurate. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Claims Administrator reconciles the identified deceased individuals documented within the Oracle database to the files receive from PBIS, LexisNexis and LifeStatus360. • The Company obtains valid proofs of death to validate deaths listed in the PBIS, LexisNexis and LifeStatus360 death index data. • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objective 28

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Vertical Management System ("VMS")	Qualified Plans & Institutional Trustee and Independent Fiduciary Services	Vertical Management System provides change management, logical security, and computer operations for the HUB+ application that is used for direct trading of mutual funds with the National Securities Clearing Corporation ("NSCC"). The following control area is critical to achieving the applicable control objectives: • Controls around ensuring changes to HUB+ are tested and approved prior to implementation into production. • Controls around limiting physical access to the system resources to authorized individuals, and the monitoring and protection of the physical environment from disruptive events. • Controls around limiting logical access to programs and data to properly authorized individuals. • Controls around backup and restoration procedures. • Controls around the monitoring of computer operations. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objective 7 Control Objective 8 Control Objective 10 Control Objective 11 Control Objective 36 Control Objective 37 Control Objective 38 Control Objective 39

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Mid Atlantic Trust Company ("MATC")	Qualified Plans & Institutional Trustee and Independent Fiduciary Services	MATC provides trust accounting, trading operations, and aspects of custodial services. The following control areas are critical to achieving the applicable control objectives: • Controls around the assurance that the bank accounts for Trust Accounting Locations are reconciled, and the financial statements are reviewed for accuracy. • Controls around the assurance that trading operations are recorded accurately and completely. • Controls around management safeguarding assets under custody, produces reliable financial reports, and complies with laws and regulations. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objective 10 Control Objective 11 Control Objective 29 Control Objective 30 Control Objective 31

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Matrix Trust Company ("Matrix")	Qualified Plans & Institutional Trustee and Independent Fiduciary Services	Matrix provides trust accounting, trading operations, and aspects of custodial services. The following control areas are critical to achieving the applicable control objectives: • Controls around the assurance that the bank accounts for Trust Accounting Locations are reconciled, and the financial statements are reviewed for accuracy. • Controls around the assurance that trading operations are recorded accurately and completely. • Controls around management safeguarding assets under custody, produces reliable financial reports, and complies with laws and regulations. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objective 10 Control Objective 11 Control Objective 29 Control Objective 30 Control Objective 31

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Charles Schwab ("Schwab")	Qualified Plans & Institutional Trustee and Independent Fiduciary Services	Charles Schwab provides trust accounting, trading operations, and aspects of custodial services. The following control areas are critical to achieving the applicable control objectives: • Controls around the assurance that the bank accounts for Trust Accounting Locations are reconciled, and the financial statements are reviewed for accuracy. • Controls around the assurance that trading operations are recorded accurately and completely. • Controls around management safeguarding assets under custody, produces reliable financial reports, and complies with laws and regulations. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objective 10 Control Objective 11 Control Objective 29 Control Objective 30 Control Objective 31

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
RR Donnelley Thurmont ("RRD Thurmont")	Qualified Plans	RRD Thurmont provides external print and fulfillment services for scheduled and ad-hoc mailings, including enrollments, quarterly participant statements, year-end reporting, and 1099 tax filings. The following control areas are critical to achieving the applicable control objectives: • Controls around the completeness, accuracy, timely printing, and mailing of tax filling, participant statements and plan sponsor administration reports. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objective 12 Control Objective 13

Subservice Organization	Relevant Business Area	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
QUODD Financial Information Services, Inc. (“QUODD")	Qualified Plans	QUODD provides pricing information that is loaded into the system. They are responsible for providing market quotations for the majority of securities, which are then uploaded into ARS via automated data interfaces. The following control areas are critical to achieving the applicable control objectives: • Controls around the completeness, accuracy and timely communication of pricing information and market quotations. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	Control Objective 10 Control Objective 11

H. Complementary User Entity Controls

Ascensus, LLC’s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company’s system. It is not feasible for the control objectives to be solely achieved by the Company. Therefore, each user entity’s internal control over financial reporting must be evaluated in conjunction with the Company’s controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified within the table below, where applicable. Complementary user entity controls and their associated control objectives are included within the table below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Qualified Retirement Plans

User Entity Controls	Associated Control Objectives
User entities are responsible for reviewing plan documents and approving the plan/system setup for completeness and accuracy. Based on partner agreements, PEKs are reviewed for accuracy.	Control Objective 1
User entities are responsible for providing written notification of plan changes to Ascensus timely.	Control Objective 1 Control Objective 2
For conversion plans, the user entities are responsible for reviewing and communicating any required changes to the participant-indicative and financial information acquired from the prior recordkeeper.	Control Objective 2
User entities are responsible for reviewing plan valuation reports, trust asset reconciliation reports and summaries of participant changes and communicate any discrepancies to Ascensus timely.	Control Objective 2
User entities are responsible for providing complete and accurate transaction information.	Control Objective 3 Control Objective 4 Control Objective 6
User entities are responsible for updating and communicating the necessary partner guidelines to Ascensus.	Control Objective 4
User entities are responsible for communicating to participants their responsibility for ensuring trades processed, including those by phone, are accurate.	Control Objective 4
User entities are responsible for authorizing internet and IVR system-initiated disbursements for plans requiring plan sponsor authorization for distributions. User entities are responsible for communicating to participants their responsibility for ensuring transactions entered IVR are accurate.	Control Objective 5 Control Objective 6
User entities are responsible for securely maintaining their login credentials. User entities are responsible for communicating to participants their responsibility for maintaining their login credentials.	Control Objective 6
Participant contributions are submitted to the trustee, consistent with DOL guidelines.	Control Objective 7
User entities are responsible for providing employee payroll information sent to Ascensus for contributions (associate and employer), loan repayments and compliance processing is accurate, complete, and provided on a timely basis.	Control Objective 7 Control Objective 9 Control Objective 11

User Entity Controls	Associated Control Objectives
User entities are responsible for timely communication of any changes to the individuals authorized to approve distributions for plans requiring plan sponsor authorization for distributions.	Control Objective 8 Control Objective 11
User entities are responsible for reviewing an approving participant-submitted forms, including Enrollments, Loan Requests, Fund Balance Transfers, Investment Allocation Changes, Distribution Requests and Qualified Domestic Relation Orders (QDROs) prior to submission to Ascensus, depending on plan specifications.	Control Objective 2 Control Objective 7 Control Objective 8 Control Objective 9 Control Objective 11
User entities are responsible for reviewing participant forms submitted to Ascensus to ensure they are accurate, complete, properly authorized, and in accordance with the plan's requirements and criteria.	Control Objective 2 Control Objective 7 Control Objective 8 Control Objective 11
User entities are responsible for providing complete and accurate plan and participant compliance data (highly compensated associates, loan default determinations, etc.) and the overall status of plan compliance consistent with IRS and DOL guidelines.	Control Objective 12 Control Objective 13
User entities are responsible for reviewing participant data contained within the ADP/ACP test generated by Ascensus in the event of failures so that appropriate corrective action can be taken by the end of the following plan year. User entities are responsible for reviewing the accuracy of Form 5500 produced by Ascensus prior to filing with the IRS by the required deadline.	Control Objective 13
User entities are responsible for reviewing, removing, or modifying access to client portals as necessary.	Control Objective 36 Control Objective 37

Non-Qualified Retirement Plan Business Line User Entity Controls

User Entity Controls	Associated Control Objectives
User entities are responsible for providing complete and accurate client provisions within the Plan Information Guide.	Control Objective 14 Control Objective 16
User entities are responsible for providing complete and accurate transaction information.	Control Objective 15
User entities are responsible for designating a Plan Sponsor who is authorized to make decisions for the plan. User entities are responsible for reviewing and approving the plan level and investment level liability reconciliations between the prior record keeper and Ascensus.	Control Objective 16
User entities are responsible for designating a Plan Client/Sponsor to review and approve the Plan Administration Manual, including plan setups.	Control Objective 16
User entities are responsible for reviewing the disbursement amount, generating the disbursement proceeds, and delivering these proceeds to the participant.	Control Objective 17
User entities are responsible for providing complete and accurate payroll information and resolving any discrepancies related to payroll data.	Control Objective 17
User entities are responsible for notifying the Company of retirements, terminations, and known deaths or any other participant status or election changes for each plan participant and insured employee, where applicable, in a timely manner following the applicable status change, along with effective termination date and/or end of severance date.	Control Objective 17
User entities are responsible for establishing guidelines related to wire transfers. User entities are responsible for reviewing the wire transfer confirmation and notifying the Company of any errors. User entities are responsible for the completeness and accuracy of the allocation instructions.	Control Objective 18
User entities are responsible for the review of the trade confirmations for completeness and accuracy and to inform the Company of any changes/updates.	Control Objective 19

User Entity Controls	Associated Control Objectives
User entities are responsible for ensuring that participants understand their responsibilities with regards to accurate and complete information for participant requested activities, as follows: • Participants are responsible for reviewing their statements and communicating with the Company if discrepancies are detected. • Participants are responsible for reviewing prospectuses for investments that provide prospectuses prior to investing. • Participants are responsible for reviewing the Fund Transfer and Allocation Changes they entered on the Company's website. • Participants are responsible for the accuracy of participant elections. • Participants are responsible for reviewing non-financial data changes prior to releasing the transaction for processing. • Participants are responsible for reviewing confirmation statements and notifying the sponsor if inaccurate information was processed. • Participants are responsible for reviewing their Enrollment Confirmation and contacting the Company for any noted discrepancies.	Control Objective 20
User entities are responsible for the review of the Corporate Reporting package for completeness and accuracy and to inform the Company of any changes/updates.	Control Objective 22
For newly implemented plans, user entities are responsible establishing delivery guidelines for the first participant statement.	Control Objective 23
User entities are responsible for communicating Imputed Income Reporting deadlines.	Control Objective 25
User entities are responsible for providing accurate and complete client data and Client Agreements.	Control Objective 26
User entities are responsible for communicating the applicable tax year end to the Company.	Control Objective 27
User entities are responsible for notifying the Company in the event of an insured's death that they are aware of and for authorizing any claim forms required to submit a death claim to carriers.	Control Objective 28
User entities are responsible for securely maintaining their login credentials. User entities are responsible for communicating to participants their responsibility for maintaining their login credentials.	Control Objective 36

User Entity Controls	Associated Control Objectives
User entities are responsible for reviewing, removing or modifying access to client portals as necessary.	Control Objective 36 Control Objective 37

Institutional Trustee and Independent Fiduciary Services Business Line User Entity Controls

User Entity Controls	Associated Control Objectives
User entities are responsible for the following: • Providing current signed plan documents. • Communicating changes to the plan and new plan amendments on a timely basis. • Providing instructions and information that are in accordance with the provisions of the account agreement. • Providing timely notification of changes to account documents and other significant account information. • Providing timely notification to changes to individuals authorized to instruct the Company on behalf of the plan sponsor. • Performing timely review of reports provided by the Company and notification of any inaccuracies. • Providing timely written notification of changes to related parties. • Plan sponsors should provide timely written notification of account termination to Ascensus.	Control Objective 29 Control Objective 30 Control Objective 31 Control Objective 32 Control Objective 33
User entities are responsible for sending complete and accurate trade requests.	Control Objective 32
User entities are responsible for sending complete and accurate distribution requests.	Control Objective 32
User entities are responsible for sending complete and accurate stock distribution requests.	Control Objective 32
User entities are responsible for reviewing, removing or modifying access to client portals as necessary.	Control Objective 36 Control Objective 37

IV. Description of Ascensus, LLC's Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results

A. Types and Descriptions of the Tests of Operating Effectiveness Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at user entities and subservice organizations, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at the Company.

Our examination was limited to the control objectives and related controls specified by the Company in Sections III and IV of the report and did not extend to the controls in effect at user entities and subservice organizations.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess the internal control environment. If the internal controls are not effective at a user entity, the Company's controls may not compensate for such weaknesses.

The Company's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by the Company, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used within this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observed the application, performance, or existence of the control
Inspection	Inspected documents, records, or other evidence indicating performance of the control
Reperformance	Reperformed the control, or processing of the application control, for accuracy of its operation

Inquiries were performed for substantially all controls in Section IV, and, therefore, inquiries were not separately listed as a test for every control.

Additionally, procedures were performed to evaluate whether information produced by the service organization was sufficiently reliable for our purposes, including (i) information provided by the service organization in response to ad hoc requests from the service auditor, such as population lists; (ii) information used in the execution of a control, such as exception reports or transaction reconciliations; and (iii) information prepared for user entities, such as user access lists. “Sufficiently reliable” for our purposes means that we obtained evidence about the accuracy and completeness of such information and evaluated whether the information was sufficiently precise and detailed. Information produced by the service organization that we utilized as evidence included, but was not limited to, the following:

- System-generated reports without customization (canned reports);
- System-generated reports with customization (internally developed custom reports, queries, or ad hoc custom reports); and
- Manually prepared spreadsheets, analysis, schedules, or other evidence prepared by the service organization and utilized for the performance or testing of a control.

The procedures we performed to evaluate whether the information was sufficiently reliable included obtaining evidence regarding accuracy and completeness, including procedures to address the accuracy and completeness of source data, as well as the creation and modification of applicable report logic and parameters. The procedures performed included tests of controls over the preparation and maintenance of the information or observation or inspection procedures on the information. Although these procedures are not separately listed as a test procedure, the procedures were completed as part of our testing to support the evaluation of whether the information produced by the service organization was sufficiently precise and detailed for purposes of testing the controls identified by the service organization in Section IV.

B. Control Objectives, Control Activities, Tests of Controls, and Results

Control Objective 1

Controls provide reasonable assurance that plan parameters and specifications are set up accurately, completely, and timely for new and converted plans.

Control Activity		Tests Performed By Service Auditor	Results of Testing
1-1	New and converted plan installation policies and procedures are documented and available on the Ascensus intranet site.	**Observation:** Observed the Ascensus intranet site to determine that new and converted plan installation policies and procedures were documented and available.	No exceptions noted.
		Inspection: Inspected new and converted plan installation policies and procedures documentation to determine that new and converted plan installation policies and procedures were documented.	No exceptions noted.
1-2	Timelines for the installation of new and converted plans are recorded and monitored by the Installation Coordinator using an installation timeline.	**Inspection:** Inspected the installation timeline for a sample of new and converted plans to determine that each selected new or converted plan was recorded and monitored by the Installation Coordinator using an installation timeline.	No exceptions noted.
1-3	A quality review is performed to verify plan parameters (such as parameters for calculating vesting amounts) have been set up completely and accurately in ARS. The reviewer signs off on the Plan Rules Audit Memo as evidence of review prior to sending the go-live email to the client confirming that all final go live activities have been completed.	**Inspection:** Inspected the quality review documentation for a sample of new and converted plans to determine that, for each selected new or converted plan, a quality review was performed to verify plan parameters had been set up completely and accurately in ARS and the reviewer signed off on the Plan Rules Audit Memo prior to sending the email to the client confirming all final go live activities have been completed.	No exceptions noted.

Control Objective 1

Controls provide reasonable assurance that plan parameters and specifications are set up accurately, completely, and timely for new and converted plans.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
1-4	On a daily basis, a review is performed of the Business Projections Report that shows the status of each plan. Plans on the report that have not been installed are tracked and their status is documented.	**Inspection:** Inspected the business projections report for a sample of days to determine that a review was performed and showed the status of each plan on each selected day. Further, determined that for each selected day, any plans on the report that had not been installed were tracked and their status was documented.	No exceptions noted.

Control Objective 2

Controls provide reasonable assurance that participant records received from prior recordkeepers are reflected accurately and completely on the Ascensus Recordkeeping System, and that the conversion fund balances are complete and accurate.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
2-1	For conversion plans, Ascensus works with the plan's prior recordkeeper to acquire participant-indicative and financial information for upload into ARS. Plan data from the prior recordkeeper (vested amounts, hardships available, YTD date, etc.) is reviewed in ARS for accuracy by Transition Services associate. Conversion fund balances and loans loaded into ARS are reconciled to the prior recordkeeper's ending balance from the Participant Account Status Report via transfer method checklists to ensure fund balances are converted completely.	**Inspection:** Inspected the checklist and supporting documentation related to a selected sample of converted plans to determine that, for each selected plans' data from the prior recordkeeper was reviewed in ARS for accuracy by Transition Services associate. Further, determined that, for each selected plan, conversion fund balances and loans loaded into ARS were reconciled to the prior recordkeeper's ending balance from the Participant Account Status Report via transfer method checklists to ensure fund balances were converted completely.	No exceptions noted.
2-2	Transition Services associates reconcile final valuation data from the prior recordkeeper to the total amount in the contribution account at the trust company via the Trust System Plan Activity Report.	**Inspection:** Inspected the checklist and Trust System Plan Activity Report related to a sample of converted plans to determine that, for each selected plan, Transition Services associates reconciled final valuation data from the prior recordkeeper to the total amount in the contribution account at the trust company via the Trust System Plan Activity Report.	No exceptions noted.

Control Objective 2

Controls provide reasonable assurance that participant records received from prior recordkeepers are reflected accurately and completely on the Ascensus Recordkeeping System, and that the conversion fund balances are complete and accurate.

Control Activity		Tests Performed By Service Auditor	Results of Testing
2-3	Ascensus associates complete and sign the Service Item Checklist and IC Final Audit Go Live Checklist as evidence of review and that participant and financial information was loaded into ARS completely and accurately.	**Inspection:** Inspected the checklist and supporting documentation related to a selected sample of converted plans to determine that, for each selected plan, Ascensus associates completed and signed the Service Item Checklist and IC Final Audit Go Live Checklist as evidence of review and that participant and financial information was loaded into ARS completely and accurately.	No exceptions noted.

Control Objective 3

Controls provide reasonable assurance that participant transactions received via mail or fax are processed accurately, completely, and timely.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
3-1	An audit trail is maintained in the BPM tool to help ensure that transactions modified by Ascensus associates are properly logged within the system.	**Observation:** Observed the audit trail within the BPM tool to determine that transactions modified by Ascensus associates were properly logged within the system.	No exceptions noted.
3-2	The BPM tool is configured to prevent null or invalid SSN and required data from being entered into transaction forms by the Transaction Processing associates.	**Observation:** Observed a user attempt to input null or invalid SSN and required data into the BPM tool to determine that the BPM tool was configured to prevent null or invalid SSN and required data from being entered into transaction forms by the Transaction Processing associates.	No exceptions noted.
3-3	The BPM tool is utilized to monitor the business area queues to help ensure work is processed timely.	**Observation:** Observed the work queues in BPM to determine that the BPM tool was utilized to monitor the queues to help ensure work was processed in a timely manner.	No exceptions noted.
3-4	Ascensus associates use a BPM tool to scan and index transaction requests, which are then electronically sent to the relevant business unit. Images are stored in the BPM tool for retrieval. Operations associates review financial transactions entered in ARS for accuracy, completeness and timeliness after data entry and evidence their review by signing off on the corresponding transmittal form or via electronic sign-off in the BPM system. Any issues identified are resolved prior to sign-off.	**Observation:** Observed the Associate of the Service Support Group scan and index a selected incoming transaction request to the BPM system to determine that the request was scanned and electronically delivered to the appropriate business unit for processing and document images were stored in the BPM tool for retrieval.	No exceptions noted.

Control Objective 3

Controls provide reasonable assurance that participant transactions received via mail or fax are processed accurately, completely, and timely.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the corresponding transmittal form and/or electronic sign-off in the BPM system related to a sample of financial transactions entered in ARS to determine that operations associates reviewed and signed off on each selected financial transaction entered into ARS for accuracy, completeness, and timeliness after data entry and any issues were resolved prior to sign-off.	No exceptions noted.
3-5	Activity entered and verified in ARS prior to the cut-off time is submitted for trading that day. Transactions entered in ARS after the cut-off time are automatically pended by the system until the next day's processing.	**Observation:** Observed Ascensus personnel enter activity into ARS prior to the cut-off time to determine that the transaction entered was automatically submitted for trading that day.	No exceptions noted.
		Observation: Observed Ascensus personnel enter activity into ARS after the cut-off time to determine that the transaction entered after the cut-off time were automatically pended by the system until the next day's processing.	No exceptions noted.

Control Objective 4

Controls provide reasonable assurance that participant transactions received via phone are authorized and processed accurately, completely, and timely.

Control Activity		Tests Performed By Service Auditor	Results of Testing
4-1	Participant Services associates are required to repeat the trade transaction details to the caller prior to processing the request. Once the trade transaction has been processed, the Participant Services associates provide the caller with the system-generated confirmation number as evidence that the transaction was processed.	**Inspection:** Inspected the corresponding recordings related to a sample of participant transactions requested via telephone to determine that, for each selected transaction, the Participant Services associate repeated the trade transaction details to the caller prior to processing the request. Further, determined that, once the selected trade transaction had been processed, the Participant Services associate provided the caller with the system-generated confirmation number as evidence that the transaction was processed.	No exceptions noted.
4-2	Participant Services associates authenticate participants, in accordance with partner guidelines, prior to processing account information or transactions.	**Inspection:** Inspected the corresponding recordings related to a sample of participant transactions requested via telephone to determine that, for each selected transaction, Participant Services associates authenticated participants, in accordance with partner guidelines, prior to processing account information or transactions.	No exceptions noted.

Control Objective 4

Controls provide reasonable assurance that participant transactions received via phone are authorized and processed accurately, completely, and timely.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
4-3	Trade transactions received via phone for accounts with balances over $100,000 are systematically routed for a second independent review by the Participant Services team for accuracy and completeness. Any issues noted are resolved prior to processing.	**Inspection:** Inspected the review evidence related to a sample of participant transactions requested via telephone over $100,000 to determine that the selected trade transactions in accounts with balances over $100,000 were systematically routed for a second independent review by the Participant Services team for accuracy and completeness. Further, inspected the review evidence related to a sample of participant transaction requested via telephone over $100,000 and inquired of the Senior Call Center Representative to determine that there were no issues identified; however, if any issues has been identified, each issue would be resolved prior to processing.	No exceptions noted.
		Observation: Observed a transaction in an account with a balance over $100,000 to determine that transactions in accounts with balances over $100,000 were systematically routed for a second independent review by the Participant Services team for accuracy and completeness.	No exceptions noted.
4-4	Activity entered and verified in ARS prior to the cut-off time is submitted for trading that day. Transactions entered in ARS after the cut-off time are automatically pended by the system until the next day's processing.	**Observation:** Observed Ascensus personnel enter activity into ARS prior to the cut-off time to determine that the transaction entered was automatically submitted for trading that day.	No exceptions noted.
		Observation: Observed Ascensus personnel enter activity into ARS after the cut-off time to determine that the transaction entered after the cut-off time were automatically pended by the system until the next day's processing.	No exceptions noted.

Control Objective 4

Controls provide reasonable assurance that participant transactions received via phone are authorized and processed accurately, completely, and timely.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
4-5	Participant calls are conducted on recorded lines and archived by the Telecommunications department.	**Inspection:** Inspected the corresponding recordings and archive documentation related to a sample of participant transactions requested via telephone to determine that, for each selected transaction, participant calls were conducted on recorded lines and archived by the Telecommunications department.	No exceptions noted.

Control Objective 5

Controls provide reasonable assurance that participant transactions received via the Interactive Voice Response (IVR) system are authorized and processed accurately, completely, and timely.

Control Activity		Tests Performed By Service Auditor	Results of Testing
5-1	Participants must enter a social security number (SSN) and personal identification number (PIN) to access their account and perform transactions via the IVR.	**Observation:** Observed a user acting as a participant access the IVR to determine that they were required to enter their social security number (SSN) and personal identification number (PIN) to access their account and perform transactions.	No exceptions noted.
5-2	The IVR system is programmed to prevent transactions under the following conditions: • Pending unposted transactions exist (error message given to participant). • Individual funds are restricted. • The participant attempts more fund-to-fund transfers than allowed by the plan.	**Observation:** Observed a user access the IVR system to determine that error messages were generated and the transaction was prevented when the following conditions were met: • Pending unposted transactions existed (error message given to participant). • Individual funds were restricted. • The participant attempted more fund-to-fund transfers than allowed by the plan.	No exceptions noted.
5-3	The IVR is programmed to repeat the details of the transaction and prompt the participant to confirm the details prior to submitting the transaction to ARS for processing. The IVR provides the user with a verbal confirmation.	**Observation:** Observed a user access the system using a test account to determine that the IVR was programmed to repeat the details of the transaction and prompt the participant to confirm the details prior to submitting the transaction to ARS for processing, and the IVR provided the user with a verbal confirmation.	No exceptions noted.
5-4	The IVR is programmed to permit a participant to cancel a transaction by pressing the star key at any time during the call.	**Observation:** Observed a user access the IVR system using a test account to determine that the IVR was programmed to permit a participant to cancel a transaction by pressing the star key at any time during the call.	No exceptions noted.

Control Objective 5

Controls provide reasonable assurance that participant transactions received via the Interactive Voice Response (IVR) system are authorized and processed accurately, completely, and timely.

Control Activity		Tests Performed By Service Auditor	Results of Testing
5-5	Activity entered and verified in ARS prior to the cut-off time is submitted for trading that day. Transactions entered in ARS after the cut-off time are automatically pended by the system until the next day's processing.	**Observation:** Observed Ascensus personnel enter activity into ARS prior to the cut-off time to determine that the transaction entered was automatically submitted for trading that day.	No exceptions noted.
		Observation: Observed Ascensus personnel enter activity into ARS after the cut-off time to determine that the transaction entered after the cut-off time were automatically pended by the system until the next day's processing.	No exceptions noted.
5-6	The IVR requires participants to access the participant website under the following conditions: • The participant attempts to perform a contribution. • Participant attempts to perform a deferral. • The participant attempts to submit a loan request.	**Observation:** Observed a user access the IVR system to determine that the participant was prompted to access the participant website when the following transactions were attempted: • The participant attempted to perform a contribution. • Participant attempted to perform a deferral. • The participant attempted to submit a loan request.	No exceptions noted.

Control Objective 6

Controls provide reasonable assurance that participant transactions received via the internet are authorized and processed accurately, completely, and timely.

Control Activity		Tests Performed By Service Auditor	Results of Testing
6-1	Participants must enter a web user ID and password to access their account and perform transactions via the internet.	**Observation:** Observed a user access the participant website using a test account to determine that participants were required to enter a valid user ID and password in order to access their account and perform transactions via the internet.	No exceptions noted.
6-2	Plan Administrators must enter the client number and PIN to access participant accounts and perform transactions via the internet.	**Inspection:** Inspected the multi-factor authentication (MFA) configurations for the employer site to determine that the site required the plan administrators to enter a 6-digit pin to access participant accounts and perform transactions via the internet.	No exceptions noted.
		Observation: Observed a plan administrator successfully access a participant account via a test account with a username and password to determine that Plan Administrators must enter a valid client number to access participant accounts and perform transactions via the internet.	No exceptions noted.

Control Objective 6

Controls provide reasonable assurance that participant transactions received via the internet are authorized and processed accurately, completely, and timely.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
6-3	Participant sites are programmed to prevent transactions under the following conditions: • Pending unposted transactions exist. • Transaction data entered by participant does not correspond to the allowable amounts set within the system. • Individual funds are restricted. • The participant attempts more fund-to-fund transfers than allowed by the plan. • The participant attempts to submit a loan that would exceed the maximum number of loans allowed by the plan. • The participant attempts to submit a loan that would exceed the maximum dollar amount available for loan to the participant. • The participant attempts to submit a termination payout request but has not been put into a terminated status with a valid termination date by the plan sponsor.	**Observation:** Observed the attempted processing of invalid transactions to determine that the participant sites were programmed to prevent transactions under the following conditions: • Pending unposted transactions existed. • Transaction data entered by participant did not correspond to the allowable amounts set within the system. • Individual funds were restricted. • The participant attempted more fund-to-fund transfers than allowed by the plan. • The participant attempted to submit a loan that exceeded the maximum number of loans allowed by the plan. • The participant attempted to submit a loan that exceeded the maximum dollar amount available for loan to the participant. • The participant attempted to submit a termination payout request but had not been put into a terminated status with a valid termination date by the plan sponsor.	No exceptions noted.

Control Objective 6

Controls provide reasonable assurance that participant transactions received via the internet are authorized and processed accurately, completely, and timely.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
6-4	The sponsor site is programmed to restrict plan-level transactions under the following conditions: • Plan is not valid for changes to plan-level rules. • Contributions are specified as going to a frozen or closed fund.	**Observation:** Observed the attempted processing of an invalid transaction to determine that the sponsor site was programmed to restrict plan-level transactions under the following conditions: • Plan was not valid for changes to plan-level rules. • Contributions were specified as going to a frozen or closed fund.	No exceptions noted.
6-5	The sponsor site is programmed to restrict participant transactions under the following conditions: • Pending unposted transactions exist. • Transaction data entered by sponsor does not correspond to the allowable amounts set within the system. • Individual funds are restricted. • The sponsor attempts to submit a loan that would exceed the maximum number of loans allowed by the plan. • The sponsor attempts to submit a loan that would exceed the maximum dollar amount allowed by the plan. • The sponsor attempts to submit a termination payout request but has not put the participant into a terminated status with a valid termination date.	**Observation:** Observed the attempted processing of invalid transactions to determine that the sponsor site was programmed to restrict participant transactions under the following conditions: • Pending unposted transactions existed. • Transaction data entered by sponsor did not correspond to the allowable amounts set within the system. • Individual funds were restricted. • The sponsor attempted to submit a loan that exceeded the maximum number of loans allowed by the plan. • The sponsor attempted to submit a loan that exceeded the maximum dollar amount allowed by the plan. • The sponsor attempted to submit a termination payout request but had not put the participant into a terminated status with a valid termination date.	No exceptions noted.

Control Objective 6

Controls provide reasonable assurance that participant transactions received via the internet are authorized and processed accurately, completely, and timely.

Control Activity		Tests Performed By Service Auditor	Results of Testing
6-6	Activity entered and verified in ARS prior to the cut-off time is submitted for trading that day. Transactions entered in ARS after the cut-off time are automatically pended by the system until the next day's processing.	**Observation:** Observed Ascensus personnel enter activity into ARS prior to the cut-off time to determine that the transaction entered was automatically submitted for trading that day.	No exceptions noted.
		Observation: Observed Ascensus personnel enter activity into ARS after the cut-off time to determine that the transaction entered after the cut-off time were automatically pended by the system until the next day's processing.	No exceptions noted.
6-7	The participant site is configured to restrict users from selecting a deferral amount outside of plan-defined limits and, upon submission, automatically displays a confirmation of the elected deferral percentage and the effective date of the change.	**Observation:** Observed a user attempt to elect a deferral amount outside of plan-defined limits and an amount within plan-defined limits to determine that the participant site was configured to restrict users from selecting a deferral amount outside of plan-defined limits and, upon submission, automatically displayed a confirmation of the elected deferral percentage and the effective date of the change.	No exceptions noted.

Control Objective 7

Controls provide reasonable assurance that contributions and loan repayments are credited to participant accounts on the Ascensus Recordkeeping System completely, accurately, and timely.

Control Activity		Tests Performed By Service Auditor	Results of Testing
7-1	Contribution activity that does not process successfully to ARS during the nightly batch cycle (e.g., due to missing investment elections in ARS, inadequate funding, missing participant data) is identified daily on the Ascensus Contribution Engine (ACE) Report, which is monitored throughout the day. Items remain on the ACE Report until resolved (e.g., sufficient funds are received). Aged items are escalated to management.	**Inspection:** Inspected the Ascensus Contribution Engine (ACE) error report related to a selected sample of days and errors to determine that, for each selected day, contribution activity that did not process successfully to ARS during the nightly batch cycle was identified daily on the report and was monitored throughout the day. Further, for a sample of days and errors, determined that selected items remained on the ACE report until resolved and any aged items were escalated to management.	No exceptions noted.
7-2	ARS holds each participant's investment elections. Contributions and loan payments are allocated into investment funds based on selected investment elections. Loan repayments are automatically allocated between the principal and interest based on the interest rate and life of the loan per the amortization schedule. ARS updates participant accounts during the daily posting cycles in accordance with current investment elections.	**Observation:** Observed the processing of a sampled loan repayment transaction to determine that ARS held each participants investment elections, contributions and loan payments were allocated into investment funds based on selected investment elections, loan repayments were automatically allocated between the principal and interest based on the interest rate and life of the loan per the amortization schedule, and ARS updated participant accounts during the daily posting cycles in accordance with investment elections.	No exceptions noted.
7-3	Variances between a plan's contribution amount at the trust company and the cash position in ARS are identified on daily variance reports, which are monitored throughout the day by Ascensus associates until corrected.	**Inspection:** Inspected the Daily Variance Report related to a sample of days and variances to determine that for each selected day, variances between a plan's contribution amount at the trust company and the cash position in ARS were identified on daily variance reports, which were monitored throughout the day by Ascensus associates until corrected.	No exceptions noted.

Control Objective 7

Controls provide reasonable assurance that contributions and loan repayments are credited to participant accounts on the Ascensus Recordkeeping System completely, accurately, and timely.

Control Activity		Tests Performed By Service Auditor	Results of Testing
7-4	Vesting amounts are automatically calculated based on defined vesting schedules. Unvested employer contributions are automatically credited to a forfeiture account.	**Observation:** Observed Ascensus personnel select a plan and subsequent participant and review the participant's vested contributions to determine that unvested employer contributions were automatically credited to a forfeiture account.	No exceptions noted.
		Reperformance: Reperformed the vesting amount calculation for a sampled user to determine that vesting amounts were automatically calculated based on the defined vesting schedules.	No exceptions noted.

Control Objective 8

Controls provide reasonable assurance that distributions are authorized, processed accurately, completely, and on a timely basis in compliance with plan provisions.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
8-1	Participant distribution transactions require the plan sponsor's and/or participant's authorizing signature(s) (depending upon plan specifications) prior to processing in ARS. Distribution transactions that do not contain the required signatures are returned to the plan sponsor or participant for correction as necessary.	**Inspection:** Inspected the participant distribution request form for a sample of participant distribution transactions to determine that, for each selected sample, the plan sponsor's and/or participant's authorizing signatures were required prior to processing in ARS and for any distribution transactions that did not contain the required signatures were returned to the plan sponsor or participant for correction as necessary.	No exceptions noted.
8-2	Distribution transactions are rejected by automated system edits, based on plan provisions, which identify missing data and potential duplicate submissions. Transactions that are rejected after passing initial system edits are identified in the ARS error report and monitored daily to avoid aging and to determine if items need to be escalated to management.	**Observation:** Observed the attempted processing of invalid transactions to determine that distribution transactions were rejected by automated system edits which identified missing data and potential duplicate submissions.	No exceptions noted.
		Inspection: Inspected the ARS Error Report related to a sample of business days to determine that, for each selected business day, transactions that were rejected after passing initial system edits were identified in the ARS error report and monitored daily to avoid aging and to determine if items needed to be escalated to management.	No exceptions noted.
8-3	On a daily basis, Distribution Services associates review distribution transactions, including discrepancies between ARS and the trust company. The discrepancies are noted on the Mismatch Fund Report and researched and resolved.	**Inspection:** Inspected the Mismatch Fund Report related to a sample of discrepancies and days to determine that for each selected day, Distribution Services associates reviewed distribution transactions, including discrepancies between ARS and the trust company. Further, determined that each selected discrepancy noted on the Mismatch Fund Report was researched and resolved.	No exceptions noted.

Control Objective 8

Controls provide reasonable assurance that distributions are authorized, processed accurately, completely, and on a timely basis in compliance with plan provisions.

Control Activity		Tests Performed By Service Auditor	Results of Testing
8-4	The BPM tool is utilized to monitor the business area queues to help ensure work is processed timely.	**Observation:** Observed the work queues in BPM to determine that the BPM tool was utilized to monitor the queues to help ensure work was processed in a timely manner.	No exceptions noted.
8-5	Ascensus associates use a BPM tool to scan and index transaction requests, which are then electronically sent to the relevant business unit. Images are stored in the BPM tool for retrieval. Operations associates review financial transactions entered in ARS for accuracy, completeness and timeliness after data entry and evidence their review by signing off on the corresponding transmittal form or via electronic sign-off in the BPM system. Any issues identified are resolved prior to sign-off.	**Observation:** Observed the Associate of the Service Support Group scan and index a selected incoming transaction request to the BPM system to determine that the request was scanned and electronically delivered to the appropriate business unit for processing and document images were stored in the BPM tool for retrieval.	No exceptions noted.
		Inspection: Inspected the corresponding transmittal form and/or electronic sign-off in the BPM system related to a sample of financial transactions entered in ARS to determine that operations associates reviewed and signed off on each selected financial transaction entered into ARS for accuracy, completeness, and timeliness after data entry and any issues were resolved prior to sign-off.	No exceptions noted.

Control Objective 9

Controls provide reasonable assurance that tax withholding is accurately calculated for distributions and payout transactions, and reflected accurately and completely in year-end tax reports.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
9-1	ARS automatically calculates the amount of tax withholding required for pre-tax distributions that are not loans or qualified rollovers based on IRS rules, and automatically creates a 1099R record in the system.	**Observation:** Observed the distribution process for pre-tax distributions that were not loans or qualified rollovers within ARS to determine that ARS automatically calculated the amount of tax withholding required and automatically created a 1099R record in the system.	No exceptions noted.
9-2	At the end of the calendar year, an edit report program is executed for end-of-year records. A report detailing alerts triggered by the edit report program is generated in spreadsheet format and reviewed by the Distribution Services department to verify that accurate tax information will be reported. Distribution Services associates resolve the issues and update ARS data as necessary.	**Inspection:** Inspected the edit report to determine that the edit report program was executed at the end of the calendar year for end-of-year records.	No exceptions noted.
		Inspection: Inspected the edit report to determine that a report detailing alerts triggered by the edit report program was generated in spreadsheet format and reviewed by the Distribution Services department to verify that accurate tax information was reported, and Distribution Services associates resolved the issues and updated ARS data as necessary.	No exceptions noted.
9-3	Prior to submitting the information to the IRS, Distribution Services associates review a sample of 1099R transactions and compare them to the end-of-year file to verify that transactions have been accurately captured. A QC spreadsheet is used to track the review of sample 1099R forms by Distribution Services associates.	**Inspection:** Inspected the QC spreadsheet to determine that, prior to submitting the information to the IRS, Distribution Services associates reviewed a sample of 1099R transactions and compared them to the end-of-year file to verify that transactions had been accurately captured.	No exceptions noted.

Control Objective 9 Controls provide reasonable assurance that tax withholding is accurately calculated for distributions and payout transactions, and reflected accurately and completely in year-end tax reports.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
9-4	The Distribution Services department reconciles distribution accounts with the trust company on an annual basis. Ascensus associates research and resolve any variances.	**Inspection:** Inspected the annual reconciliation report to determine that the Distribution Services department reconciled distribution accounts with the trust company on an annual basis, and Ascensus associates researched and resolved any variances.	No exceptions noted.

Control Objective 10

Controls provide reasonable assurance that account positions, pricing, dividends and investment income received from external sources (via the trading system) are loaded to the Ascensus Recordkeeping System completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
10-1	The Missing Price Report is automatically generated every night. The report identifies missing prices and rates and is reviewed to verify that prices have been obtained. Errors are researched and resolved.	**Inspection:** Inspected the Missing Price Report related to a sample of days to determine that the report was automatically generated each selected day and was reviewed to verify that missing prices and rates were obtained. Further, determined that for each selected date any errors were researched and resolved.	No exceptions noted.
		Inspection: Inspected the configuration of the Missing Price Report to determine that the Missing Price Report was automatically generated on a nightly basis.	No exceptions noted.
10-2	The ability to modify the pricing in ARS is limited to appropriate associates based on their job responsibilities.	**Inspection:** Inspected the system generated listing of users with the ability to modify the pricing in ARS and the corresponding job titles for all users on the listing to determine that the ability to modify the pricing in ARS was limited to appropriate associates who required the access to perform their job responsibilities.	No exceptions noted.
10-3	The Daily Variance Report is generated daily to help ensure that variances between ARS and the transfer agent or trust company are identified and assigned to an Ascensus associate for review and resolution.	**Inspection:** Inspected the Daily Variance Report for a selected sample of days to determine that, for each selected day, the report was generated to help ensure that variances between ARS and the transfer agent or trust company were identified and assigned to an Ascensus associate for review and resolution.	No exceptions noted.

Control Objective 10

Controls provide reasonable assurance that account positions, pricing, dividends and investment income received from external sources (via the trading system) are loaded to the Ascensus Recordkeeping System completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
10-4	ARS is programmed to allocate investment income to the individual participant accounts based on shares held by each participant on the dividend record date of the interest income period. ARS automatically posts the related shares to individual participant accounts on pay date.	**Observation:** Observed the allocation process for a selected participant account to determine that ARS allocated investment income to the individual participant accounts based on shares held by each participant on the dividend record date of the interest income period.	No exceptions noted.
		Observation: Observed a participant transaction to determine that ARS automatically posted the related shares to individual participant accounts on pay date.	No exceptions noted.

Control Objective 11

Controls provide reasonable assurance that rejected contribution, distribution and exchange transactions are identified, analyzed and corrected on a timely basis.

Control Activity		Tests Performed By Service Auditor	Results of Testing
11-1	Participant transactions are monitored throughout the trading day via automated messages within the trading system.	**Observation:** Observed the trading system and automated messages onscreen to determine participant transactions were monitored throughout the trading day via automated messages within the trading system.	No exceptions noted.
11-2	Trades that must be placed manually (outside the automated trading interface) are documented using Trade Logs and are QC'd by a Trade associate (other than the one that entered the trade) and a Trade Specialist.	**Inspection:** Inspected the manual Trade Logs for a sample of business days to determine that for each selected business day, trades that were placed manually were documented using a Trade Log and were QC'd by a Trade associate (other than the one that entered the trade) and a Trade Specialist.	No exceptions noted.
11-3	On a daily basis, trade requests that are not acted upon by the fund company are documented within Trade Reject Reports and are researched and resolved by Trade associates to help ensure that they are corrected and placed in a timely manner.	**Inspection:** Inspected the Trade Reject Reports related to a sample of business days to determine that for each selected business day, trade requests that were not acted upon by the fund company were documented within Trade Reject Reports and were researched and resolved by Trade associates to help ensure that they were corrected and placed within two business days.	No exceptions noted.

Control Objective 11

Controls provide reasonable assurance that rejected contribution, distribution and exchange transactions are identified, analyzed and corrected on a timely basis.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
11-4	Trade associates use Balance Review Reconciliation Summary screens within ARS to identify position differences between the trading system and the transfer agent. Comments are entered within the screens to document the status and monitor research and resolution of position differences. Balance Review Reports are used to summarize this information and are generated and reviewed on a daily basis by Trade associates.	**Observation:** Observed the Balance Review Reconciliation Summary screens within ARS to determine that Trade associates used the screens to identify position differences between the trading system and transfer agent, and comments were entered within the screens to document the status and monitor research and resolution of position differences.	No exceptions noted.
		Inspection: Inspected the Balance Review Reports for a sample of days to determine that, for each selected day, the Balance Review Reports were generated to summarize differences between the trading system and the transfer agent and results were reviewed by Trade associates.	No exceptions noted.
11-5	Variances between a plan's contribution amount at the trust company and the cash position in ARS are identified on daily variance reports, which are monitored throughout the day by Ascensus associates until corrected.	**Inspection:** Inspected the Daily Variance Report related to a sample of days and variances to determine that for each selected day, variances between a plan's contribution amount at the trust company and the cash position in ARS were identified on daily variance reports, which were monitored throughout the day by Ascensus associates until corrected.	No exceptions noted.
11-6	On a daily basis, Distribution Services associates review distribution transactions, including discrepancies between ARS and the trust company. The discrepancies are noted on the Mismatch Fund Report and researched and resolved.	**Inspection:** Inspected the Mismatch Fund Report related to a sample of discrepancies and days to determine that for each selected day, Distribution Services associates reviewed distribution transactions, including discrepancies between ARS and the trust company. Further, determined that each selected discrepancy noted on the Mismatch Fund Report was researched and resolved.	No exceptions noted.

Control Objective 11

Controls provide reasonable assurance that rejected contribution, distribution and exchange transactions are identified, analyzed and corrected on a timely basis.

Control Activity		Tests Performed By Service Auditor	Results of Testing
11-7	The Daily Variance Report is generated daily to help ensure that variances between ARS and the transfer agent or trust company are identified and assigned to an Ascensus associate for review and resolution.	**Inspection:** Inspected the Daily Variance Report for a selected sample of days to determine that, for each selected day, the report was generated to help ensure that variances between ARS and the transfer agent or trust company were identified and assigned to an Ascensus associate for review and resolution.	No exceptions noted.

Control Objective 12

Controls provide reasonable assurance that participant statements and plan sponsor administration reports are accurate, complete, and sent on a timely basis.

Control Activity		Tests Performed By Service Auditor	Results of Testing
12-1	Systematic data exceptions (e.g., unit balances are not in agreement with trust company or transfer agent data, incorrect fund profile) are in place to confirm the completeness and accuracy of the statement information. Systematic data exceptions cannot be processed for upload until they are remediated.	**Observation:** Observed a data exception for a sampled plan to determine that systematic data exceptions (e.g., unit balances are not in agreement with trust company or transfer agent data, incorrect fund profile) were in place to confirm the completeness and accuracy of the statement information and that exceptions could not be processed for upload until they were remediated.	No exceptions noted.
		Inspection: Inspected the listing of status checks to determine that systematic data exceptions were in place to confirm the completeness and accuracy of statement information.	No exceptions noted.
12-2	Access to override statement edits and force statement production is restricted to senior Plan Reconciliation and Plan Reconciliation leadership associates. All overrides must be approved by senior Plan Reconciliation associates or Plan Reconciliation leadership prior to forcing the production of statements.	**Inspection:** Inspected the listing of users with access to override statement edits and force statement production and the corresponding job titles for each user on the listing to determine that access was restricted to senior Plan Reconciliation associates and Plan Reconciliation leadership associates.	No exceptions noted.
		Inspection: Inspected the override forms and supporting documentation related to a sample of override statement edits to determine that for each selected override, was approved by senior Plan Reconciliation associates or Plan Reconciliation leadership prior to forcing the production of statements.	No exceptions noted.

Control Objective 12

Controls provide reasonable assurance that participant statements and plan sponsor administration reports are accurate, complete, and sent on a timely basis.

Control Activity		Tests Performed By Service Auditor	Results of Testing
12-3	Access to statement production programs is restricted to appropriate associates.	**Inspection:** Inspected the system generated listing of users with access to statement production programs and the corresponding job titles for each user on the listing to determine that access to statement production programs was restricted to appropriate associates based on job function.	No exceptions noted.
12-4	Associates print and review a representative sample of statements before generating a complete set of statements. This review is indicated on a QC checklist.	**Inspection:** Inspected the QC checklist related to a sample of plans and quarters to determine that for each selected plan and quarter, associates printed and reviewed a representative sample of statements before generating a complete set of statements.	No exceptions noted.
12-5	Ascensus associates use participant statement status reports generated from ARS to monitor the statement delivery process to help ensure that participant statements are delivered to a fulfillment house or provided via the web portal after each quarter end.	**Observation:** Observed the participant portal statement pages to determine that statements were provided to participants via the web portal.	No exceptions noted.
		Inspection: Inspected the participant statement status report for a sample of quarters to determine Ascensus associates used participant statement status reports generated from ARS to monitor the statement delivery process to help ensure that participant statements were delivered to a fulfillment house or provided via the web portal after each quarter end.	No exceptions noted.
12-6	Participant distribution, exchange and allocation change transactions are reported on a timely basis to plan sponsors via the MPCs.	**Inspection:** Inspected the plan confirmation related to a sample of plan sponsors and months to determine that, for each selected plan sponsor and month, the participant distribution, exchange and allocation change transactions were reported within five business days to plan sponsors via the MPCs.	No exceptions noted.

Control Objective 13

Controls provide reasonable assurance that plan year-end Annual Deferral Percentage ("ADP")/Annual Contribution Percentage ("ACP") test results are based on accurate and complete data.

Control Activity		Tests Performed By Service Auditor	Results of Testing
13-1	Associates on the Year-End Services team have the ability to update data tables in the ADP/ACP program with the current IRS limits.	**Inspection:** Inspected the system generated listing of users with access to update data tables in the ADP/ACP program with the current IRS limits and the corresponding job titles for each user on the listing to determine that the ability to update data tables in the ADP/ACP program within the current IRS limits was restricted to associates on the Year-End Services team.	No exceptions noted.
13-2	For plans that require ADP/ACP testing, the ADP/ACP program identifies inconsistencies with the participant-level testing data by running a series of validation routines to identify data that is missing or inaccurate, or that does not appear to be in good order. The detailed alerts, by participant, are listed within the plan status history notes with a link to the website for review by each client. An email is sent to the plan sponsor when the annual ADP/ACP test is produced and available for review on the plan sponsor website. Interim ADP/ACP testing can be run on the plan sponsor website at any time.	**Inspection:** Inspected the summary test results for a sample of participants with plans that required ADP/ACP testing to determine that the ADP/ACP program identified inconsistencies with the participant-level testing data to identify data that was missing or inaccurate, or that did not appear to be in good order. Furthermore, inspected the test summary results for a sample of participants with plans that required ADP/ACP testing to determine that the detailed alerts, by participant, were listed within the plan status history notes with a link to the website for review by each client.	No exceptions noted.
		Inspection: Inspected the emails sent for a sample of participants with plans that required ADP/ACP testing to determine that an email was sent to the plan sponsor when the annual ADP/ACP test was produced and available for review on the plan sponsor website.	No exceptions noted.
		Inspection: Inspected the plan sponsor website to determine that the interim ADP/ACP testing could be run on the plan sponsor website at any time.	No exceptions noted.

Control Objective 13 Controls provide reasonable assurance that plan year-end Annual Deferral Percentage ("ADP")/Annual Contribution Percentage ("ACP") test results are based on accurate and complete data.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
13-3	A daily testing summary report is automatically generated and is made available to the Year-End Services management team to review the completion of ADP/ACP year-end testing.	**Inspection:** Inspected the daily testing summary report for a sample of days to determine that, for each selected day, a daily testing summary report was automatically generated and was made available to the Year-End Services management team to review the completion of ADP/ACP year-end testing.	No exceptions noted.

Control Objective 14

Enrollment/Re-enrollment for Non-Qualified: Controls provide reasonable assurance that Plan Enrollment Kits and the online enrollment website screens are created in accordance with the provisions in the Plan Sponsor's contract and that the census file data (enrollments) is complete or that the pre-populated data (re-enrollments) used for the initial site population is complete.

Control Activity		Tests Performed By Service Auditor	Results of Testing
14-1	The Relationship Manager reviews enrollment requests to ensure that a Plan Enrollment Kit is created in accordance with client provisions.	**Inspection:** Inspected the enrollment checklist related to a sample of enrollments and re-enrollments to determine that each selected sample was reviewed by the relationship manager to ensure that a Plan Enrollment Kit was created in accordance with client provisions.	No exceptions noted.
14-2	For new clients with enrollments: A member of the Product Support Team compares the number of records provided in the census file to the enrollment system to confirm that the number of records provided match those loaded. Any discrepancies are researched and resolved.	**Inspection/Inquiry:** Inspected the Case Tracking logs and Enrollment Reports related to a sample of new client enrollments to determine that for each selected sample, a member of the Product Support Team compared the number of records provided in the census file to the enrollment system to confirm that the number of records provided match those loaded. Further, inspected the Case Tracking Logs and inquired of the Director of Operations to determine that no discrepancies were identified; however, if any discrepancies had been identified, each discrepancy would have been researched and resolved.	No exceptions noted.
14-3	A review and approval of the online enrollment test scripts is completed by the Implementation Project Manager or the Relationship Manager to verify that website screen errors are identified and corrected prior to activation and that the online enrollment website screens are created in accordance with client provisions.	**Inspection:** Inspected the Case Tracking logs related to a sample of enrollments and re-enrollments to determine that, for each selected sample, a review and approval of the online enrollment test scripts was completed by the Implementation Project Manager or the Relationship Manager to verify that website screen errors were identified and corrected prior to activation and that the online enrollment website screens were created in accordance with client provisions.	No exceptions noted.

Control Objective 14

Enrollment/Re-enrollment for Non-Qualified: Controls provide reasonable assurance that Plan Enrollment Kits and the online enrollment website screens are created in accordance with the provisions in the Plan Sponsor's contract and that the census file data (enrollments) is complete or that the pre-populated data (re-enrollments) used for the initial site population is complete.

Control Activity		Tests Performed By Service Auditor	Results of Testing
14-4	For re-enrollments: A review is completed by the Implementation Manager or Plan Administrator of the pre-populated data for re-enrollments to verify that all elections were carried forward from the prior period to help ensure the completeness of the re-enrollment data loaded into the enrollment system. Any discrepancies are researched and resolved.	**Inspection/Inquiry:** Inspected the Case Tracking logs related to a sample of plans with re-enrollments to determine that, for each selected plan, a review was completed by the Implementation Manager or Plan Administrator of the pre-populated data for re-enrollments to verify that all elections were carried forward from the prior period to help ensure the completeness of the re-enrollment data loaded into the enrollment system. Further, inspected the case tracking logs related to a sample of plans and inquired with Director, NQ Implementation & Product Support, to determine there were no noted discrepancies; however, if there were noted discrepancies those discrepancies would have been researched and resolved.	No exceptions noted.

Control Objective 15

Enrollment/Re-enrollment for Non-Qualified: Controls provide reasonable assurance that enrollment and re-enrollment information for participants is entered into the Transaction System accurately, completely, and prior to pre-defined payroll deadlines, if required by the client agreement.

Control Activity		Tests Performed By Service Auditor	Results of Testing
15-1	Client Services reconciles enrollment elections and participant data from enrollment results reports (deferral elections, account allocations, investment elections, and beneficiary information when applicable) generated from the online enrollment site to the enrollment specifications in the Client Agreement to verify that all data was captured and updated completely and accurately in the Transaction System.	**Inspection:** Inspected the Case Tracking logs related to a selected sample of enrollments and re-enrollments to determine that, for each selected sample, Client Services reconciled enrollment elections and participant data from enrollment results reports (deferral elections, account allocations, investment elections, and beneficiary information when applicable) generated from the online enrollment site to the enrollment specifications in the Client Agreement to verify that all data was captured and updated completely and accurately in the Transaction System.	No exceptions noted.
15-2	Once the enrollment information is uploaded to the Transaction System, an exception report is generated. The Plan Administrator reviews this report to verify that all enrollment information was uploaded completely and accurately. Any exceptions are researched and resolved.	**Inspection:** Inspected the Exception Report and the corresponding Case Tracking logs related to a sample of enrollments and re-enrollments to determine that, for each selected sample, the Plan Administrator reviewed the exception report to verify that all enrollment information was uploaded completely and accurately. Further, inspected the Exception Report and the corresponding Case Tracking logs and inquired of the Director of Operations to determine that no exceptions were identified; however, if any exceptions had been identified, each exception would have been researched and resolved.	No exceptions noted.

Control Objective 15

Enrollment/Re-enrollment for Non-Qualified: Controls provide reasonable assurance that enrollment and re-enrollment information for participants is entered into the Transaction System accurately, completely, and prior to pre-defined payroll deadlines, if required by the client agreement.

Control Activity		Tests Performed By Service Auditor	Results of Testing
15-3	The Plan Administrator reviews the Case Tracking System to help ensure that at the end of the enrollment period a Deferral Election Report is provided to the Plan Sponsor prior to their pre-defined payroll deadline, if required by the client agreement.	**Inspection:** Inspected the Case Tracking logs related to a sample of enrollments and re-enrollments to determine that, for each selected sample, the Plan Administrator reviewed the Case Tracking System to help ensure that at the end of the enrollment period, a Deferral Election Report was provided to the Plan Sponsor prior to their pre-defined payroll deadline, if required by the client agreement.	No exceptions noted.
15-4	Valid user IDs and passwords are required to access the network, in-scope applications, website and related databases.	**Observation:** Observed a user attempt to gain access to the website to determine that a valid user ID and password was required to access the website.	No exceptions noted.
		Observation: Observed a user attempt to gain access to Qualified and Non-Qualified Services applications and related databases to determine that valid user IDs and passwords were required to access the Qualified and Non-Qualified Services applications and related databases.	No exceptions noted.

Control Objective 16

Enrollment/Re-enrollment for Non-Qualified: New and Converted Plan Setup: Controls provide reasonable assurance that plans are set up in the Transaction System in accordance with the provisions detailed in the client's/Plan Sponsor's contract.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
16-1	A Plan Administration Manual is created as an addendum to the client contract to detail the plan information such as the last day of the plan year, plan type, effective date, anniversary date, investment types, account types, money types, distribution types, and vesting schedules. The Plan Administration Manual is signed by the client/sponsor indicating that they have reviewed and approved the plan setup prior to the go-live date.	**Inspection:** Inspected the Plan Administration Manual related to a sample of new and converted plans to determine that for each selected sample, the Plan Administration Manual was created as an addendum to the client contract to detail the plan information such as the last day of the plan year, plan type, effective date, anniversary date, investment types, account types, money types, distribution types, and vesting schedules.	No exceptions noted.
		Inspection: Inspected the Plan Administration Manual related to a sample of new and converted plans to determine that for each selected sample, the Plan Administration Manual was signed by the client/sponsor indicating that they reviewed and approved the plan setup prior to the go-live date.	No exceptions noted.
16-2	For converted plans, a plan and investment level reconciliation is performed to verify that the converted plan's liability records agree to the prior Recordkeeper's data. This reconciliation is provided to the Plan Sponsor for review and approval.	**Inspection:** Inspected the plan and investment level reconciliations related to a sample of converted plans to determine that, for each selected converted sample, a plan and investment level reconciliation was performed to verify that the converted plan's liability records agreed to the prior Recordkeeper's data and that the reconciliation was provided to the Plan Sponsor for review and approval.	No exceptions noted.

Control Objective 16

Enrollment/Re-enrollment for Non-Qualified: New and Converted Plan Setup: Controls provide reasonable assurance that plans are set up in the Transaction System in accordance with the provisions detailed in the client's/Plan Sponsor's contract.

Control Activity		Tests Performed By Service Auditor	Results of Testing
16-3	The Implementation Project Manager completes the Implementation and Conversion "Go Live" checklist verifying that the Plan Administration Manual agrees to its source documents including contract provisions and that the plan is set up within the Transaction System in accordance with contract provisions as detailed within the Plan Administration Manual.	**Inspection:** Inspected the Implementation and Conversion "Go Live" checklist related to a sample of new and converted plans to determine that, for each selected sample, the Implementation Project Manager completed the Implementation and Conversion "Go Live" checklist and verified that the Plan Administration Manual agreed to the source documents, including contract provisions, and that the plan was set up in the Transaction System in accordance with contract provisions as detailed within the Plan Administration Manual.	No exceptions noted.

Control Objective 17

Transaction Processing for Non-Qualified: Controls provide reasonable assurance that transactions (i.e., payroll, deferral, client/Plan Sponsor contribution information, scheduled and non-scheduled disbursement information, participant fund transfers, allocation charges, and rebalances) are processed completely and accurately in the Transaction System.

Control Activity		Tests Performed By Service Auditor	Results of Testing
17-1	The Operations Team performs a reconciliation of the payroll information received from the Plan Sponsor to the payroll information input into the Transaction System. Any identified discrepancies are communicated to the Plan Sponsor.	**Inspection:** Inspected the payroll control log related to a sample of payrolls determine that, for each selected sample, the Operations Team performed a reconciliation of the payroll information received from the Plan Sponsor to the payroll information input into the Transaction System and that any identified discrepancies were communicated to the Plan Sponsor.	No exceptions noted.
17-2	The Transaction System is programmed to process the information in the contributions file accurately based on selected investment elections, allocation percentages, and the funds' prices.	**Observation:** Observed a demo plan within the Transaction System to determine that the Transaction System was programmed to process the information in the contributions file accurately based on selected investment elections, allocation percentages, and the fund's prices.	No exceptions noted.
17-3	The Operations Team reviews the payroll batch process to help ensure that there are no event sequence errors in the batch process. Any identified event sequence errors are researched and resolved.	**Inspection/Inquiry:** Inspected the payroll processing logs related to a sample of payrolls to determine that, for each selected sample, the Operations team reviewed the payroll batch process to help ensure that there were no event sequence errors in the batch process. Further, inspected the payroll status report and inquired of the Director, NQ Operations, to determine that there were no identified event sequence errors for the selected payrolls; however, if there had been any event sequence errors, each error would have been researched and resolved.	No exceptions noted.

Control Objective 17

Transaction Processing for Non-Qualified: Controls provide reasonable assurance that transactions (i.e., payroll, deferral, client/Plan Sponsor contribution information, scheduled and non-scheduled disbursement information, participant fund transfers, allocation charges, and rebalances) are processed completely and accurately in the Transaction System.

Control Activity		Tests Performed By Service Auditor	Results of Testing
17-4	Client services maintains a payroll processing log to help ensure that payroll, deferral, and Plan Sponsor contribution information is received from the Plan Sponsor and is processed after receiving all the necessary data at the Company.	**Inspection:** Inspected the payroll processing logs related to a sample of payrolls to determine that, for each selected sample, client services maintained a payroll processing log to verify that payroll, deferral, and sponsor contribution information was received from the Plan Sponsor, and was processed after receiving all the necessary data from the Company.	No exceptions noted.
17-5	Upon notification of a participant's separation of service from the Plan Sponsor, the Plan Administrator or Client Service Manager processes the event triggered disbursements.	**Inspection:** Inspected the disbursement documentation related to a sample of terminated participants to determine that, for each selected sample, the Plan Administrator or Client Service Manager processed the event triggered disbursements upon notification of a participant's separation of service from the Plan Sponsor.	No exceptions noted.
17-6	Disbursement amounts (including any forfeited amounts) are processed in the Transaction System and are then sent to the Plan Sponsor or the paying agent.	**Inspection:** Inspected the disbursement reports and corresponding email communications related to a sample of scheduled disbursements to determine that, for each selected disbursement, the disbursement amount (including any forfeited amounts) was processed in the Transaction System and sent to the Plan Sponsor or the paying agent.	No exceptions noted.

Control Objective 17

Transaction Processing for Non-Qualified: Controls provide reasonable assurance that transactions (i.e., payroll, deferral, client/Plan Sponsor contribution information, scheduled and non-scheduled disbursement information, participant fund transfers, allocation charges, and rebalances) are processed completely and accurately in the Transaction System.

Control Activity		Tests Performed By Service Auditor	Results of Testing
17-7	The website edit controls require that future allocations, rebalances, and fund transfers entered by the participant must each total 100%. Entries not totaling 100% are rejected by the website.	**Observation:** Observed the attempting processing of a future allocation, a rebalance, and a fund transfer via the website (secure.ascensus.com) to determine that edit controls required future allocations, rebalances, and fund transfers to total 100% and entries not totaling 100% were rejected by the website.	No exceptions noted.

Control Objective 18

Wire Transfers for Non-Qualified: Controls provide reasonable assurance that wire transfers are processed accurately and completely, and initiated within two business days or as otherwise required by client agreement.

Control Activity		Tests Performed By Service Auditor	Results of Testing
18-1	Access to activate wire transfers is restricted to the Reconciliation Team associates and authorized approvers.	**Inspection:** Inspected the listing of users with access rights to activate wire transfers along with the active employee listing containing job titles to determine that access to activate wire transfers was restricted to the Reconciliation Team associates and authorized approvers.	No exceptions noted.
18-2	Wire transfers must be reviewed for accuracy and approved by a secondary individual prior to the wire transfer being initiated. After requests are received, wire transfers are initiated within two business days or as otherwise required by client agreement.	**Inspection:** Inspected the Wire Transfer Packet related to a sample of wire transfers to determine that each selected sample was reviewed for accuracy and approved by a secondary individual prior to the wire transfer being initiated.	No exceptions noted.
		Inspection: Inspected the Wire Transfer Packet related to a sample of wire transfers to determine that each selected sample was initiated within two business days or as otherwise required by client agreement after the request was received.	No exceptions noted.
18-3	A wire transfer confirmation is sent to the client detailing the total dollar amount transferred and the account to which it was applied.	**Inspection:** Inspected the Wire Transfer Packet related to a sample of wire transfers to determine that, for each selected sample, a wire transfer confirmation was sent to the client detailing the total dollar amount transferred and the account to which it was applied.	No exceptions noted.

Control Objective 18

Wire Transfers for Non-Qualified: Controls provide reasonable assurance that wire transfers are processed accurately and completely, and initiated within two business days or as otherwise required by client agreement.

Control Activity		Tests Performed By Service Auditor	Results of Testing
18-4	A premium invoice detailing the wire transfer information, including the Premium Roster detailing instructions for payment allocation, is reviewed for accuracy and approved by the Investment Analyst or designated approver and sent to the Insurance Carrier. Wire transfers for insurance premium payments are initiated within two business days from the date of the premium invoice.	**Inspection:** Inspected the Premium Wire Packets related to a sample of premium wire payments to determine that, for each selected sample, a premium invoice detailing the wire transfer information, including the Premium Roster detailing instructions for payment allocation, was reviewed for accuracy and approved by the Investment Analyst or designated approver and sent to the Insurance Carrier.	No exceptions noted.
		Inspection: Inspected the Premium Wire Packets related to a sample of premium wire payments to determine that, for each selected sample, wire transfers for insurance premium payments were initiated within two business days from the date of the premium invoice.	No exceptions noted.
18-5	For each wire payment related to a premium invoice, the Non-Qualified Asset & Liability Management group reconciles the data from the Insurance Carrier confirmation to the allocation instructions. Discrepancies are researched and resolved.	**Inspection:** Inspected the Premium Wire Packets related to a sample of premium wire payments to determine that for each selected sample, the Non-Qualified Asset & Liability Management group reconciled the data from the Insurance Carrier confirmation to the allocation instructions. Further, inspected corresponding review documentation and inquired of the Senior Investment Analyst to determine that no discrepancies were identified; however, if there were any discrepancies identified, each discrepancy would have been researched and resolved.	No exceptions noted.

Control Objective 19

Plan Rebalances for Non-Qualified: Controls provide reasonable assurance that plan rebalances are processed accurately and completely within the Transaction System and processed daily for Plan Sponsors requesting plan rebalances.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
19-1	The Asset & Liability Management team compares either the final fund allocation or the individual trade transactions from the trade confirmation to the original trade instructions to verify that all trades were performed and that the trades were performed accurately and completely within the Transaction System.	**Inspection:** Inspected the Rebalance Packets related to a sample of rebalances to determine that, for each selected rebalance, the Asset & Liability Management team compared either the final fund allocation or the individual trade transactions from the confirmation to the original trade instructions to verify that all trades were performed and that the trades were performed accurately and completely within the Transaction System.	No exceptions noted.
19-2	The Event Tracking system is monitored by the Non-Qualified Asset & Liability Management team to verify that trade confirmations are sent to the client for their review for accuracy and completeness as required. Required rebalances are flagged as completed once confirmations have been sent to the client.	**Inspection:** Inspected the Rebalancing Packets related to a sample of rebalances to determine that, for each selected rebalance, the Event Tracking system was monitored by the Non-Qualified Asset & Liability Management team to verify that trade confirmations were sent to the client for their review for accuracy and completeness as required.	No exceptions noted.
		Inspection: Inspected the Rebalancing Packets related to a sample of rebalances to determine that the selected rebalances were flagged as completed once confirmations were sent to the client.	No exceptions noted.

Control Objective 20 Investing/Pricing for Non-Qualified: Controls provide reasonable assurance that fund prices are processed accurately, completely, and on a daily basis within the Transaction System and BOSS.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
20-1	On a daily basis, the Processing Specialist resolves all errors on the daily transaction load log and reviews an exception report that details if a fund's price is valued at zero or if there is a major fluctuation in the fund's price in order to process requested participants' elections. An independent QC review is performed to help ensure that all errors were addressed and fund price updates were processed completely and accurately.	**Inspection:** Inspected the Morning Processing Checklist and related pricing information related to a sample of days to determine that, for each selected day, the Processing Specialist validated the previous nightly transaction load, resolved all errors on the daily transaction load log, and reviewed an exception report that detailed if a fund's price was valued at zero or if there was a major fluctuation in the fund's price in order to process requested participants' elections.	No exceptions noted.
		Inspection: Inspected the Morning Processing Checklist related to a sample of days to determine that, for each selected day, an independent QC review was performed to help ensure that all errors were addressed, and fund price updates were processed completely and accurately.	No exceptions noted.
20-2	The ability to update pricing is limited to Operations and Implementations personnel assigned access to the BOSS pricing module.	**Inspection:** Inspected the system generated listing of users with the ability to update pricing and the corresponding job titles for each user on the listing to determine that the ability to update pricing was limited to Operations and Implementations personnel assigned access to the BOSS pricing module.	No exceptions noted.
20-3	All retroactive price corrections are reviewed for accuracy by the Operations Supervisor, Director of NQ Operations, Manager of NQ Operations, or client prior to being executed within the Transaction System.	**Inspection:** Inspected the Non-Qualified Price Correction Cover Sheet related to a sample of retroactive price corrections to determine that each selected sample was reviewed for accuracy by the Operations Supervisor, Director of NQ Operations, Manager of NQ Operations, or client prior to being executed within the Transaction System.	No exceptions noted.

Control Objective 21 Custodial Activity for Non-Qualified: Controls provide reasonable assurance that participant trade instructions received after designated trading cut-off times are processed the following business day or trading day.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
21-1	The Transaction System is programmed to process and trade participant trade instructions received prior to 4:00 PM EST the same day. Participant requests received after 4:00 PM EST are processed and traded the following business or trading day.	**Observation:** Observed a transaction submitted prior to market close to determine that the Transaction System was programmed to process and trade participant trade instructions received prior to 4:00 PM EST the same day.	No exceptions noted.
		Observation: Observed a transaction submitted after market close to determine that participant requests received after 4:00 PM EST were processed and traded the following business or trading day.	No exceptions noted.

Control Objective 22

Participant/Plan Reporting for Non-Qualified: Controls provide reasonable assurance that the Corporate Reporting package is complete and accurate.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
22-1	At least quarterly, Accounting Services compares the Participant Account Activity Statement (PAAS) beginning balances to the ending balances of the prior month's PAAS to verify accuracy and reviews the reported gains and losses for reasonableness. Discrepancies are researched and resolved.	**Inspection:** Inspected the Reporting Packages related to a sample of plans and quarters to determine that, for each selected sample, Accounting Services compared the Participant Account Activity Statement (PAAS) beginning balances to the ending balances of the prior month's PAAS to verify accuracy and reviewed the reported gains and losses for reasonableness at least quarterly. Further, determined that any discrepancies were researched and resolved.	No exceptions noted.
22-2	At least quarterly, Accounting Services compares the Asset Value Report (AVR) from NASA to the mutual fund and Insurance Carrier reports to verify that composite totals and transaction information is accurate.	**Inspection:** Inspected the checklist within the Reporting Packages related to a sample of plans and quarters to determine that, for each selected sample, Accounting Services compared the Asset Value Report (AVR) from NASA to the mutual fund and Insurance Carrier reports to verify that composite totals and transaction information were accurate, at least quarterly.	No exceptions noted.
22-3	At least quarterly, Accounting Services compares the beginning balance of the AVR to the ending balances of the prior period's AVR and also reviews gains and losses for reasonableness based on the clients' rebalance protocol, funding status, timing of transactions, and other account factors. Discrepancies are researched and resolved.	**Inspection:** Inspected the Reporting Packages related to a sample of plans and quarters to determine that, for each selected sample, Accounting Services compared the beginning balance of the AVR to the ending balances of the prior period's AVR and also reviewed the gains and losses for reasonableness based on the clients' rebalance protocol, funding status, timing of transactions, and other account factors, at least quarterly. Further, determined that discrepancies were researched and resolved.	No exceptions noted.

Control Objective 22

Participant/Plan Reporting for Non-Qualified: Controls provide reasonable assurance that the Corporate Reporting package is complete and accurate.

Control Activity		Tests Performed By Service Auditor	Results of Testing
22-4	At least quarterly, a Journal Entry Report listing journal entries generated relative to the deferred compensation program for the period is reviewed by Accounting Services to help ensure that the journal entries reported to the client are accurate based on the AVR's and Benefit Liability Report's (BLR) ending balances.	**Inspection:** Inspected the Reporting Packages related to a sample of plans and quarters to determine that for each selected sample, a Journal Entry Report listing journal entries generated relative to the deferred compensation program for the period was reviewed by Accounting Services to help ensure that the journal entries reported to the client were accurate based on the AVR's and BLR's ending balances, at least quarterly.	No exceptions noted.
22-5	At least quarterly, a checklist is completed by the Accounting Services staff to verify that the requisite preparation steps have been followed and documented for the Corporate Reporting package (including AVR, BLR, PAAS, and Journal Entry reports, when applicable).	**Inspection:** Inspected the Reporting Packages related to a sample of plans and quarters to determine that for each selected sample. a checklist was completed by the Accounting Services staff to verify that the requisite preparation steps had been followed and documented for the Corporate Reporting package (including AVR, BLR, PAAS, and Journal Entry reports, when applicable), at least quarterly.	No exceptions noted.

Control Objective 23

Participant Statements for Non-Qualified: Controls provide reasonable assurance that quarterly participant statements are complete, accurate, and made available to participants by the last business day of the month following the close of each calendar quarter for existing plans, and by the agreed upon delivery date for new plans.

Control Activity		Tests Performed By Service Auditor	Results of Testing
23-1	On a quarterly basis, the Plan Administrator reviews and/or reconciles the following exception reports to identify discrepancies between the Transaction System, the printed statements, and the website: • The NQ Statement Balance/Units Audit Report, • The Header Audit Report, • The Deferral Audit Report, and • The Distribution Audit Report	**Inspection:** Inspected the statement audit checklist and supporting documentation related to a sample of active plans with statement services and quarters to determine that for each selected sample, the Plan Administrator reviewed and/or reconciled the exception reports defined in the Control Activity to identify discrepancies between the Transaction System, the printed statements, and the website on a quarterly basis.	No exceptions noted.
23-2	The Plan Administrator reviews quarterly participants' statements and selects a sample to verify the following for accuracy: • Financial transactions to source documents, • Distribution elections, and • Deferral elections.	**Inspection:** Inspected the statement audit checklist and supporting documentation related to a sample of active plans with statement services and quarters to determine that for each selected sample, the Plan Administrator reviewed quarterly participants' statements and selected a sample to verify accuracy of the financial transactions to source documents, distribution elections, and deferral elections.	No exceptions noted.

Control Objective 23

Participant Statements for Non-Qualified: Controls provide reasonable assurance that quarterly participant statements are complete, accurate, and made available to participants by the last business day of the month following the close of each calendar quarter for existing plans, and by the agreed upon delivery date for new plans.

Control Activity		Tests Performed By Service Auditor	Results of Testing
23-3	The Non-Qualified Client Services Team monitors Case Tracking to verify that Participant Statements are made available to participants either by quarterly mailings or online through Statement on Demand. Statements delivered via quarterly mailings or posting to the online archive are made available to the participants by the 30th business day of the month following the close of each calendar quarter.	**Observation:** Observed a user generate an account statement online to determine that Participant Statements were made available online through Statement on Demand.	No exceptions noted.
		Inspection: Inspected the Statement Tracking and Case Tracking Logs related to a sample of active clients and quarters to determine that for each selected sample, statements delivered via quarterly mailings or posting to the online archive were made available to the participants by the 30th business day of the month following the close of each calendar quarter.	No exceptions noted.

Control Objective 24

Non-Broad COLI Billings for Non-Qualified: Controls provide reasonable assurance that non-Broad Based COLI billings are accurate and communicated to the client and that billing transactions are complete.

Control Activity		Tests Performed By Service Auditor	Results of Testing
24-1	The COLI Insurance Services Administrator prepares the premium billing package. The package is reviewed by the Financial Analyst, Relationship Manager, Account Manager, Director of Financial Services, Senior Consultant, and/or Policy Administrator for reasonableness and consistency with the current Premium Payment Strategy prior to client distribution.	**Inspection:** Inspected the Premium Billing Packages related to a sample of non-broad based COLI billings to determine that, for each selected sample, the COLI Insurance Services Administrator prepared the premium billing package.	No exceptions noted.
		Inspection: Inspected the Premium Billing Packages related to a sample of non-broad based COLI billings to determine that, for each selected sample, the package was reviewed by the Financial Analyst, Relationship Manager, Account Manager, Director of Financial Services, Senior Consultant, and/or Policy Administrator for reasonableness and consistency with the current Premium Payment Strategy prior to client distribution.	No exceptions noted.
24-2	The Insurance Operations Team monitors the Work in Progress (WIP) database to determine that the COLI Insurance Services Administrator, Relationship Manager, or Account Manager transmits the Premium Billing Package to the client with the payment amount and wiring instructions.	**Inspection:** Inspected the Premium Billing Packages related to a sample of non-broad based COLI billings to determine that, for each selected sample, the Insurance Operations Team monitored the Work in Progress (WIP) database to determine that the COLI Insurance Services Administrator, Relationship Manager, or Account Manager transmitted the Premium Billing Package to the client with the payment amount and wiring instructions.	No exceptions noted.

Control Objective 24

Non-Broad COLI Billings for Non-Qualified: Controls provide reasonable assurance that non-Broad Based COLI billings are accurate and communicated to the client and that billing transactions are complete.

Control Activity		Tests Performed By Service Auditor	Results of Testing
24-3	Once the transaction date is confirmed, COLI Insurance Services verifies that the movement of money from one location to the other was performed accurately and obtains verification from the Insurance Carrier that the premium was applied in accordance with the roster that was provided to the Insurance Carrier.	**Inspection:** Inspected the Premium Billing Packages related to a sample of non-broad based COLI billings to determine that, for each selected sample, once the transaction date was confirmed, COLI Insurance Services verified that the movement of money from one location to the other was performed accurately.	No exceptions noted.
		Inspection: Inspected the Premium Billing Packages related to a sample of non-broad based COLI billings to determine that, for each selected sample, the COLI Insurance Services obtained verification from the Insurance Carrier that the premium was applied in accordance with the roster that was provided to the Insurance Carrier.	No exceptions noted.

Control Objective 25

Imputed Income Reporting for Non-Qualified: Controls provide reasonable assurance that Imputed Income Reports for Insurance Services' Benefit Plans are accurate and communicated to the client on or before the client deadline.

Control Activity		Tests Performed By Service Auditor	Results of Testing
25-1	For each report, the Insurance Services Benefit Plan Administrator, Account Manager, Financial Analyst, Relationship Manager, or Department Supervisor updates the prior year's rate table to the current year's rate table to verify the accuracy of all Insurance Carrier's one-year term insurance rate tables.	**Inspection:** Inspected the Imputed Income Tracking Sheets and supporting documentation related to a sample of imputed income reports to determine that for each selected sample, the Insurance Services Benefit Administrator, Account Manager, Financial Analyst, Relationship Manager, or Department Supervisor updated the prior year's rate table to the current year's rate table to verify the accuracy of the Insurance Carrier's one-year term insurance rate tables for each report.	No exceptions noted.
25-2	The Imputed Income Report is audited by the Account Manager, Financial Analyst, Relationship Manager, or Department Supervisor to verify that the name, the policy number (or policy ID), and the imputed income (or economic benefit) amount are reported accurately.	**Inspection:** Inspected the Imputed Income Tracking Sheets and supporting documentation related to a sample of imputed income reports to determine that for each selected sample, the Imputed Income Report was audited by the Account Manager, Financial Analyst, Relationship Manager, or Department Supervisor to verify that the name, the policy number (or policy ID), and the imputed income (or economic benefit) amount were reported accurately.	No exceptions noted.
25-3	The Plan Administrator, Account Manager, Financial Analyst, Relationship Manager, or Department Supervisor monitors the Imputed Income Tracking Sheet to verify that the Imputed Income Report is sent to the client on or before the client deadline.	**Inspection:** Inspected the Imputed Income Tracking Sheets and supporting documentation related to a sample of Imputed Income Reports to determine that for each selected sample, the Plan Administrator, Account Manager, Financial Analyst, Relationship Manager, or Department Supervisor monitored the Imputed Income Tracking Sheet to verify that the Imputed Income Report was sent to the client on or before the client deadline.	No exceptions noted.

Control Objective 26

Insurance Benefit Participant Statements for Non-Qualified: Controls provide reasonable assurance that participant Benefit Statements for Insurance Benefit Plans are accurate and made available to participants, as required by the Client Agreement.

Control Activity		Tests Performed By Service Auditor	Results of Testing
26-1	Insurance Benefit Participant Statements are reconciled to the source data from the Client and Currency Policy values and reviewed by a member of Insurance Services, Client Services or Financial Services for accuracy.	**Inspection:** Inspected the benefit statements, benefit statement quality control checklist, and supporting documentation related to a sample of benefit statement clients to determine that, for each selected sample, the insurance benefit participant statements were reconciled to the source data from the Client and Currency Policy values and reviewed by a member of Insurance Services, Client Services, or Financial Services for accuracy.	No exceptions noted.
26-2	The Benefit Plan Administrator monitors the Benefit Statement Tracking Document to verify that Insurance Benefit Participant Statements are mailed to the participants or the clients for distribution per the scheduled client due date as required by the Client Agreement.	**Inspection:** Inspected the benefit statement quality control checklist related to a sample of benefit statement clients to determine that, for each selected sample, the Benefit Plan Administrator monitored the Benefit Statement Tracking Document to verify that Benefit Statements were mailed to the participants or the clients for distribution per the scheduled client due date as required by the Client Agreement.	No exceptions noted.

Control Objective 27

COLI Best Practices Act for Non-Qualified: Controls provide reasonable assurance that the COLI Best Practices Act's (101j) packages are accurate and transmitted to the client within 45 business days of the client's tax year end.

Control Activity		Tests Performed By Service Auditor	Results of Testing
27-1	The COLI Insurance Services Administrator completes and monitors the tracking spreadsheet, evidencing preparation of the 101j Supporting Documentation and the 101j cover letters using policy values, census information, and data stored in LIAM for each client to determine that the tax year-end deadlines are met.	**Inspection:** Inspected the COLI Best Practices Reporting Quality Control Checklist and supporting documentation related to a sample of COLI clients to determine that, for each selected sample, the COLI Insurance Services Administrator completed and monitored the tracking spreadsheet evidencing preparation of the 101j Supporting Documentation and the 101j cover letters using policy values, census information, and data stored in LIAM for each client to determine that the tax year end deadlines were met.	No exceptions noted.
27-2	The COLI Best Practice Audit Checklist is completed by the COLI Insurance Services Administrator for every 101j reporting package to verify the following critical items are accurate: • Accurate policy numbers, • Accurate number insured individuals, • Multiple individual policy identification, and • Policy owner and tax information (TIN).	**Inspection:** Inspected the COLI Best Practices Reporting Quality Control Checklist related to a sample of COLI clients to determine that, for each selected sample, the COLI Best Practice Audit Checklist was completed by the COLI Insurance Services Administrator for every 101j reporting package to verify the items listed in the Control Activity were accurate.	No exceptions noted.

Control Objective 27

COLI Best Practices Act for Non-Qualified: Controls provide reasonable assurance that the COLI Best Practices Act's (101j) packages are accurate and transmitted to the client within 45 business days of the client's tax year end.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
27-3	The 101j reporting package and corresponding COLI Best Practice Audit Checklist are reviewed by the Account Manager, Relationship Manager, or a peer COLI Insurance Services Administrator to verify that all fields are complete and accurate.	**Inspection:** Inspected the 101j reporting packages and the corresponding COLI Best Practices Reporting Quality Control Checklist related to a sample of COLI clients to determine that, for each selected sample, the 101j reporting package and corresponding COLI Best Practice Audit Checklist was reviewed by the Account Manager, Relationship Manager, or a peer COLI Insurance Services Administrator to verify that all fields were complete and accurate.	No exceptions noted.
27-4	The Relationship Manager, Account Manager, or Plan Administrator verifies that 101j reporting packages are provided to the client no later than 45 business days after the client tax year.	**Inspection:** Inspected the COLI Best Practices Reporting Quality Control Checklist and supporting documentation related to a sample of COLI clients to determine that, for each selected sample, the Relationship Manager, Account Manager, or Plan Administrator verified that 101j reporting packages were provided to the client no later than 45 business days after the client tax year.	No exceptions noted.

Control Objective 28 Death Claim Processing for Non-Qualified: Controls provide reasonable assurance that death claims are processed accurately.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
28-1	On a monthly basis, the Claims Administrator collects and forwards the new insured's personal information (e.g., social security number) through a secured file to a third-party service provider in an effort to identify deceased individuals.	**Observation:** Observed the Lead Claims Administrator access the Client Import Data file transfer to determine that the Claims Administrator collected and forwarded the insured's personal information (e.g. social security number) through a secured file to a third-party service provider.	No exceptions noted.
		Inspection: Inspected the data transfer email confirmation related to a selected sample of months to determine that, for each selected month, the Claims Administrator collected and forwarded the insured's personal information (e.g., social security number) through a secured file to a third-party service provider in an effort to identify deceased individuals.	No exceptions noted.
28-2	On a weekly basis, the Claims Administrator reconciles the identified deceased insured individuals documented within the internal policy database to the file received by the sweep vendor.	**Inspection:** Inspected the weekly Sweep Search Result Report related to a sample of weeks to determine that, for each selected week, the Claims Administrator reconciled the identified deceased insured individuals documented within the internal policy database to the file received by the sweep vendor.	No exceptions noted.
28-3	Approved death claim carrier forms are obtained from the client and are submitted along with the required documentation to the carrier for payment.	**Inspection:** Inspected the death claim forms related to a selected sample of death claims to determine that for each selected sample, approved death claim forms were obtained from the client and were submitted along with the required documentation to the carrier for payment.	No exceptions noted.

Control Objective 28 Death Claim Processing for Non-Qualified: Controls provide reasonable assurance that death claims are processed accurately.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
28-4	A proceeds report is created based upon the payment made by the carrier. The report is reviewed to help ensure the accuracy of the payment received from the carrier.	**Inspection:** Inspected the distribution of proceeds report related to a sample of death claims to determine that for each selected sample, a proceeds report was created based upon the payment made by the carrier.	No exceptions noted.
		Inspection: Inspected the Distribution of Proceeds report and corresponding email communications related to a sample of death claims to determine that for each selected sample, the report was reviewed to help ensure the accuracy of payment received from carrier.	No exceptions noted.

Control Objective 29

Trust Non-Discretionary Services and Trust Fiduciary Services: Controls provide reasonable assurance that new accounts have been accepted in accordance with company policies and procedures and all required reviews, approvals and information have been obtained.

Control Activity		Tests Performed By Service Auditor	Results of Testing
29-1	New Plans are approved by the Sub-Committee.	**Inspection:** Inspected the meeting minutes related to a sample of new plans to determine that each selected new plan was approved by the Sub-Committee.	No exceptions noted.
29-2	A New Account Checklist is completed for new accounts to verify that the appropriate documents were validated for completeness and filed.	**Inspection:** Inspected New Account Checklists related to a sample of new accounts to determine that, for each selected sample, a New Account Checklist was completed to verify that the appropriate documents were validated for completeness and filed.	No exceptions noted.
29-3	For Trust Non-Discretionary Services: New Account Checklists are reviewed and approved by the Sub-Committee as evidenced by signoff on the checklist and/or documentation within the Sub-Committee meeting minutes. Any exceptions to the required documents and/or signoffs are approved by the Sub-Committee.	**Inspection:** Inspected the New Account Checklist related to a sample of new accounts to determine that for each selected sample, a New Account Checklist was reviewed and approved by the Sub-Committee as evidenced by the signoff on the checklist and/or documentation within the Sub-Committee meeting minutes. Further, inspected the New Account Checklist and inquired of the Trust Administration Manager to determine that there were no exceptions to the required documents and/or signoffs; however, if there were any exceptions to the required documents and/or signoffs, each would have been approved by the Sub-Committee.	No exceptions noted.

Control Objective 29

Trust Non-Discretionary Services and Trust Fiduciary Services: Controls provide reasonable assurance that new accounts have been accepted in accordance with company policies and procedures and all required reviews, approvals and information have been obtained.

Control Activity		Tests Performed By Service Auditor	Results of Testing
29-4	For Trust Special Fiduciary Services: Within 90 days of account setup in the Trust Application, a Relationship Manager ("RM") performs a post-acceptance review to assess whether or not the Company has the authority to maintain the account and the results of the review are provided to the Special Fiduciary Services Sub-Committee (SFC).	**Inspection:** Inspected the SFC Initial Post-Acceptance Review Form related to a sample of new accounts to determine that for each selected sample, within 90 days of account setup in the Trust Application, a Relationship Manager ("RM") performed a post-acceptance review to assess whether or not the Company had the authority to maintain the account.	No exceptions noted.
		Inspection: Inspected the Minutes of the Special Fiduciary Services Sub-Committee Meeting related to a sample of new accounts to determine that for each selected sample, the results of the review were provided to the Special Fiduciary Sub-Committee (SFC).	No exceptions noted.

Control Objective 30

Trust Non-Discretionary Services and Trust Special Fiduciary Services: Controls provide reasonable assurance that an annual review is completed to help ensure that accounts are administered in accordance with Newport policies and procedures.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
30-1	For Trust Non-Discretionary Services: Annually, the Company completes an oversight review to help ensure the following key due diligence activities were performed: • Review: Overdrafts, Elevated Action List/Customer Complaints, and Due Diligence Review Checklist, • AML: Training and Annual OFAC searches, • Review of relevant internal audit results, • Accounting and Statements (Posting of Trust Reports), • Financial Audits, • Annual review of Policy Manual, and • Vendor reviews (Including review of SOC Reports).	**Inspection:** Inspected the most recent Due Diligence Review Checklist and meeting minutes to determine that the Company completed an oversight review to help ensure key due diligence activities detailed in the Control Activity were performed.	No exceptions noted.
30-2	For Trust Non-Discretionary Services: On an annual basis, the Due-Diligence Review Checklist is reviewed by the Trust Sub-Committee and evidenced in the meeting minutes.	**Inspection:** Inspected the Sub-Committee meeting minutes to determine that the Due Diligence Review Checklist was reviewed by the Trust Sub-Committee annually and evidenced in the meeting minutes.	No exceptions noted.

Control Objective 30

Trust Non-Discretionary Services and Trust Special Fiduciary Services: Controls provide reasonable assurance that an annual review is completed to help ensure that accounts are administered in accordance with Newport policies and procedures.

Control Activity		Tests Performed By Service Auditor	Results of Testing
30-3	For Trust Special Fiduciary Services (Discretionary accounts): On an annual basis, the Special Fiduciary Services Sub-Committee performs a review of all individual accounts for which the Company has investment discretion to evaluate the suitability of the securities comprising the account.	**Inspection:** Inspected the Newport Trust Company Annual Review committee packages related to a sample of discretionary accounts to determine that each selected discretionary account was reviewed by the SFC on an annual basis to evaluate the suitability of the securities comprising the account.	No exceptions noted.

Control Objective 31

Trust Non-Discretionary Services and Trust Special Fiduciary Services: Controls provide reasonable assurance that closed accounts have been closed in accordance with company policies and procedures and that all actions necessary to close the account have been executed completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
31-1	Newport Trust Company (NTC) performs a review of all closing documents utilizing a checklist to help ensure all actions have been taken to ensure the proper closing of the account.	**Inspection:** For Non-Discretionary Services: Inspected the Account Closing Checklist related to a sample of terminated accounts to determine that for a selected sample NTC performed a review of all closing documents utilizing a checklist to help ensure all actions were taken to ensure the proper closing of the account.	No exceptions noted.
		Inspection: For Trust Special Fiduciary Services: Inspected the Account Closing Checklist, written notification, account summary report, and/or Account Deconversion/Termination notice related to a sample of terminated accounts to determine that for a selected sample NTC performed a review of all closing documents utilizing a checklist to help ensure all actions were taken to ensure the proper closing of the account.	No exceptions noted.
31-2	For Trust Non-Discretionary Services: A review of the checklist by a responsible party is performed to help ensure that the supporting documentation is on file and authorized by the Plan Sponsor, if applicable.	**Inspection:** Inspected the Account Closing checklist related to a sample of terminated accounts to determine that for each selected sample, a review of the checklist by a responsible party was performed to help ensure that the supporting documentation was on file and authorized by the Plan Sponsor, if applicable.	No exceptions noted.

Control Objective 31

Trust Non-Discretionary Services and Trust Special Fiduciary Services: Controls provide reasonable assurance that closed accounts have been closed in accordance with company policies and procedures and that all actions necessary to close the account have been executed completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
31-3	For Trust Special Fiduciary Services: A review of the checklist by a responsible party is performed to help ensure that the supporting documentation is on file and authorized by the Plan Sponsor, if applicable.	**Inspection:** Inspected the Account Closing Checklist related to a sample of terminated and transfer to successor accounts to determine that, for each selected sample, a review of the checklist by a responsible party was performed to help ensure that the supporting documentation was on file and authorized by the Plan Sponsor, if applicable.	No exceptions noted.

Control Objective 32

Trust Special Fiduciary Services: Controls provide reasonable assurance that account activity has been properly authorized, is in accordance with policies and procedures, and has been processed completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
32-1	Relationship Managers and Administrators verify that requests for new securities are submitted by authorized plan sponsor representatives.	**Inspection:** Inspected the submission requests related to a sample of requests for new securities to determine that, for each selected sample, RMs and Administrators verified that requests were submitted by authorized Plan Sponsor representatives.	No exceptions noted.
32-2	After funds and the associated Plan Sponsor instructions are received, an Administrator or Relationship Managers processes the transaction in the Trust Application, and a Relationship Manager other than the processor reviews and approves the transaction in the Trust Application to help ensure the completeness and accuracy of processing.	**Inspection:** Inspected the posting detail within the Trust Application and notice of receipt of funds related to a sample of wires and checks to determine that for each selected sample, after funds and the associated Plan Sponsor instructions were received, an Administrator or Relationship Manager processed the transaction in the Trust Application.	No exceptions noted.
		Inspection: Inspected the Receipt Detail within the Trust Application related to a sample of wires and checks to determine that for each selected sample, a Relationship Manager other than the processor reviewed and approved the transaction in the Trust Application to help ensure the completeness and accuracy of processing.	No exceptions noted.
32-3	Access to process cash receipts in the Trust Application is restricted to appropriate Relationship Managers and Administrators.	**Inspection:** Inspected the active employee listing containing job titles and the listing of users with access to process cash receipts in the Trust Application to determine that access to process cash receipts in the Trust Application was restricted to appropriate Relationship Managers and Administrators.	No exceptions noted.

Control Objective 32

Trust Special Fiduciary Services: Controls provide reasonable assurance that account activity has been properly authorized, is in accordance with policies and procedures, and has been processed completely and accurately.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
32-4	For lump sum payments: Prior to processing a distribution request, the Relationship Managers review the Plan Sponsor distribution requests to verify that the request is authorized.	**Inspection:** Inspected the Plan Sponsor authorization related to a sample of lump sum payments to determine that, for each selected sample, the Relationship Managers reviewed the Plan Sponsor distribution requests to verify that the request was authorized prior to processing.	No exceptions noted.
32-5	For lump sum payments: An Administrator and/or a Relationship Manager reviews the distribution request for completeness and confirms that adequate funds are available prior to approving and processing the payment in the Trust Application.	**Inspection:** Inspected the review of adequate funds documentation and distribution details related to a sample of distribution requests for lump sum payments to determine that, for each selected sample, an Administrator and/or RM reviewed the distribution request for completeness and confirmed that adequate funds were available prior to approving and processing the payment in the Trust Application.	No exceptions noted.
32-6	For periodic payments: Prior to month end (for monthly and quarterly payments), SFS reviews the Participant Payment Report which details scheduled transaction payments entered to help ensure that funds will be available the day payments are due to post.	**Inspection:** Inspected the Participant Payment Report, Cash and Account Summary, and related email communications related to a sample of accounts with period payments to determine that, for each selected sample, SFS reviewed the Participant Payment Report, prior to month end, which detailed scheduled transaction payments entered to help ensure that funds would be available the day payments were due to post.	No exceptions noted.

Control Objective 32

Trust Special Fiduciary Services: Controls provide reasonable assurance that account activity has been properly authorized, is in accordance with policies and procedures, and has been processed completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
32-7	Access to set up outgoing wire transfers in the Trust Application is limited to Administrators and Relationship Managers. Wire transfers must be reviewed for accuracy and approved by a secondary individual prior to disbursement.	**Observation:** Observed the Relationship Manager submit and attempt to approve a wire transfer within the Trust Application to determine that wire transfers were required to be reviewed for accuracy and approved by a secondary Relationship Manager prior to disbursement.	No exceptions noted.
		Inspection: Inspected the wire transfer details related to a sample of wire transfers to determine that each selected wire transfer was reviewed for accuracy and approved by a secondary individual prior to disbursement.	No exceptions noted.
		Inspection: Inspected the listing of users with access to set up outgoing wire transfers in the Trust Application and the corresponding job titles for each user on the listing to determine that access to set up outgoing wire transfers in the Trust Application was limited to Administrators and Relationship Managers.	No exceptions noted.
32-8	For Plan Sponsor requested stock distributions, Relationship Managers and/or Administrators verify that the request was submitted by authorized plan sponsor representatives. Authorized requests are submitted to the third-party processor for processing. The Relationship Manager and/or Administrator reviews the Trust Application for posting by the third-party processor.	**Inspection:** Inspected the submission request, Trust Application and corresponding review documentation related to a sample of Plan Sponsor stock distributions to determine that, for each selected stock distribution, the Relationship Manager and/or Administrator verified the request was submitted by authorized Plan Sponsor representatives, authorized requests were submitted to the third-party processor for processing, and the RM and/or Administrator reviewed the Trust Application for posting by the third-party processor.	No exceptions noted.

Control Objective 32

Trust Special Fiduciary Services: Controls provide reasonable assurance that account activity has been properly authorized, is in accordance with policies and procedures, and has been processed completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
32-9	For directed accounts: Before processing trades requested by the plan sponsor, the Relationship Manager verifies that the request is properly authorized.	**Inspection:** Inspected the client-directed trade instructions, the authorized signatures, and the instructions input into the Trade Application related to sample of directed account trades to determine that, for each selected sample, the Relationship Manager verified that the request was properly authorized before processing the trade requested by the Plan Sponsor.	No exceptions noted.
32-10	For discretionary accounts: The financial analyst authorizes the trade request prior to the Administrator or the Relationship Manager entering the transaction into the Trust Application.	**Inspection:** Inspected the e-mail communications and trade summary related to a sample of discretionary account trades to determine that for each selected sample, the Administrator or Relationship Manager verified that the request was properly authorized prior to entering the transaction into the Trust Application before processing trades.	No exceptions noted.
32-11	For discretionary and directed accounts: The Relationship Managers or Administrator review the trade instructions entered into the Trust Application for accuracy.	**Inspection:** Inspected the trade instructions related to a sample of discretionary and directed account trades to determine that the RM or Administrator reviewed the trade instructions entered into the Trust Application for accuracy for each selected trade.	No exceptions noted.

Control Objective 32

Trust Special Fiduciary Services: Controls provide reasonable assurance that account activity has been properly authorized, is in accordance with policies and procedures, and has been processed completely and accurately.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
32-12	For outside managed accounts: On a daily basis, the Operations Manager or designee performs an online review of DTC affirmed trades that are not pending in the Trust Application. Any DTC affirmed trades that are not pending in the Trust Application are researched and resolved.	**Inspection:** Inspected the Deplink Worksheet related to a selected sample of days to determine that for each selected day, the Operations Manager or designee performed an online review of DTC affirmed trades that were not pending in the Trust Application. Further, inspected corresponding remediation documentation to determine that any DTC affirmed trades that were not pending in the Trust Application were researched and resolved.	No exceptions noted.

Control Objective 33

Trust Special Fiduciary Services: Controls provide reasonable assurance that account asset records are reconciled daily in accordance with company policies and procedures and any discrepancies are resolved completely and accurately.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
33-1	On a daily basis, Administrators or Relationship Managers review the Daily Nightwork Batch Reports to monitor the previous day's activity. Any discrepancies are researched and resolved.	**Inspection:** Inspected the email confirmation related to a sample of days to determine that, for each selected day, Administrators or Relationship Managers reviewed the Daily Nightwork Batch Reports to monitor the previous day's activity. Further, inspected the email confirmation and inquired of the Senior Vice President of Operations, to determine that no discrepancies were identified during the selected days; however, if any discrepancies had been identified, each discrepancy would have been researched and resolved.	No exceptions noted.
33-2	For discretionary accounts: On an annual basis, the Un-invested Cash Report and Sweep Fund Balance report, which list un-invested cash broken out by discretionary accounts versus directed accounts and Custodian invested sweep fund balances, are submitted to the Special Fiduciary Services Sub-Committee ("SFC") for review.	**Inspection:** Inspected the most recent Un-invested Cash Report and Sweep Fund Balance report and corresponding SFC Meeting Minutes to determine that on an annual basis, the Un-invested Cash Report and Sweep Fund Balance report, which listed un-invested cash broken out by discretionary accounts versus directed accounts and Custodian invested sweep fund balances, were submitted to the Special Fiduciary Services Sub-Committee ("SFC") for review.	No exceptions noted.
33-3	The Company reconciles the new security setup to the Trust application against the instruction from the Plan Sponsor to help ensure complete and accurate processing by the third-party processor. Any discrepancies are researched and resolved.	**Inspection:** Inspected the new security setup reconciliation documentation related to a sample of new securities to determine that, for each selected sample, the Company reconciled the new security setup to the Trust Application against the instruction from the Plan Sponsor to help ensure complete and accurate processing by the third-party processor. Further, determined that any discrepancies were researched and resolved.	No exceptions noted.

Control Objective 33

Trust Special Fiduciary Services: Controls provide reasonable assurance that account asset records are reconciled daily in accordance with company policies and procedures and any discrepancies are resolved completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
33-4	On a daily basis, a Middle Office team member performs a reconciliation between the Trust Application and the Demand Deposit account ("DDA") to help ensure that all cash transactions are processed completely and accurately. Any differences are investigated and resolved.	**Inspection:** Inspected the reconciliation documentation related to a sample of days to determine that, for each selected day, a Middle Office team member performed a reconciliation between the Trust Application and the DDA to help ensure that all cash transactions were processed completely and accurately. Further, determined that any differences were investigated and resolved.	No exceptions noted.
33-5	On a monthly basis, the Middle Office team members review the Asset/Position Report and the Mutual Fund Reconciliation Report which provide an explanation of position breaks between the Trust Application and the custodian. Any unresolved position breaks are followed up on by the Middle Office team.	**Inspection/Inquiry:** Inspected the e-mail correspondence related to a selected sample of months to determine that, for each selected month, the Middle Office team members reviewed the Asset/Position Report and the Mutual Fund Reconciliation Report which provided an explanation of position breaks between the Trust Application and the custodian. Further, inspected the email correspondence and inquired of the Senior Vice President of Operations to determine that no unresolved position breaks were identified; however, if any unresolved position breaks had been identified, each unresolved position break would have been followed up on by the Middle Office team.	No exceptions noted.

Control Objective 34

Trust Special Fiduciary Services: For those accounts for which the company maintains valuation responsibility, controls provide reasonable assurance that assets are valued in accordance with company policies and procedures and records are reconciled completely and accurately.

Control Activity		Tests Performed By Service Auditor	Results of Testing
34-1	The Company's management and Special Fiduciary Services Sub-Committee ("SFC") review the final valuations provided by the independent Financial Advisors for privately held stock. Any issues or concerns are raised to the Trust Committee.	**Inspection:** Inspected the meeting minutes, related email communications, and valuation reports related to a sample of privately held stock to determine that for each selected sample, the Company's management and Special Fiduciary Sub-Committee ("SFC") reviewed the final valuations provided by the independent Financial Advisors for privately held stock. Further, determined that any issues or concerns were raised to the Trust Committee.	No exceptions noted.
34-2	For securities that are not publicly traded (e.g., closely held equities, insurance contract, limited partnership), Relationship Manager and/or Administrators submit the reviewed prices to the third-party processor for processing.	**Inspection:** Inspected the committee meeting minutes and price submissions related to a sample non-publicly traded securities to determine that, for each selected security, an RM and/or Administrator submitted the reviewed prices to the third-party processor for processing.	No exceptions noted.
34-3	Relationship Managers and/or Administrators reconcile the pricing entries in the Trust Application to the updates provided by the pricing source to verify that pricing of non-publicly traded securities were entered accurately into the Trust Application.	**Inspection:** Inspected the price submissions and email communications related to a sample of non-publicly traded securities to determine that, for each selected sample, an RM and/or Administrator reconciled the pricing entries in the Trust Application to the updates provided by the pricing source to verify that the pricing of non-publicly traded securities were entered accurately into the Trust Application.	No exceptions noted.

Control Objective 35 Controls provide reasonable assurance that backup and restoration procedures are implemented to preserve the integrity of programs and data files.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
35-1	Backups to the in-scope applications and related databases are configured to be performed daily. The backup system is configured to alert Application Technology of any backup failures, and any repeated backup failures are investigated and resolved.	**Inspection:** Inspected the backup configurations related to the Non-Qualified and Qualified applications and related databases to determine that backups were configured to be performed daily and that Application Technology was notified of any backup failures.	No exceptions noted.
		Inspection: Inspected the backup reports and associated tickets for a sample of days to determine that any backup failures and repeated backup failures were investigated and resolved.	No exceptions noted.
35-2	Access to the backup tool is restricted to appropriate individuals based on job function.	**Inspection:** Inspected the listing of users with access to the backup tool and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function.	No exceptions noted.
35-3	On an annual basis, a business continuity and disaster recovery plan is documented and is tested, and any issues are documented and resolved.	**Inspection:** Inspected the Business Continuity and Disaster Recovery Plan to determine that Ascensus had established policies and procedures for business continuity and disaster recovery.	No exceptions noted.
		Inspection: Inspected the results for the annual BCP/DR test to determine that the plan was tested and any issues were documented and resolved.	No exceptions noted.

Control Objective 36

Controls provide reasonable assurance that logical access to programs and data is limited to properly authorized individuals.

Control Activity		Tests Performed By Service Auditor	Results of Testing
36-1	Requests to add and or modify access to the network, in-scope applications, and the related databases and infrastructure are approved by a manager prior to access being granted.	**Inspection:** Inspected the access request tickets for a sample of requests to grant or modify access to the network, in-scope applications, related databases and infrastructure to determine that each selected access request was approved by a manager prior to access being granted.	No exceptions noted.
36-2	Valid user IDs and passwords are required to access the network, in-scope applications, website and related databases.	**Observation:** Observed a user attempt to gain access to the website to determine that a valid user ID and password was required to access the website.	No exceptions noted.
		Observation: Observed a user attempt to gain access to Qualified and Non-Qualified Services applications and related databases to determine that valid user IDs and passwords were required to access the Qualified and Non-Qualified Services applications and related databases.	No exceptions noted.
36-3	Password parameters for the website are configured to require, at minimum: • Passwords must be a minimum of 14 characters in length, • Password history of 3 is enforced, • Password complexity settings are enforced.	**Inspection:** Inspected password parameters to the website to determine that the passwords complied with the following standards: • Passwords must be a minimum of 14 characters in length, • Password history of 3 is enforced, • Password complexity settings are enforced.	No exceptions noted.

Control Objective 36

Controls provide reasonable assurance that logical access to programs and data is limited to properly authorized individuals.

Control Activity		Tests Performed By Service Auditor	Results of Testing
36-4	A tracking ticket to revoke access is automatically created when Human Resources approves an employee termination entered by a manager in the Workday application. Access is revoked within two business days following notification of termination from HR and is documented in a tracking ticket.	**Observation:** Observed the HR Director approve an employee termination within Workday to determine that a tracking ticket to revoke access was automatically created when Human Resources approved an employee termination entered by a manager in the Workday application.	No exceptions noted.
		Inspection: Inspected the termination ticket related to a sample of terminated employees to determine that each selected employees access was removed within two business days following notification of termination from HR and was documented in a tracking ticket.	No exceptions noted.
36-5	Administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers is restricted to appropriate individuals based on job function.	**Inspection:** Inspected the list of users with administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers and the corresponding job titles for all users on the listing to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.
36-6	Administrative access to the website, in-scope applications, and related databases is restricted to appropriate individuals based on job function.	**Inspection:** Inspected the listing of users with administrative access to the Qualified and Non-Qualified production applications and related databases and the corresponding job titles to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.
		Inspection: Inspected the listing of users with administrative access to the website and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function.	No exceptions noted.

Control Objective 36 Controls provide reasonable assurance that logical access to programs and data is limited to properly authorized individuals.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
36-7	On a periodic basis, Ascensus performs a review of access to the network, in-scope applications, and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.	**Inspection:** Inspected the access review documentation related to the network, in-scope applications, and related databases to determine that Ascensus performed a review of access to the network, in-scope applications, and related databases at least annually to help ensure that user access was appropriate.	No exceptions noted.
		Inspection: Inspected the Access Removal Tickets related to a sample of changes identified during the review of access to the network, in-scope applications, and related databases to determine that each selected user's access was removed as requested.	No exceptions noted.
36-8	Ascensus management performs annual reviews of workstation configurations in order to verify that RRD personnel cannot print, save or download data to local workstations or servers.	**Inspection:** Inspected the results of the annual review of offshore workstations to determine that Ascensus management verified that RRD personnel could not print, save or download data to local workstations or servers.	No exceptions noted.
36-9	Non-management offshore associates (below the level of Assistant Team Manager - Level 5, except for Level 4 associates designated as temporary Shift Leads) are restricted from printing hard copy data from ARS. This restriction is enforced through Citrix configurations controlled by Ascensus.	**Inspection:** Inspected the Citrix configurations pertaining to offshore network to determine that non-management offshore associates (below the level of Assistant Team Manager - Level 5, except for Level 4 associates designated as temporary Shift Leads) were restricted from printing hard copy data from ARS and that this restriction was enforced through Citrix configurations controlled by Ascensus.	No exceptions noted.

Control Objective 36

Controls provide reasonable assurance that logical access to programs and data is limited to properly authorized individuals.

Control Activity		Tests Performed By Service Auditor	Results of Testing
36-10	Password parameters for the in-scope applications are configured to require, at minimum: • Length of 8 characters • Complexity requirements	**Inspection:** Inspected password parameters for the Qualified and Non-Qualified applications to determine that passwords were configured to have a minimum length of 8 characters and complexity required.	No exceptions noted.
36-11	Password parameters for the network, operating systems, and databases related to the in-scope applications are configured to require, at minimum: • Length of 6 characters • Complexity requirements	**Inspection:** Inspected password parameters for the Qualified and Non-Qualified network, operating systems, and databases to determine that passwords were configured to have a minimum length of 6 characters and complexity required.	No exceptions noted.

Control Objective 37

Controls provide reasonable assurance that changes to existing applications are authorized, tested, approved, implemented by authorized personnel and documented.

Control Activity		Tests Performed By Service Auditor	Results of Testing
37-1	Ascensus utilizes development regions that are logically separate from the production environments.	**Inspection:** Inspected the separate development and production environments for the Qualified and Non-Qualified Applications to determine that the development regions that were logically separate from the production environments.	No exceptions noted.
		Inspection: Inspected the separate development and production environments related to the in-scope application's databases to determine that the development regions were logically separated from the production environments.	No exceptions noted.
37-2	Program changes are implemented using an automated deployment tool that requires review and approval by two separate users before the change is included in a build and pulled into the production environment. Access to promote changes into the production environment is restricted to appropriate individuals based on job function.	**Inspection:** Inspected the automated deployment tool configurations to determine that the tool required program changes to be reviewed and approved by two separate users before changes were included in a build and pulled into the production environment.	No exceptions noted.
		Inspection: Inspected the listing of users with access to promote changes into the production environment and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function.	No exceptions noted.
		Inspection: Inspected the deployment tool configurations related to the Non-Qualified and Qualified applications and related databases to determine that segregation of duties was systematically enforced via branch protection policies.	No exceptions noted.

Control Objective 37

Controls provide reasonable assurance that changes to existing applications are authorized, tested, approved, implemented by authorized personnel and documented.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the listing of individuals with access to promote changes into the production environment for the Non-Qualified, Qualified, RPS applications and related databases and the corresponding job titles for all users to determine that access to promote changes into the production environment was restricted to appropriate individuals based on job function.	No exceptions noted.
37-3	Changes to the in-scope applications and related databases, including emergency changes, are tested and approved by a member of management prior to promotion into the production environment.	**Inspection:** Inspected the change tickets for a sample of changes related to the in-scope applications and related databases to determine that each change was tested and approved by a member of management prior to promotion into the production environment.	No exceptions noted.
37-4	The Company maintains a release calendar that is available to business owners and IT management via the Company's internal website, to help ensure program changes are communicated to relevant stakeholders.	**Inspection:** Inspected the Company's release calendar on the Company's internal website to determine that the Company maintained a release calendar that was available to business owners and IT management via the Company's internal website to help ensure program changes were communicated to relevant stakeholders.	No exceptions noted.

Control Objective 38

Controls provide reasonable assurance that new and changes to existing system resources are authorized, tested and approved prior to implementation.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
38-1	On a monthly basis, updates and security patches to the existing server environments are documented using the ticketing system, and are authorized and implemented to development and Quality Assurance for testing prior to approval for implementation to production.	**Inspection:** Inspected the security patch change ticket for a sample of months to determine that, for each selected month, updates and security patches to the existing server environments were documented using the ticketing system, and were authorized and implemented to development and Quality Assurance for testing prior to approval for implementation to production.	No exceptions noted.
38-2	Build standards are documented to provide consistency when building and implementing servers supporting the in-scope applications. Servers are approved by a member of the Infrastructure team prior to use in production.	**Inspection:** Inspected the Virtual Machine process document to determine that build standards were documented to provide consistency when building and implementing servers supporting the in-scope applications.	No exceptions noted.
		Inspection: Inspected the change ticket and supporting documentation related to a sample of new servers to determine that servers were approved by a member of the Infrastructure team prior to use in production.	No exceptions noted.

Control Objective 39

Controls provide reasonable assurance that computer operations are monitored to ensure that problems are identified, documented and resolved on a timely basis.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
39-1	Critical jobs are run via a Batch Scheduler. Operators monitor daily processing using run sheets that list all of the expected jobs and verifies the jobs have completed successfully and resolve any issues that may arise.	**Inspection:** Inspected the run sheets related to a selected sample of days to determine that, for each selected day, Operators monitored daily processing using run sheets that listed all of the expected jobs and verified the jobs had completed successfully and resolved any issues.	No exceptions noted.
		Inspection: Inspected the Batch Scheduler used to run critical jobs and the alert configuration to notify the support team in the event of a job failure.	No exceptions noted.
39-2	Operations issues are documented in the daily shift turnover emails and follow-up actions are recorded. Open items that appear in the email are reviewed on a daily basis to help ensure that open production issues are addressed in a timely manner.	**Inspection:** Inspected the daily shift turnover emails related to a selected sample of days to determine that, for each selected day, operations issues were documented in the emails and follow-up actions were recorded. Further, determined that, for each selected day, opened items that appeared in the email were reviewed to help ensure that open production issues were addressed in a timely manner.	No exceptions noted.
39-3	Daily production meetings are held for IT and Operations management to discuss and monitor open action items, a report of recent events, and production status.	**Inspection:** Inspected the meeting minutes for sample of days to determine that, for each selected day, a production meeting was held to discuss open action items, report recent events, and discuss production status.	No exceptions noted.

Control Objective 39

Controls provide reasonable assurance that computer operations are monitored to ensure that problems are identified, documented and resolved on a timely basis.

Control Activity		Tests Performed By Service Auditor	Results of Testing
39-4	Ascensus maintains an Escalation and Incident Response Policy. Security incidents resulting in unauthorized access to, or misuse of, data are subjected to documented procedures, including notification of affected parties per operational agreements, contractual commitments, and statutory requirements.	**Inspection:** Inspected the Escalation and Incident Response Policy to determine that the policy outlined documented incident response procedures, specifically including the notification of affected parties per operational agreements, contractual commitments, and statutory requirements.	No exceptions noted.
		Inspection: Inspected the incident summary and timeline for a sample of security incidents to determine that each selected security incident resulting in unauthorized access to, or misuse of, data was subjected to documented procedures, including notification of affected parties per operational agreements, contractual commitments, and statutory requirements.	The Service Auditor noted that this portion of the control activity did not operate during the specified period, as there were no security incidents resulting in the unauthorized access to, or misuse of, data during the specified period. Therefore, this portion of the control activity could not be tested for operating effectiveness.
		Inspection/Inquiry: Inspected the Ascensus Information Security SharePoint data repository that stored the security incidents to determine that there were no security events resulting in the unauthorized access to, or misuse of, data during the specified period. Further, inquired of the Director of Risk Management to confirm that there were no security events resulting in the unauthorized access to, or misuse of, data during the specified period.	No exceptions noted.



© Grant Thornton LLP
All rights reserved.
A U.S. member firm of Grant Thornton International Ltd.

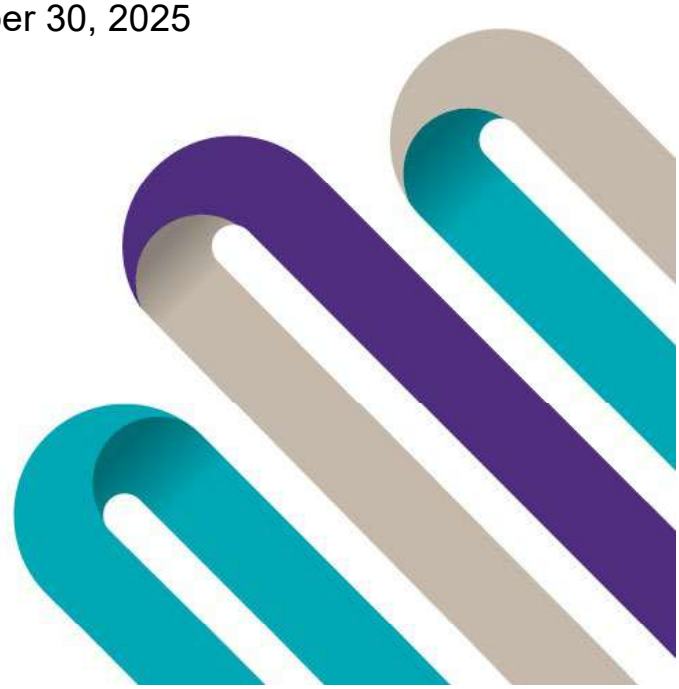
This report is confidential. Unauthorized use of this report in whole or in part is strictly prohibited.

Ascensus® and the Ascensus logo are registered trademarks of Ascensus, LLC.

ASCENSUS, LLC; ASCENSUS COLLEGE SAVINGS RECORDKEEPING SERVICES, LLC; ASCENSUS BROKER DEALER SERVICES, LLC; AND NEWPORT GROUP, INC.

Retirement and Government Savings Systems

System and Organization Controls (SOC) for Service Organizations Report
for the period of October 1, 2024 to September 30, 2025



Grant Thornton

Report of Independent Service Auditors issued by
Grant Thornton LLP

Contents

I. Report of Independent Service Auditors 1

II. Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. Assertion 5

III. Management of Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. Description of its System and Controls 7

A. Overview of Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. (collectively, the "Company" or "Ascensus") and Services Provided 7

B. Service Commitments and System Requirements 16

C. System Overview 18

D. Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication 22

E. Control Activities 26

F. Changes to the System During the Specified Period 28

G. Additional Information about Management's Description 28

H. Subservice Organizations 29

I. Complementary User Entity Controls 40

IV. Description of the Trust Services Categories, Criteria, Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results 44

A. Types and Descriptions of the Tests of Operating Effectiveness Provided by the Independent Service Auditor 44

B. Trust Services Categories, Criteria, Control Activities, Test of Controls, and Results 46

V. Other Information Provided by Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. 106

A. SPARK Data Security Control Objectives 106

GRANT THORNTON LLP
1415 Vantage Park Drive, Suite 500
Charlotte, NC 28203

D +1 704 632 3500
F +1 704 334 7701

I. Report of Independent Service Auditors

Board of Directors and Management
Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc.

Scope

We have examined Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. (the "Company" or "Ascensus") accompanying description of its Retirement and Government Savings Systems for processing transactions titled "Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc.'s Description of System and Controls" ("description") throughout the period October 1, 2024 to September 30, 2025 (the "specified period"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of the controls stated in the description throughout the specified period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information included in Section V of this report, "Other Information Provided by Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc.," is presented by management of the Company to provide additional information and is not a part of the Company's description. Information about the Company's SPARK data security control objectives has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria and, accordingly, we express no opinion on it.

The Company uses the subservice organizations listed in Subsection H within Section III of this report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the complementary

Grant Thornton LLP is a U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL and each of its member firms are separate legal entities and are not a worldwide partnership.

user entity controls assumed in the design of the Company's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service organization's responsibilities
The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled " Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. Assertion" ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Company is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service auditor's responsibilities
Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent limitations
The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria.
Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion
In our opinion, in all material respects,

a. The description presents Ascensus' Retirement and Government Savings Systems that were designed and implemented throughout the period October 1, 2024 to September 30, 2025, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Ascensus' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Ascensus' controls throughout the period October 1, 2024 to September 30, 2025.
c. The controls stated in the description operated effectively throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Ascensus' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Ascensus' controls operated effectively throughout the period October 1, 2024 to September 30, 2025.

Restricted use
This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Company, user entities of the Company's Retirement and Government Savings Systems during some or all of the specified period, business partners of the Company subject to risks arising from interactions with the Retirement and Government Savings Systems, practitioners providing services to such user entities and business partners, prospective user

entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization;
- how the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- internal control and its limitations;
- complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- user entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- the applicable trust services criteria; and
- the risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Grant Thornton LLP

Charlotte, North Carolina
December 5, 2025

The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.

II. Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. Assertion

We have prepared the accompanying description of Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. (collectively, the “Company” or “Ascensus”) Retirement and Government Savings Systems (the “System”) titled "Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc.’s Description of its System and Controls" throughout the period October 1, 2024 to September 30, 2025 (the “specified period”) (description) based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the System that may be useful when assessing the risks arising from interactions with Ascensus’ system, particularly information about system controls that Ascensus has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Company uses the subservice organizations listed in Subsection H within Section III of this report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ascensus, to achieve Ascensus’ service commitments and system requirements based on the applicable trust services criteria. The description presents Ascensus’ controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Ascensus’ controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with related controls at Ascensus, to achieve Ascensus’ service commitments and system requirements based on the applicable trust services criteria. The description presents Ascensus’ controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Ascensus’ controls.

We confirm, to the best of our knowledge and belief, that:

A. The description presents the System that was designed and implemented throughout the specified period, in accordance with the description criteria.

B. The controls stated in the description were suitably designed throughout the specified period to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the specified period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout the specified period.

C. The controls stated in the description operated effectively throughout the specified period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization controls and complementary user entity controls assumed in the design of the Company's controls operated effectively throughout the specified period.

III. Management of Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. Description of its System and Controls

A. Overview of Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. (collectively, the "Company" or "Ascensus") and Services Provided

Ascensus, LLC

Ascensus LLC, which includes Newport Group, Inc. ("Newport"), has more than 40 years of industry experience providing solutions that help institutional retirement plan providers and selected intermediaries service their plan sponsors and participant clients. The Company's core offerings include:

- Administration
- Recordkeeping
- Employee Retirement Income Security Act of 1974 (ERISA) consulting
- Compliance and sales support
- Trust and custody services
- Multilingual participant education programs, training, and documentation

The majority of business operations to which Ascensus provides services are subject to Federal laws and regulations pursuant to ERISA.

With offices throughout the United States, Ascensus is a provider of participant recordkeeping, plan administration, marketing support services and supplemental solutions for 401(k) plans. Further, Newport's breadth of services span industry-leading non-qualified retirement plan services, fiduciary consulting services, and corporate and bank-owned life insurance practices. Through relationships with various mutual fund companies, insurance companies, banks, credit unions, third-party administrators (TPAs) and broker-dealer firms, Ascensus currently services client across the United States.

Ascensus also provides individual retirement account (IRA), health savings account (HSA), and education savings account (ESA) administration, institutional trust and independent fiduciary services,

consulting services, training and reference materials, plan documents, document services, and commercial software and technology solutions for financial organizations across the United States.

Ascensus Retirement

The Retirement division's key client-facing groups are:

- **Qualified Plan Services Group** provides full-service recordkeeping and administration for retirement plans. A proprietary recordkeeping system at the core of this function allows Ascensus to process transactional activity, execute trades in support of that activity, and complete administrative functions such as regulatory compliance testing and client service support.

  The recordkeeping system is used exclusively by Ascensus associates to provide these services, as clients and business partners do not have access to it.

- **Retirement Products & Solutions** (RPS) provides outsourced and supplemental solutions in the areas of technology, product design, consulting, forms development, and educational products and services. The RPS team is also responsible for creating sales and marketing materials. The RPS team licenses internet-based software to financial organizations to facilitate the selection of appropriate forms as well as the completion of certain calculations and forms to help ensure compliance with Federal laws and regulations. The Ascensus-hosted RPS system allows external parties at user organizations to directly access the information and databases specific to their customer base and records. In addition, the system allows access to calculations and forms specific to each user organization's customer base through the user organizations' individual websites.

Newport, an Ascensus LLC Company

- **Non-Qualified Retirement Plan Services**: Newport is a leading provider of deferred compensation and executive benefit plan services. With over 35 years of market leadership, plan sponsors benefit from our plan consulting, independent funding strategies, communication and education and administration services.

  Newport's non-qualified deferred compensation programs provide key executives with information and education that will assist them in building wealth and a tax-efficient way to supplement their retirement. Newport provides all elements of managing a contemporary non-qualified plan—consulting, asset management, communication and education, and administration/recordkeeping.

- **Institutional Trustee and Independent Fiduciary Services**: Newport provides trust and custodial services through a wholly owned subsidiary chartered by the New Hampshire State Banking Department. Newport serves as discretionary and non-discretionary trustee and custodian for qualified and non-qualified employee benefit plans, including defined benefit pension plans, voluntary employee beneficiary association plans, employee stock ownership plans, 401(k) plans, profit sharing plans and rabbi trusts.

- **Insurance Services**: The suite of insurance services offered by Newport is provided by a responsive, experienced team of specialists who work closely with independent advisors and their clients to develop unbiased strategies and deliver programs that help meet each client's specific financial objectives.

  Our suite of corporate insurance services covers a range of options for different types of organizations and their unique needs. Whether you're looking for a solution for a bank, corporation, or insurance company, Newport can help you design and implement a plan that enhances your financial performance and rewards your key employees.

  BOLI

  Newport provides clients with a full range of services to help them optimize their BOLI program. Advisors and clients can rely on our BOLI team to provide expertise throughout the entire BOLI

lifecycle. This lifecycle includes product selection, pre-purchase due diligence, implementation, monthly reporting, regulatory compliance and death claim sweeps and processing.

COLI

Newport has a comprehensive platform designed to provide clients with a full range of services to help them optimize their COLI program. Advisors and clients can rely on our COLI team to provide expertise throughout the entire COLI lifecycle. This lifecycle includes product selection, pre-purchase due diligence, implementation, monthly reporting, regulatory compliance and death claim sweeps and processing.

ICOLI

Insurance company-owned life insurance is a form of life insurance where the insurance company is the purchaser, beneficiary and owner of policies on the lives of select executives. Newport offers a suite of services to evaluate the key elements necessary to structure, implement and maintain an efficient ICOLI program.

Ascensus Government Savings (AGS)

The Government Savings division of Ascensus comprises wholly owned subsidiaries:

- Ascensus Broker Dealer Services, LLC (ABD) – A U.S. Securities and Exchange commission (SEC) registered broker-dealer and a member of the Financial Industry Regulatory Authority (FINRA);
- Ascensus College Savings Recordkeeping Services, LLC (ACSR) – An SEC registered transfer agent; and
- Ascensus Investment Advisors, LLC (AIA) - An SEC-registered investment adviser.

Ascensus Broker Dealer Services, LLC and Ascensus College Savings Recordkeeping Services, LLC are the subsidiaries in scope for this report and are collectively referred to as “Ascensus Government Savings.”

Ascensus Broker Dealer Services, LLC

Ascensus Broker Dealer Services, LLC is a registered broker-dealer pursuant to Section 15 of the Securities Exchange Act of 1934. In addition, ABD has been a FINRA member, in good standing, since July 19, 1994. ABD is also a registered member of the Municipal Securities Rulemaking Board (MSRB) and the Securities Investor Protection Corporation (SIPC).

Ascensus College Savings Recordkeeping Services, LLC

Ascensus College Savings Recordkeeping Services, LLC (ACSR) is registered with the SEC as a transfer agent and provides program management, recordkeeping, and/or transfer agency services for certain 529, ABLE and State Facilitated Retirement Programs (SFRP) plans.

Scope of this Report

This report describes Ascensus’s system of controls for:

- **Ascensus, LLC: Qualified Plan Retirement Plan Services** – Applications considered for this report are the applications supporting recordkeeping processing for its recordkeeping services, including the Ascensus Recordkeeping System (ARS) and applications built to support specific functions within ARS, and Ascensus’s use of the HUB+ trading software provided through a subservice organization, Vertical Management Systems (VMS).
- **Ascensus, LLC: RPS** – Applications considered for this report include the Retirement Central®, IRA Service CenterTM, HSA Service CenterTM, Plan Adoption SystemTM, IRAdirect®, WebSite Administrator and Single Sign-On (SSO) applications as they apply to RPS operations.

- **Ascensus, LLC: Newport** – Applications considered for this report are the applications supporting Non-Qualified plan services, including Case Tracking System, NASA Application, Electronic Database Tool (EDB), and BOSS application. The applications supporting BOLI considered for this report include the BOLI application. In addition, Newport uses the following applications that are vendor hosted:
    - McCamish offered in a software-as-a-service (SaaS) model by third party subservice organization InfoSys (IMS) and is used to administer the daily transaction calculation and balance calculations for non-qualified retirement plan participants' accounts. Transactional information from the McCamish application is then transmitted to the EDB to provide participants\sponsors with non-qualified retirement plan account balances.
    - The Q+ Benefits Administration Application (Q+) is offered in a software-as-a-service (SaaS) model, by the third-party subservice organization, Andesa Services, Inc., and supports Newport's Benefit Administration processes for the BOLI team.
    - The Trust 3000 Application, the Retirement Benefit Plan System (RBPS), Customer Strata Station Browser (CSS), Cconnect, are supplied and supported by SEI, and support Newport's Institutional Trustee and Independent Fiduciary Trust Services.
- **Ascensus College Savings Recordkeeping Systems, LLC and Ascensus Broker Dealer Services, LLC: Ascensus Government Savings ("AGS")** – Applications considered for this report include applications supporting processing for its program management and recordkeeping services. Operations support for this system is provided through AGS locations.

This report has been prepared for the use of Ascensus's user entities. As this description is intended to focus on features of Ascensus's business operations relevant to customers who use the aforementioned services, it does not encompass all aspects of the services provided or procedures followed by Ascensus.

SOC 2 reports are conducted in accordance with AT-C Section 205 and utilize the AICPA audit guide titled *Reporting on Controls at a Service Organization Relative to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2).*

The scope of this report covers the **Security and Availability Criteria**.

For the purposes of this report, the following applications are considered in scope:

Application	Description	Hosted by
Qualified Plan Retirement Plan Services		
Ascensus Recordkeeping System (ARS)	The ARS is a proprietary in-house application that supports all aspects of the recordkeeping and administration of retirement plans. The ARS is used exclusively by Ascensus associates to complete their job functions.	Csquare Data Center
HUB+	HUB+ is a software package (hosted by the subservice organization VMS) that in-house Ascensus Trade team associates use to execute trading activity originating in the ARS. The system is used exclusively to execute trading functions, including reconciliation and settlement of trades, and is not used by external resources for any Ascensus functions.	Vertical Management Systems *

Application	Description	Hosted by
RPS		
Retirement Central	Retirement Central is an internet-based solution that integrates retirement-oriented content, education and planning tools with targeted planning activities related to retirement benefits. Retirement Central users have access to online informational content, planning tools, and forms such as online rollover IRA applications. Retirement Central also offers financial organizations customization options that allow them to incorporate their own unique content and activities, as well as their own links to other areas within their enterprise-wide websites.	Csquare Data Center
IRA Service Center™	IRA Service Center is an internet-based solution designed with interactive questionnaires. IRA Service Center assists financial organizations' customers and internal staff in opening and servicing Traditional and Roth IRAs and Coverdell ESAs. IRA Service Center also provides "Learn About" text to aid in the decision-making process.	Csquare Data Center
HSA Service Center™	HSA Service Center is an internet-based solution designed with interactive questionnaires for opening and completing HSA forms. HSA Service Center also provides planning and "what-if" tools, "Learn About" text, and broker/consumer-focused guidance.	Csquare Data Center
Plan Adoption System™	Plan Adoption System is an internet-based solution designed to make the plan design and setup process more accurate, professional and efficient. Plan Adoption System includes version history, compliance controls, and dynamic Summary Plan Description generation, as well as functions for creating user profiles and interfaces, which allows financial organizations to expand system access as their distribution and servicing models evolve.	Csquare Data Center

Application	Description	Hosted by
IRAdirect™	IRAdirect is the platform used to support Ascensus's IRA HSA and ESA Administration service offerings. IRAdirect is an internet-based solution that financial organizations access to generate transaction forms, transmit data to Ascensus and generate reports. Ascensus also utilizes IRAdirect to perform functions on behalf of the financial institutions, such as tax reporting, periodic payment processing, and death claim processing.	Csquare Data Center
WebSite Administrator	WebSite Administrator is a module embedded within the Retirement Central, IRA Service Center, HSA Service Center and Plan Adoption System applications. WebSite Administrator enables organizations to administer certain functions of their applications, including user administration, site configuration (including content), and access to collected data. WebSite Administrator is a password-protected feature designed for use by Ascensus and the user organizations (i.e., financial organizations) only; it is not for customers or potential customers of user organizations.	Csquare Data Center
Single Sign-On (SSO)	SSO is the central point of authentication and user management for the IRAdirect software. To gain access to IRAdirect, users must first authenticate through SSO using a username and password. Users can self-register for an SSO account, which requires them to select a unique username and establish a strong password. After completing the registration process, a Security Administrator, which is a role fulfilled by an approved individual for each client, is prompted to allow or deny the request for access. The Security Administrator also resets or removes access for existing user accounts.	Csquare Data Center
Non-Qualified Retirement Plans (Newport)		
Case Tracking System	The Case Tracking System is tool utilized to verify that enrollments and re-enrollments are completed prior to the pre-defined payroll deadline, if required by client agreement	Csquare Data Center

Application	Description	Hosted by
Electronic Database Tool (EDB)	Detailed plan and participant information maintained in the Transaction System is downloaded into the Electronic Database Tool (EDB) daily and participant information is available online through the Company's website	Csquare Data Center
BOSS	BOSS is a proprietary application that consists of various operational modules developed to complement business processes and reporting	Csquare Data Center
NASA	Newport Accounting Services Application (NASA) is a proprietary reporting application tied to the NQServices SQL Server database and is utilized to generate the monthly Corporate Reporting	Csquare Data Center
McCamish	McCamish is an application the Company uses to administer the daily transaction calculation and balance calculations for non-qualified retirement plan participants' accounts. Transactional information from the McCamish application is then transmitted to the EDB to provide participants\sponsors with non-qualified retirement plan account balances.	Infosys McCamish (IMS) *
BOLI (Newport)		
BOLI Application	The BOLI Application was developed by an internal development team to address internal processing, data access, and data loading needs coupled with the ability to report accurate and real-time data to clients in either a structured or an ad-hoc format.	Oracle *
Institutional Trustee and Independent Fiduciary Services (Newport)		
Trust 3000	This system is supplied and supported by SEI and is used as a trust accounting, processing, and custody system by Newport to maintain plan sponsor accounts, move cash and securities, produce plan sponsor statements, and make distribution payments.	SEI *
Retirement Benefit Plan System ("RBPS")	This system is supplied and supported by SEI and is designed to generate participant level distribution payments. RBPS transmits participant distribution data to the Trust 3000 application	SEI *

Application	Description	Hosted by
Customer Strata Station Browser ("CSS")	This application is supplied and supported by SEI and is a cash transaction processing system that provides real-time access to Trust 3000 account record information via an extranet connection. Newport users can view account information, add accounts, manage contacts, create notes and activities, and create, approve, and post transactions to Trust 3000 application records	SEI *
Cconnect	This application is supplied and supported by SEI and is designed to provide SEI customers and clients the ability to access certain account information via the internet. The product is designed to enable customers to retrieve real-time account holdings, market values, tax lot information, cash information, transactions, position details, asset summaries, available funds, balance summaries, and pending trades. Access is assigned by SEI and users have read-only access	SEI *
Ascensus Government Savings		
Unite	Unite provides 529 and ABLE plan account owners (or their authorized representatives) with complete online enrollment, and account maintenance functionality, including the ability to open initial and subsequent accounts, make contributions, request withdrawals, and register for statement e-delivery. All 529 and ABLE account transactions can be originated on Unite, either directly through the web applications supporting each 529 and ABLE plan, or through a CSR using a custom front-end application. Unite is built on an Oracle® database platform.	Csquare Data Center and Switch

Application	Description	Hosted by
ASTRO	ASTRO (Ascensus State Retirement Online) provides SFRP account owners with access to online enrollment, account maintenance functionality, and the ability to request financial transactions. This includes opening accounts, maintaining profile information, making one-time or recurring Electronic Bank Transfer (EBT) contributions, and requesting an exchange or a withdrawal. ASTRO also provides employers with access to online registration, employee maintenance functionality, and the ability to manage payroll contributions. This includes registering for the SFRP program, maintaining a company profile, creating, and maintaining pay schedules, adding administrators or payroll representatives, and submitting payroll contributions for processing. ASTRO is built on an Oracle database platform, with physical infrastructure residing in both the “BOS1” data center in the Watertown, MA co-location facility, (owned and managed by Csquare), and the “NAP10” data center in Las Vegas, NV co-location facility (owned and managed by Switch). ASTRO is a hybrid on-premises (back-end) and cloud (front-end presentation and web tier) platform leveraging Amazon Web Services (AWS) for cloud computing services.	Csquare Data Center and Switch
JETT	JETT is an internally developed recordkeeping subsystem that services ABLE and SFRP plans, direct-sold 529 plans and a subset of advisor-sold 529 plans. Batch processes are executed throughout the day to transfer trade activities for each participant account in Unite and ASTRO to JETT. Transactions are processed and posted to participant accounts every night in JETT and transmitted back to Unite and ASTRO. Trade details for fund managers and custodian banks are generated from Unite and ASTRO.	Csquare Data Center
Kofax Capture®	The Kofax Capture application (“Kofax”) is used to automate the capture of information from paper documents and forms received by mail, email, or fax. Data and images captured using Kofax are exported automatically into the applicable processing platform.	Csquare Data Center

Application	Description	Hosted by
Hyperscience	Hyperscience is optical character recognition (OCR) software that systematically transcribes and validates information from paper documents and forms received by mail, email, or fax.	Csquare Data Center
Documentum	Documentum combines document imaging and management technologies. Images, such as checks or forms captured by the Kofax optical scanners, are stored in the Documentum image repository. CSRs use Documentum to view and research account transactions initiated within the Kofax, Unite and ASTRO environments. Transactions are batched together in “vouchers” which enable detailed tracking and accelerated search and processing capabilities.	Csquare Data Center
Envision PowerAgent529	PowerAgent529 is a primary recordkeeping database that services a subset of 529 plans. Batch processes are executed each night to transfer trade information between Unite and PowerAgent529. Certain trades are recorded directly in PowerAgent529, and records of those trades are transmitted back to Unite. PowerAgent529 is supported by the vendor, Envision Financial Systems, Inc. (“Envision”).	Envision *
Frontier	Frontier automates Ascensus Government Savings’ account reconciliation processes for financial transactions. Using Frontier, AGS associates reconcile financial transactions (i.e., Demand Deposit Account balances) and portfolio units daily for each 529, ABLE and SFRP program.	Csquare Data Center
Amazon Web Services	AWS provides AGS with an on-demand cloud computing platform. The technology provides a virtual cluster of computers, available all the time, through the internet. AWS's virtual computers emulate most of the attributes of a real computer, including CPU for processing, memory, storage, operating systems, and networking.	Amazon Web Services *
** All data is housed in the United States at all times.*		

B. Service Commitments and System Requirements

Ascensus recognizes the primary need to secure the information with which they are entrusted as part of their service commitment to clients. Security commitments to user entities are documented and

communicated in established customer agreements. A comprehensive set of security policies that are regularly reviewed and updated that govern our corporate security program and include:

- Data Classification & Protection Policy
- Incident Response Policy and Procedures
- Administrative Access Control Policy
- Back-up Policy
- Security Monitoring Policy
- Privacy Policy
- IT Security Policies
- Password Policy
- Remote Access
- Acceptable Use

These policies are supported by programs, controls and tools that include, but are not limited to, the following:

- **Logical Access Controls** – Ascensus uses various mechanisms to restrict associates' access to operating systems, data files, databases and programs in production and development environments. Access to computer resources is based upon an individual's job duties. System access must be approved by the associate's manager before it is granted. Ascensus also employs identification and authentication methods, including unique user/client IDs and password restrictions, to restrict access for any external parties accessing the systems.
- **Firewall Protections** – Ascensus maintains both network and application firewalls to protect its systems from unauthorized network, application, and database activity. These firewalls are layered to provide perimeter security and are configured to allow only recognized IP addresses. Ascensus also deploys firewalls at the Web layer, application layers, and at all wide-area network termination points. Redundancy has been built into the architecture to provide for timely resumption of service in the event of a system failure.
- **Intrusion Detection and Prevention** – In addition to the firewall technology, Ascensus has implemented network Intrusion Detection Systems (IDS) that provide real-time detection mechanisms through the monitoring of inbound and outbound network traffic. The technology also acts as an Intrusion Prevention System (IPS) by blocking malicious activity.
- **Encryption** – Ascensus employs encryption technology to establish secure connections between browsers and web applications. Ascensus's policy prohibits clear-text transmissions of customer data over the internet. Ascensus uses encryption methods that include PGP, (S)FTP, TLS and VPN.
- **Data Loss Prevention** – Ascensus leverages a Data Loss Prevention (DLP) solution that provides monitoring of information flows into and out of the network. Unauthorized or unsecured transfers of sensitive information are blocked.
- **Physical Security Controls** – Access throughout Ascensus's facilities is restricted through electronic cardkeys. Access rights to Ascensus facilities are granted through requests to an access management system, with most associates working remotely and not granted daily access to facilities. These physical security controls are in place both at Ascensus facilities and at our vendor supplied data center hosting facilities.

- **Secure Destruction of Data and Equipment** – Ascensus maintains destruction methods to ensure hard-copy documents or electronic equipment that may contain client data is securely disposed of. Ascensus contracts with bonded vendors that dispose of hard-copy documents in locked shred bins. The vendor responsible for destroying hard drives and other electronic media is also bonded. All media are stored in a physically secured area to restrict access while awaiting disposal. Industry standard methods for data destruction are used, such as secure erasure or physical destruction.

- **Associate Training** – Ascensus requires all associates to complete security and privacy training at time of hire and at least annually thereafter, with attendance tracked by our corporate Risk Management team to ensure all associates complete the requirement. Additionally, associates are regularly reminded of their duty to protect confidential information through emails, internal publications and office postings.

On an annual basis, or more frequently as warranted, Ascensus evaluates the third parties with access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, the Company either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary

Ascensus has defined standard provisions required of key vendors and third parties, and formally included in our contracts with them, which includes the required security commitments in accordance with the organization's security policies. These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. A member of the Legal Department is responsible for reviewing and approving all new third-party contracts to help ensure that they include the applicable security practices and commitments.

Ascensus performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (*including environmental, regulatory, and technological changes, and threats related to fraud*), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (*including threats related to the use of vendors and other third parties providing goods and services*). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.

Direct access to the in-scope databases is restricted to appropriate personnel based on job function. Version control software is in place to manage current versions of source code related to the in-scope applications. The ability to modify source code is limited to appropriate users based on job function.

Encryption management software is in place and configured to enforce hard drive encryption on all Company connected to the Company's network. Endpoint management software is deployed to protect mobile devices (*such as laptops, smart phones, and tablets*) that serve as information assets.

C. System Overview

The following components of Ascensus's systems are used to provide the services within the scope of this report:

- Infrastructure – The physical structures, Information Technology (IT) and other hardware (e.g., facilities, computers, equipment, mobile devices, and telecommunications networks).

- Software – The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

- People – The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel and managers).

- Processes – The automated and manual procedures.

- Data – Transaction streams, files, databases, tables, and output used or processed by the systems.

These components are described in detail below.

1. Infrastructure

Corporate Data center operations are conducted from the Csquare Data Center in Watertown, MA. Ascensus's infrastructure within the data center used redundant links, redundant power supplies, redundant monitoring, multiple tier-one internet service providers and storage arrays. Csquare and other data center providers are responsible for providing n+1 redundancy (a form of resilience that ensures system availability in the event of component failure). This includes generators, uninterruptible power supplies (UPS) and dual power feeds.

Ascensus's corporate network is based on Windows Active Directory®. Virtual private networks (VPNs) using Internet Protocol Security (IPsec) and Transport Layer Security (TLS) encryption, Secure File Transfer Protocol (SFTP) servers, and other file and data encryption methodologies are utilized to transfer data internally and between third parties.

Firewalls separate Ascensus's internal network resources from three separate demilitarized zones. Switch access control lists (ACLs) restrict active ports to specific Virtual Local Area Networks (VLANs), adding additional defense. Fiber switches are zoned by worldwide names to restrict access to legitimate storage arrays and systems.

2. Software

Qualified plan retirement services have developed applications to conduct business functions related to retirement plan recordkeeping and administration, including ARS and supporting functions. RPS has developed proprietary applications to conduct everyday business functions, including the Retirement Central, IRA Service Center, HSA Service Center, Plan Adoption System, and IRAdirect applications.

Non-Qualified plan services have developed proprietary applications Case Tracking, EDB, BOSS, and NASA to conduct functions related to Non-Qualified Plan processing.

The BOLI team has developed its proprietary BOLI Application to support their business line.

Government Savings has developed proprietary applications, Unite, JETT and ASTRO, to conduct business functions related to 529, SFRP, and ABLE plan processing.

These functions, and others described in this report, also use third-party supplied and hosted applications to support their business lines.

The Development teams regularly update the applications to add functionality or adjust for any changes in the business or regulatory environment. Below are the major components of systems maintained by Ascensus and Newport.

The list below highlights the major software components that are utilized to provide **ARK**:

- Operating System: Windows Server 2019 CORE, AIX 7.2
- Web Server: IIS 10.0
- Database: Sybase - Adaptive Server Enterprise/16.0 SP04 PL06 HF1/EBF 31041, SQL Server 15.0.4360.2, 2019 CU25
- Application: ASP.NET MVC - .NET Framework 4.7.2
- Security: SentinelOne
- Management: SolarWinds® Network Monitoring/NewRelic APM/Infrastructure Monitoring, ELK Logging

The list below highlights the major software components that are utilized to provide the **RPS system**:

- Operating System: Windows Server 2016, Windows Server 2019, Linux RHEL 7
- Web Server: IIS 8.5, IIS 10.0, WebLogic 14c, Kubernetes
- Database: Oracle 19c, SQL Server 15.0.4360.2, 2019 CU25
- Application: ASP.NET MVC / .NET Framework 4.7, Java SE 11
- Security: SentinelOne
- Management: SolarWinds® Network Monitoring, NewRelic, ELK Logging

The list below highlights the major software components that are utilized in the **Government Savings system**:

- Operating System: LINUX, Windows Server 2012R2, Server 2016, Server 2019, Server 2022
- Web Server: Apache, Nginx, Umbraco CMS Cloud
- Database: Oracle 19c, Windows SQL Server
- Application: JBOSS, Tomcat, Struts, SpringBoot, NodeJS. Angular
- Security: SentinelOne
- Management: SolarWinds® Network Monitoring, Nagios

The list below highlights the major software components that are utilized in the **BOLI system**:

Production Application Server

- OS: Oracle Linux 8.10
- Web Server: Apache 2.4.37 2/20/25
- Form Software: ColdFusion Server 2023,0,12,330713
- Programming Language Software: 7.2.24
- Security: SentinelOne
- Management: SolarWinds® Network Monitoring, Nagios

Production Database Server

- OS: Oracle Linux 8.8
- Database Version: Oracle Database 19c Enterprise Edition 19.27.0.0.0
- Security: SentinelOne
- Management: SolarWinds® Network Monitoring, Nagios

Production Crystal Reports Server

- OS: Windows Server 2022 Standard 10.0.20348
- Crystal Reports Software: SAP BI Platform 4.3 Support Pack 3 Patch 6 14.3.3.4682

3. People

Ascensus's systems are supported by in-house development and IT teams that ensure system availability and accuracy. IT leadership works closely with other divisions to ensure that enhancements meet clients' needs and expectations.

IT comprises the following teams who are responsible for supporting the Retirement (Qualified, Non-Qualified plans and RPS), COLI/BOLI, Institutional Trust and Independent Fiduciary Services, and Government Savings systems:

- The Infrastructure team is responsible for the IT environment, e.g., systems, telephony, network and desktop.
- The Retirement Production Support team manages the daily processing, monitors and implements production code, and ensures that system changes are tested prior to implementation into production.

The following functions are fulfilled by the Development teams dedicated to their specific business group:

- Application Development teams are responsible for the development and delivery of modifications to existing applications or the creation of new applications in accordance with business requirements.
- IT Project Management teams document the business requirements for IT initiatives and manage the components needed to ensure a successful implementation of code.
- IT Quality Assurance teams perform comprehensive testing of system changes to ensure the systems are functioning as requested and the introduction of the code into production will not negatively impact current applications or performance.

Risk Management

Risk Management is responsible for monitoring and investigating realized and potential fraud, coordinating internal and external audit engagements, evaluating and assessing operational risk, and providing management with recommendations for remediating governance and control deficiencies as necessary. Risk Management also updates and maintains Ascensus's Disaster Recovery and Business Continuity Plan and coordinates the updates to key governing policies.

Procurement and Vendor Strategy

Procurement and Vendor Strategy is responsible for third-party vendor oversight. This includes evaluating the vendor to determine their risk-rating and if necessary, performing a security assessment and review of the vendor's SOC reports. Vendors are subjected to continuous monitoring and corrective actions are taken, if necessary.

Information Security

Information Security works with Information Technology to secure systems and network resources in order to protect the confidentiality of associates' and account owners' information. To support this objective, Information Security identifies risks to the security of information systems and mitigates those risks to levels that meet acceptable tolerances. Information Security also defines security requirements, establishes baselines, and measures compliance based on applicable laws, regulations, and best practices and increases associates' awareness of information security through training and communications. Information Security includes Business Information Security Officers (BISO's) assigned to each division and a 24x7x365 Security Operations Center that monitors the environment. The group reports to the Chief Information Security Officer (CISO), who in turn reports to the Corporate CIO.

The following groups provide support to Ascensus's business operations but are not in scope for this examination:

Legal

Legal maintains corporate governance filings and documentation, supervises litigation, maintains contracts and disclosure documents, and provides legal support, as necessary.

Compliance

Compliance monitors adherence to applicable federal securities laws, rules and regulations and applicable state securities laws relating to broker-dealers, investment advisors and transfer agents. This also includes federal and state laws, rules and regulations associated with (i) "qualified tuition plans" as authorized by Section 529 of the Internal Revenue Code (IRC): (ii) savings accounts under Section 529A of the IRC for individuals who meet the Social Security Administration's definition of disabled; and (iii) State-Facilitated Retirement Savings Plans for private sector workers.

In addition, Compliance monitors adherence to anti-money laundering requirements and associated implementing regulations (e.g., The Bank Secrecy Act and USA PATRIOT Act) in an effort to prevent and combat financial crimes, such as money laundering and terrorist financing. This includes Compliance activities to (i) maintain a customer identification program and due diligence program; and (ii) work with Risk Management in monitoring transactions for suspicious activity and the filing of Suspicious Activity Reports, as necessary, and records to safeguard the U.S. financial system.

4. Processes

Ascensus has developed policies and standard operating procedures to operate, maintain and secure the Retirement, COLI/BOLI, Institutional Trust and Fiduciary Services, and Government Savings systems, and to achieve the AICPA Trust Principles and Criteria for security. Procedures for the following key control topics have been defined and formally documented to support the systems:

- Logical Access
- Physical Security
- Monitoring of Computer Operations
- Change Management
- Disaster Recovery (DR) / Business Continuity

Procedures and controls are described in Section IV of this report.

5. Data

Data includes customer and transaction data and applications hosted in the Retirement, COLI/BOLI, Institutional Trust and Fiduciary Services, and Government Savings systems' infrastructure. Users, both internal and external, access the systems and data through a role-based user interface. User entities are restricted to their accounts and the data related to their accounts. Controls for securing and restricting access to customer data are described in Section IV of this report.

D. Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication

1. Control Environment

Ascensus Organization Structure

- Retirement Services
  - Client Service*
  - Retirement Operations
  - Retirement Administration*
  - Ascensus Trust**
  - Provident Trust Group**
  - FuturePlan**
  - Plan Services Sales*
  - ERISA Compliance*

  - Business Development*
  - Retirement Products & Solutions (RPS)
    - Total Benefit Communications, LLC (TBC)**
    - Wrangle**
- Newport
  - Non-Qualified plans
  - Bank Owned Life Insurance (BOLI), Company Owned Life Insurance (COLI), and Insurance Company Owned Life Insurance (ICOLI)
  - Newport Trust - Institutional Trustee and Independent Fiduciary Services (NDS & SFS)
- Information Technology
- Corporate
  - Legal, Risk, and Compliance (LRC)*
  - Human Resources (HR)
  - Corporate Finance*
  - Corporate Development and Mergers & Acquisitions (M&A)*
- Government Savings
  - 529, ABLE, and SFRP
- Strategic Business Support Services*

*Indicates groups that are not included in the scope of this report

**Indicates divisions that are not included in the scope of this report

Each division is led by a Vice President or Executive Vice President who reports to the President of Ascensus.

Organizational and Management Controls

A primary responsibility of management is the establishment of an appropriate control environment to help achieve specified business objectives.

Ascensus's organizational structure is designed to provide adequate segregation of duties, as well as clearly defined areas of functional responsibility over the processing areas. Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems. Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.

Human Resources Policies

Ascensus has established hiring policies and guidelines designed to assist managers in selecting appropriate applicants for available positions. Ascensus hiring policy requires the following: a minimum level of education and experience as fits the position, completion of relevant application forms, execution of confidentiality statements and successful completion of the background investigation, which includes criminal, financial, education, and employment verification, as well as professional references.

On an annual basis, performance reviews are performed to help ensure that each employee's skill set matches his/her job responsibilities. The process evaluates an associate's performance against their established goals, as well as their core competencies. The competency assessment ensures alignment with the four cornerstones of Ascensus's products and client service: (1) Client, (2) Associate, (3) Policy and Process, and (4) Fiscal Responsibility. This focus, combined with Ascensus's Core Values of People Matter, Quality First and Integrity Always, promotes a professional working environment for associates.

To encourage staff continuity, supervisory personnel are eligible to receive an annual bonus that is directly tied to client retention and client satisfaction, associate satisfaction, and the achievement of agreed-upon performance standards.

Ascensus recognizes the dignity of each of its associates and believes in the importance of cultivating a diverse and inclusive working environment. The organization embraces, respects, and appreciates the contributions of all associates. Through programs and practices, Ascensus is committed to fostering inclusion and tolerance, promoting an appreciation of differences and creating a culture where there is mutual respect among all associates. Ascensus's diversity mission statement defines a core component of the core value that "People Matter."

Learning and Development

Associates receive training through in-house classroom and self-paced training courses, supervised on-the-job training, formal coaching programs, and external seminars and education programs. Content for in-house classroom and self-paced training courses is reviewed and updated annually or when there are regulatory updates. This review and update are performed by Learning and Development and by Subject Matter Experts (SMEs) from various business units. New associates attend an onboarding training program to ensure they understand their job functions and how their responsibilities fit into overall business objectives. On an annual basis, Ascensus communicates the code of conduct, security policies and practices, and procedures for submitting complaints and/or unethical behavior to Ascensus personnel. On an annual basis, Ascensus personnel must complete Annual Security Awareness Training confirm their understanding of and compliance with the Ascensus's code of conduct and security policies.

2. Risk Assessment

Ascensus has implemented processes that enable management to proactively monitor and manage risks impacting its ability to achieve business objectives, meet operational service levels and provide reliable transaction processing for clients. These processes identify, assess, and mitigate risks associated with implementing new technologies and service solutions while addressing regulatory and industry matters and other critical business initiatives.

Risk Management facilitates periodic risk assessments with the senior management teams of each business division to identify key risk concerns. The results of these assessments are used to assist management with developing an internal control evaluation plan for the year.

Ascensus's Compliance team facilitates annual compliance inspections of its securities operations to determine its level of compliance with applicable SEC and FINRA rules and regulations and to assess the effectiveness of internal controls and supervisory procedures. These compliance inspections are similar in scope to examinations conducted by the SEC and FINRA and are designed to focus on those areas with the highest potential risk to business operations.

On an annual basis, Ascensus contracts with an outside firm to conduct an AML program review to ensure compliance with FINRA's Rule 3310. The scope of the AML review also includes an assessment of compliance with applicable sections of the Advisers Act, SEC Rule 17a-8, the Bank Secrecy Act, Office of Foreign Asset Control requirements and applicable filing and reporting requirements of the Financial Crimes Enforcement Network.

3. Monitoring

Each of Ascensus's divisional management teams monitors the quality of its operational activities, including the internal control environment, as a routine part of their daily activities. Management reports are used for each significant function and are monitored at established intervals. The Executive Steering Committee, which includes senior management and IT representatives, meets to discuss the status of current and proposed projects.

Ascensus's leadership teams have developed and implemented processes to provide assurance that system controls are adequately designed to address identified risks relevant to the operation of the systems and that those controls operate in an effective manner. These processes include a risk identification and assessment process to review any existing or new risks that could threaten the operation of the systems. Controls are implemented to mitigate known risks. This information serves as a basis for the assertion Ascensus management makes in Section II of this report.

A comprehensive vendor management framework exists to ensure appropriate due diligence is performed before Ascensus enters into third-party relationships. Provisions are made for effective oversight after the relationship has been established, including periodic reassessments of each vendor against established due diligence standards. The framework also provides guidance for procurement efforts, including sourcing needs assessment, vendor selection, contract management and ongoing monitoring. A fundamental component of the framework is a structured vendor risk management program that classifies vendors based on risk potential, requires greater scrutiny of vendors identified with higher risk potential and ensures appropriate monitoring and mitigation of identified risks.

Vendor performance is overseen by the Procurement and Vendor Strategy group with direct monitoring of each vendor done by an assigned vendor owner from the line of business that primarily utilizes the services of each subservice organization. As applicable, vendor owners solicit input and feedback from the business areas that use each vendor's services to ensure a comprehensive view of vendor performance. The monitoring and oversight performed by the vendor owners are done at a level of detail commensurate with the business relationship and criticality of the vendor.

When available, Ascensus's management obtains and reviews SOC 1 and/or SOC 2 reports from subservice organizations to verify that adequate controls relevant to Ascensus's control environment are in place and operating effectively. Details on governance programs, including Business Continuity and Vendor Management programs are also collected from vendors for Ascensus' review.

4. Information and Communication

Ascensus employs various methods of communication to ensure that associates understand their individual roles and responsibilities and to ensure that significant events are communicated in a timely and secure manner. These methods include orientation and training programs for newly hired employees, internal communications that summarize significant events and changes, and the use of email messages to communicate time-sensitive, legislative and regulatory messages and information. Executive management and corporate leadership hold periodic meetings to provide insight into strategic direction, key decisions, and company performance summaries. Managers also hold periodic staff meetings as appropriate to disseminate Mission critical information.IT communicate initiatives, performance, and IT security effectiveness to leadership members to ensure that SLAs and security obligations are sustained. Key IT initiatives are presented to senior leadership to ensure timely progress and the proper prioritization of upcoming projects. Ascensus IT monitors network performance and provides a summary to IT leadership. Ascensus IT also performs network scans and regularly scheduled external scans to validate these results. Summaries regarding infrastructure performance, security scan results, and enhancement initiatives are communicated to Ascensus IT leadership.

E. Control Activities

1. Physical Security

Ascensus data center operations are conducted from the Csquare colocation Data Center in Watertown, MA. Ascensus's contract with Csquare mandates a security environment that includes physical access security controls to protect access to Ascensus equipment, including keycard access directly controlled by Ascensus, biometric verification as a multi-factor authentication tool, and CCTV coverage. In addition, Csquare is required to maintain environmental controls including HVAC, fire suppression, backup UPS power, and water detection/raised flooring.

Csquare's continued adherence to those contractual mandates is overseen by the Ascensus Vendor Strategy program, which assesses all vendors on at least an annual basis via detailed questionnaires, ad hoc reviews to ensure that key remediating actions are taken promptly when significant vulnerabilities have been identified, and on-site reviews.

2. Logical Access

Access to Ascensus's systems is controlled via a ticketing system to ensure that all requests receive the proper approvals before any access is established or altered.

Internally, for all business divisions, access to customer information is limited to those Ascensus associates with a business reason to know or use such information. Associates are educated on the importance of maintaining the confidentiality of customer information and on the provisions of Ascensus's policies and procedures regarding the handling of customer information via annual required training.

Associates' access to Ascensus's systems that house client data is monitored. Administrative access to Ascensus's systems is commensurate with the user's job responsibility. Requests for new or modified access are submitted, reviewed to ensure that access is commensurate with job functions and approved by management before the access is granted. In order to ensure that access is commensurate with job functions, users are granted access based on profiles defined by business group management.

Users must be authenticated to Ascensus's systems using a unique confidential username and password. Multi-Factor Authentication, via a one-time code sent to a registered device, is required for all remote access. Passwords must conform to corporate requirements for length and complexity, and users are required to periodically change their passwords. Associates who terminate their employment with Ascensus have their access to Ascensus's systems removed timely via a process coordinated by the Human Resources team.

3. Business Continuity

Ascensus has established policies and procedures for business continuity, incident management and reporting. Ascensus's recovery management is organized by site into teams with specific roles and responsibilities. The Site Incident Coordinator (IC) has the overall responsibility and accountability for managing and coordinating the response should an incident occur at an Ascensus location. The IC leads the Site Incident Management team (SIMT), a team of managers representing major functional areas at a site. Responsibilities of the IC and the other SIMT members are documented in the business continuity plan (BCP) for the site; this is the highest-level plan at a site.

To support the BCP, additional plans are used for clients or departments at the site. Each plan has its own designated owner who is accountable for executing their specific plan.

The BCP includes the names, contact information and communications procedures for plan stakeholders, including the plan owner, recovery team leaders, recovery team members, clients and vendors. Ascensus's Risk Management team is responsible for testing the plan at least annually, coordinating updates (done at least annually), and training recovery team members.

All plan owners are responsible for keeping their plan updated and aligned with current business practices. The SIMT and the recovery team review the BCP on a periodic basis.

4. Disaster Recovery

Primary and recovery data centers are utilized to maintain a comprehensive disaster recovery arrangement. If the primary data center is impacted by a disruption, the recovery data center will be brought into service; communications lines are switchable from one data center to the other. To ensure the validity of this contingency plan, these arrangements are tested several times per year, involving a selection of clients' information and Ascensus service centers. Data is replicated and stored at the disaster recovery sites to enable quicker recovery. Data at the disaster recovery site is stored on Ascensus-owned storage equipment in locked cages segregated from other organizations' data.

5. Backup

In order to ensure that Ascensus can effectively recover operations as quickly as possible in the event of a system interruption or unintended loss of data, backup records for the systems are produced each business day and stored at secure off-site locations. Ascensus has protocols in place to create these backups, and has secure methods to track and retrieve them, when needed.

Backups are tested at least annually in conjunction with the disaster recovery testing to ensure that, in the event of an incident or data loss, Ascensus is prepared to resume operations and/or recover data as quickly as possible. During the DR testing, backups are used to bring the systems up remotely and business users mimic live production processing using the backups.

6. Monitoring of Computer Operations

Ascensus has tools in place to monitor the systems and processes and to alert Ascensus personnel of potential threats in their environment. Ascensus has defined escalation rules based on the severity of the threat, which are incorporated into the ticketing system to ensure timely action is taken.

7. System Maintenance

Ascensus has a documented change management process for system implementations and maintenance.

A software implementation project must be approved by management before it is initiated. Projects that are categorized as production support, including bug fixes, branding, or required regulatory changes, are pre-approved and require no additional approvals prior to initiation. All other projects require approval by senior management, which is captured in a project tracking system.

Management is informed on a regular basis of the status of active projects, and projects that are scheduled but awaiting initialization.

Once a project has been initiated, a documented Agile Software Development Life Cycle (SDLC) is followed to ensure changes are executed in a controlled and consistent manner. The SDLC includes steps to validate that all changes are tested and approved before they are promoted to a production environment. Software tools are in place to enforce adherence to the defined SDLC. Source code is maintained on and accessed via a Team Foundation Server (TFS).

Development work is performed in a segregated development environment to reduce the impact on live business processes during the development process. Once development changes have been completed, they are moved to a Quality Assurance (QA) environment where formal testing is completed. Once successful testing has been completed and approval obtained, projects can be scheduled for promotion to the production environment. Application programmers are logically restricted from moving programs into the production environment, or reviews are performed periodically to identify unauthorized changes to the production environment. Segregation of duties is either systematically enforced via branch protection policies or access to promote changes is

governed by policies that prevent promotion of code by an individual without appropriate approvals. Additionally, on a monthly basis, all changes to the production environment related to the BOLI application, its code, and associated databases are reviewed by a member of management to verify that each change was authorized and that no changes were developed and promoted by the same individual. Changes to the production environment are scheduled on pre-approved implementation days and are documented in a weekly implementation report that is distributed to managers, supervisors, and other support staff. If a change needs to be implemented outside of the approved days, a process exists to accommodate these as emergency changes. These changes are documented through the completion of an emergency implementation authorization form that requires the approval of senior management.

When new servers are built within Ascensus's environment, the process is completed based on pre-defined standards and checklists. These checklists ensure adherence to the standards and must be approved via digital signature by Infrastructure team associates before the server is used in production.

8. Change Management

Several critical activities are performed in the QA environment. These include:

- Testing new releases of application software
- Testing new or additional functionality
- Testing changes to system or application configurations
- Performance testing

The QA environment mirrors the production environment in terms of release level, instances, user entities and the interface systems. This is to provide a valid test environment for both project implementation and post-implementation go-live support.

Code is developed and unit-tested in the Development (DEV) environment. Once ready for QA testing, code is migrated to the QA environment by the Implementations team. The QA team logs any defects and assigns them to the Development team for resolution in DEV. Upon resolution of defects, the Implementations team migrates the revised code to the QA environment for further testing. This cycle continues until QA testing is successful.

Once testing is successful in QA, a production implementation schedule is established that aligns with business objectives and the Implementations team's release schedule. The Implementation team then migrates the code from the QA environment to the production environment.

F. Changes to the System During the Specified Period

There were no changes that are likely to affect report users' understanding of how the Retirement and Government Savings Systems are used to provide the service during the period from October 1, 2024 through September 30, 2025.

G. Additional Information about Management's Description

The controls supporting the service organization's service commitments and system requirements based on the applicable trust services criteria are included within Section IV of this report, "Description of the Trust Services Category, Criteria, Ascensus' Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results." Although the applicable trust services criteria and related control activities are presented within Section IV, they are an integral part of the Company's description of its system.

H. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Vertical Management Systems (VMS)	Vertical Management Services provides Qualified Plan Retirement teams with the HUB+ application that is used for direct trading of mutual funds with the National Securities Clearing Corporation (NSCC). The following controls are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Physical access to the Data Center hosting the VMS software is restricted to authorized personnel. • Changes to application and system software are authorized, tested, approved, and implemented by authorized personnel. • Backups are performed regularly and stored in a secure location. • Computer operations are monitored to ensure that problems are identified, documented, and resolved on a timely basis. • Logical access to system files, data files, program files and transactions is restricted to authorized users. In addition, the Company has identified the following controls to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 2.1 CC 4.1 CC 4.2 CC 5.1 CC 5.3 CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.4 CC 6.6 CC 6.7 CC 6.8 CC 7.5 CC 8.1 CC 9.1

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Csquare	Csquare is the primary site for third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Center ensuring that physical access to the system resources is restricted to authorized individuals, and the physical environment is monitored and protected from disruptive events. In addition, the Company has identified the following controls to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 6.4

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Switch	Switch is the backup site for third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Center ensuring that physical access to the system resources is restricted to authorized individuals, and the physical environment is monitored and protected from disruptive events. In addition, the Company has identified the following controls to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 6.4

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Envision Financial Systems	Envision Financial Systems provides the PowerAgent529 recordkeeping platform. AGS currently utilizes PowerAgent529 in an ASP mode to provide recordkeeping of certain 529 plans' participant accounts. The following controls are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Physical access to the Data Center hosting the PowerAgent529 software is restricted to authorized personnel. • Changes to application and system software are authorized, tested, approved, and implemented by authorized personnel. • Backups are performed regularly and stored in a secure location. • Computer operations are monitored to ensure that problems are identified, documented, and resolved on a timely basis. • Logical access to system files, data files, program files and transactions is restricted to authorized users. In addition, the Company has identified the following controls to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 2.1 CC 4.1 CC 4.2 CC 5.1 CC 5.3 CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.4 CC 6.6 CC 6.7 CC 6.8 CC 7.5 CC 8.1 CC 9.1

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services, Inc. (“AWS”)	The Company uses Amazon Web Services for its third-party hosting of AGS’s Unite and ASTRO platforms. The following controls are critical to achieving the Company’s service commitments and system requirements based on the applicable trust services criteria: • Physical access to the Data Center hosting the cloud software is restricted or authorized. • Changes to application and system software are authorized, tested, approved, and implemented by authorized personnel. • Encryption keys are held securely and segregated by the tenant. • Computer operations are monitored to ensure that problems are identified, documented, and resolved on a timely basis. • Logical access to system files and transactions is restricted to authorized users. In addition, the Company has identified the following controls to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 2.1 CC 4.1 CC 4.2 CC 5.1 CC 5.2 CC 5.3 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8 CC 8.1

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Infosys McCamish Systems, LLC ("McCamish")	McCamish develops and maintains the calculation module portion of the Transaction System. The following controls are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls provide reasonable assurance that changes to the calculations of the transaction module are tested and approved prior to implementation into production. • Logical access to system files, data files, program files and transactions is restricted to authorized users. In addition, the Company has identified the following controls to help monitor the subservice organization: • The Plan Administrator reviews and reconciles the exception reports that identify discrepancies between the Transaction System, the printed website to be sure all areas reconcile. • Automated and manual reconciliation controls are utilized to confirm calculations. • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8 CC 8.1

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
SS&C Technologies, Inc. ("SS&C")	SS&C provides change management, logical security, and computer operations for the Interactive Voice Response (IVR) Application, and Automated Workflow Distributor (Chorus). The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls provide reasonable assurance that the application is monitored to help ensure data integrity and accuracy. • Controls provide reasonable assurance that logical access to the applications and related databases is appropriate. • Controls provide reasonable assurance that changes to the applications and related databases are tested and approved prior to implementation into production. In addition, the Company has identified the following controls to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review. of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 2.1 CC 4.1 CC 4.2 CC 5.1 CC 5.2 CC 5.3 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8 CC 8.1

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
SEI Private Trust Company ("SEI")	SEI Private Trust Company provide change management, logical security, and computer operations for the Trust 3000, DepLink, RBPS, CSS, and Cconnect applications. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls provide reasonable assurance that the application is monitored to help ensure data integrity and accuracy. • Controls provide reasonable assurance that logical access to the applications and related databases is appropriate. • Controls provide reasonable assurance that changes to the applications and related databases are tested and approved prior to implementation into production. In addition, the Company has identified the following controls to help monitor the subservice organization. • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 2.1 CC 4.1 CC 4.2 CC 5.1 CC 5.2 CC 5.3 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8 CC 8.1

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Andesa Services, Inc. ("Andesa")	Andesa Services, Inc. provides change management, logical security, and computer operations for the Q+ Benefit Administration Application. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls provide reasonable assurance that logical access to the Q+ Benefits Administration Application and related database is restricted to appropriate users based upon assigned job functions. • Controls provide reasonable assurance that the application is monitored to help ensure data integrity and accuracy. • Controls provide reasonable assurance that changes to the Q+ Benefits Administration Application and related database are tested and approved prior to implementation into production. In addition, the Company has identified the following controls to help monitor the subservice organization. • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 2.1 CC 4.1 CC 4.2 CC 5.1 CC 5.2 CC 5.3 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8 CC 8.1

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Oracle Cloud	The Company uses Oracle Cloud for its third-party servers and equipment, including the restriction of physical access to the defined system including, but not limited to backup media. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Centers where the in-scope applications are backed up. • Controls around the backup processes of servers hosting the in-scope applications to support disaster recovery processes. In addition, the Company has identified the following control activities to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 6.4 CC 7.5 CC 9.1

Subservice Organization	Service Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Vital Records, Inc (VRI)	The Company uses Vital Records, Inc. (VRI) for storage of system backup tapes. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Center ensuring that physical access to the system resources is restricted to authorized individuals, and the physical environment is monitored and protected from disruptive events. In addition, the Company has identified the following controls to help monitor the subservice organization: • The Company has a Vendor Compliance process that provides on-going monitoring of all vendor relationships to ensure that they are adhering to contractual requirements around both service delivery and information security. Detailed reviews are completed that include inquiries, review of relevant audit reports. SOC and other attestation reports, if available, are reviewed by Ascensus management.	CC 6.4

I. Complementary User Entity Controls

Ascensus' controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated criteria are included within the table below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity controls have been implemented and are operating effectively.

User Entity Control	Associated Criteria
For the Qualified Retirement Plan Applications, user entities are responsible for granting access to their respective client portals to authorized individuals.	CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.8

User Entity Control	Associated Criteria
For the Qualified Retirement Plan Applications, user entities are responsible for removing access for individuals who no longer require access.	CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.8
For the Qualified Retirement Plan Applications, user entities are responsible for periodically reviewing individuals in their organizations who have access to the ARS and for removing or modifying that access as necessary.	CC 6.1 CC 6.2 CC 6.3 CC 6.5 CC 6.6 CC 6.8
For the Retirement Products & Solutions (RPS), user entities are responsible for granting appropriate user access rights through the use of roles, based on the job function of personnel within the user organization.	CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.8
For the Retirement Products & Solutions (RPS), user entities are responsible for revoking user access at the organization.	CC 6.1 CC 6.2 CC 6.3 CC 6.5 CC 6.6 CC 6.8
For the Retirement Products & Solutions (RPS), user entities are responsible for resetting accounts and passwords at the user organization.	CC 6.1 CC 6.2 CC 6.3 CC 6.5 CC 6.6 CC 6.8

User Entity Control	Associated Criteria
For the Retirement Products & Solutions (RPS), user entities are responsible for establishing controls to maintain the confidentiality of user passwords.	CC 6.1 CC 6.2 CC 6.3 CC 6.5 CC 6.6 CC 6.8
For the Ascensus Government Saving Applications, user entities are responsible for ensuring that access to their instance of the Unite or ASTRO application is appropriate for their associates and that AGS is notified timely of necessary changes to access.	CC 6.1 CC 6.2 CC 6.3 CC 6.5 CC 6.6 CC 6.8
For the Ascensus Government Saving Applications, user entities are responsible for ensuring that any sensitive data transmitted or sent to AGS is encrypted using approved encryption technology.	CC 6.1 CC 6.6 CC 6.7 CC 6.8
For the Non-Qualified Retirement Plan Applications, to the extent user entities have administrative access to Company terminals and systems, including access via the Internet, each user entity is responsible for establishing and maintaining adequate controls over physical and logical access at the user entity's location. Each user entity is responsible for the provisioning and deprovisioning of access to the in-scope systems.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8
For the Non-Qualified Retirement Plan Applications, user entities are responsible for establishing their own access controls and authorization policies and procedures and for implementing them within the framework of the Company's system.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8

User Entity Control	Associated Criteria
For the Non-Qualified Retirement Plan Applications, user entities are responsible for thoroughly testing the initial configuration of system access to ensure the configurations have been performed in accordance with the entity's requirements.	CC 5.2 CC 6.1 CC 6.6 CC 6.7 CC 6.8 CC 8.1
For the Non-Qualified Retirement Plan Applications, user entities are responsible for notifying the Company when contact information such as e-mail addresses or phone numbers for key contacts at the user organization changes.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.8

.

IV. Description of the Trust Services Categories, Criteria, Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc. Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results

A. Types and Descriptions of the Tests of Operating Effectiveness Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at user entities and subservice organizations, is intended to provide user entities of the Company's System, those prospective user entities, practitioners providing services to such user entities, and other specified parties with information about the control features of the Company's System. The description is intended to provide users with information about the System. Our examination was limited to the applicable trust services criteria and related controls specified by the Company in Sections III and IV of the report and did not extend to the controls in effect at user entities and subservice organizations. It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. If internal control is not effective at user entities, the Company's controls may not compensate for such weaknesses.

The Company's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of our testing of the controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observed the application, performance, or existence of the control
Inspection	Inspected documents, records, or other evidence indicating performance of the control

Inquiries were performed for substantially all controls in Section IV, and, therefore, inquiries were not separately listed as a test for every control.

Additionally, procedures were performed to evaluate whether information produced by the service organization was sufficiently reliable for our purposes, including (i) information provided by the service organization in response to ad hoc requests from the service auditor, such as population lists; (ii) information used in the execution of a control, such as exception reports or transaction reconciliations; and (iii) information prepared for user entities, such as user access lists. ”Sufficiently reliable” for our purposes means that we obtained evidence about the accuracy and completeness of such information and evaluated whether the information was sufficiently precise and detailed. Information produced by the service organization that we utilized as evidence included, but was not limited to, the following:

- System-generated reports without customization (canned reports);
- System-generated reports with customization (internally developed custom reports, queries, or ad hoc custom reports); and
- Manually prepared spreadsheets, analysis, schedules, or other evidence prepared by the service organization and utilized for the performance or testing of a control.

The procedures we performed to evaluate whether the information was sufficiently reliable included obtaining evidence regarding accuracy and completeness, including procedures to address the accuracy and completeness of source data, as well as the creation and modification of applicable report logic and parameters. The procedures performed included tests of controls over the preparation and maintenance of the information or observation or inspection procedures on the information. Although these procedures are not separately listed as a test procedure, the procedures were completed as part of our testing to support the evaluation of whether the information produced by the service organization was sufficiently precise and detailed for purposes of testing the controls identified by the service organization in Section IV.

B. Trust Services Categories, Criteria, Control Activities, Test of Controls, and Results

The trust services criteria relevant to security address that information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the Company's ability to achieve its service commitments and system requirements.

The trust services criteria relevant to availability address that information and systems are available for operation and use to achieve the Company's service commitments and system requirements.

COMMON CRITERIA

Common Criteria to Security and Availability	
CC1: Control Environment	
Control ID	**Control Activity Description**
CC1.1 — COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
PP-35	On an annual basis, Ascensus communicates the code of conduct, security policies and practices, and procedures for submitting complaints and/or unethical behavior to Ascensus personnel. On an annual basis, Ascensus personnel must complete Annual Security Awareness Training confirm their understanding of and compliance with the Ascensus's code of conduct and security policies.
PP-37	Within 30 days of hire date, new employees and contractors must sign a non-disclosure agreement that indicates they understand the confidential nature of the data that they will interact with, and they also electronically acknowledge that they are aware of and bound to follow the information security policies and the Company's code of conduct as outlined in the Company's Policy Manual and the Code of Conduct Handbook.
PP-38	On an annual basis, performance reviews are completed as part of the employee compensation review process to help ensure that each employee's skill set matches his/her job responsibilities.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
PP-41	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.

Common Criteria to Security and Availability	
CC1: Control Environment	
Control ID	**Control Activity Description**
CC1.2 — COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
PP-43	Ascensus has an independent Board of Directors that meets quarterly to oversee the control environment, allocate resources to key security functions, review key risks impacting organizational objectives and corporate culture, and authorize consulting resources as needed.
PP-45	The Ascensus Security Council (ASC) is a cross-functional committee that meets on a monthly basis to review potential security-related issues or concerns.
PP-47	Ascensus has reporting mechanisms for associates in place for reporting operational failures, security incidents, problems, and compliance concerns through an anonymous hotline, and both identified and anonymous reporting mechanisms are available. This anonymous hotline is communicated to all stakeholders via the Policy Manual.
CC1.3 — COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
PP-41	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.
PP-42	The Company has a documented and published organizational structure which is available to internal users via the Company's intranet.
PP-46	A CISO role is maintained and is responsible for changes to security practices and commitments. A formal process is documented to communicate these changes and is made available to applicable internal and external users, related parties, and vendors.
TPM-6	Ascensus has an established Vendor Management Program to review and evaluate third-party relationships and ensure that vendors are adhering to contractual service delivery requirements and information security obligations.

Common Criteria to Security and Availability	
CC1: Control Environment	
Control ID	**Control Activity Description**
TPM-7	Acceptable use and limits of use for user entities and external third parties (including vendors and SSOs) are documented within the standard contract template.
CC1.4 — COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
PP-35	On an annual basis, Ascensus communicates the code of conduct, security policies and practices, and procedures for submitting complaints and/or unethical behavior to Ascensus personnel. On an annual basis, Ascensus personnel must complete Annual Security Awareness Training confirm their understanding of and compliance with the Ascensus's code of conduct and security policies.
PP-36	Before starting, each employee and contractor is subjected to a background check in accordance with the Ascensus hiring procedures.
PP-37	Within 30 days of hire date, new employees and contractors must sign a non-disclosure agreement that indicates they understand the confidential nature of the data that they will interact with, and they also electronically acknowledge that they are aware of and bound to follow the information security policies and the Company's code of conduct as outlined in the Company's Policy Manual and the Code of Conduct Handbook.
PP-38	On an annual basis, performance reviews are completed as part of the employee compensation review process to help ensure that each employee's skill set matches his/her job responsibilities.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
PP-41	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.

Common Criteria to Security and Availability	
CC1: Control Environment	
Control ID	**Control Activity Description**
CC1.5 — COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented.
PP-38	On an annual basis, performance reviews are completed as part of the employee compensation review process to help ensure that each employee's skill set matches his/her job responsibilities.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
PP-41	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.

Common Criteria to Security and Availability	
CC2: Information and Communication	
Control ID	**Control Activity Description**
CC2.1 — COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
COM-7	A centralized logging solution is implemented to collect system and application logs for monitoring and alerting purposes. Only appropriate individuals have access to the logs to help ensure that they are protected from alteration.
COM-8	On an annual basis, penetration testing is performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
COM-9	On a monthly basis, internal network scans are performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
PP-41	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.
RA-6	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.
RA-7	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.

Common Criteria to Security and Availability	
CC2: Information and Communication	
Control ID	**Control Activity Description**
CC2.2 — COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CM-28	Ascensus's release calendar describes the in-scope application and related database changes to be implemented, is posted on the intranet, and is available to internal users within the IT department.
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
PP-35	On an annual basis, Ascensus communicates the code of conduct, security policies and practices, and procedures for submitting complaints and/or unethical behavior to Ascensus personnel. On an annual basis, Ascensus personnel must complete Annual Security Awareness Training confirm their understanding of and compliance with the Ascensus's code of conduct and security policies.
PP-37	Within 30 days of hire date, new employees and contractors must sign a non-disclosure agreement that indicates they understand the confidential nature of the data that they will interact with, and they also electronically acknowledge that they are aware of and bound to follow the information security policies and the Company's code of conduct as outlined in the Company's Policy Manual and the Code of Conduct Handbook.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
PP-41	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.
PP-42	The Company has a documented and published organizational structure which is available to internal users via the Company's intranet.
PP-44	Ascensus has provided a description of the in-scope applications and its services, including applicable information related to the boundaries of the System and its processing integrity, on internal repositories and are accessible as needed.
PP-46	A CISO role is maintained and is responsible for changes to security practices and commitments. A formal process is documented to communicate these changes and is made available to applicable internal and external users, related parties, and vendors.

Common Criteria to Security and Availability	
CC2: Information and Communication	
Control ID	**Control Activity Description**
CC2.3 — COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal controls.	
PP-42	The Company has a documented and published organizational structure which is available to internal users via the Company's intranet.
PP-44	Ascensus has provided a description of the in-scope applications and its services, including applicable information related to the boundaries of the System and its processing integrity, on internal repositories and are accessible as needed.
PP-46	A CISO role is maintained and is responsible for changes to security practices and commitments. A formal process is documented to communicate these changes and is made available to applicable internal and external users, related parties, and vendors.

Common Criteria to Security and Availability	
CC3: Risk Assessment	
Control ID	**Control Activity Description**
CC3.1 — COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
PP-41	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.
RA-6	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.
RA-7	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.
CC3.2 — COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
RA-6	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.
RA-7	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.

Common Criteria to Security and Availability	
CC3: Risk Assessment	
Control ID	**Control Activity Description**
TPM-6	Ascensus has an established Vendor Management Program to review and evaluate third-party relationships and ensure that vendors are adhering to contractual service delivery requirements and information security obligations.
TPM-7	Acceptable use and limits of use for user entities and external third parties (including vendors and SSOs) are documented within the standard contract template.
CC3.3 — COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
RA-6	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.
RA-7	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.
CC3.4 — COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
RA-6	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.

Common Criteria to Security and Availability	
CC3: Risk Assessment	
Control ID	**Control Activity Description**
RA-7	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.
TPM-6	Ascensus has an established Vendor Management Program to review and evaluate third-party relationships and ensure that vendors are adhering to contractual service delivery requirements and information security obligations.

Common Criteria to Security and Availability	
CC4: Monitoring Activities	
Control ID	**Control Activity Description**
CC4.1 — COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
COM-8	On an annual basis, penetration testing is performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
COM-9	On a monthly basis, internal network scans are performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
CC4.2 — COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
COM-8	On an annual basis, penetration testing is performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
COM-9	On a monthly basis, internal network scans are performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.

Common Criteria to Security and Availability	
CC5: Control Activities	
Control ID	**Control Activity Description**
CC5.1 — COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
COM-7	A centralized logging solution is implemented to collect system and application logs for monitoring and alerting purposes. Only appropriate individuals have access to the logs to help ensure that they are protected from alteration.
COM-8	On an annual basis, penetration testing is performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
COM-9	On a monthly basis, internal network scans are performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
RA-6	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.
RA-7	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.
CC5.2 — COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CM-23	Changes to the in-scope applications and related databases, including emergency changes, are tested and approved by a member of management prior to promotion into the production environment.

Common Criteria to Security and Availability	
CC5: Control Activities	
Control ID	**Control Activity Description**
CM-24	Ascensus follows a documented SDLC workflow that addresses how program changes and system enhancement projects are initiated, authorized, defined, documented in requirements, programmed, tested, approved for implementation, and promoted into production.
CM-26	Ascensus utilizes development regions that are logically separate from the production environments.
CM-29	Access to update key system parameters that control compliance restrictions is limited to authorized associates based on job function.
CM-30	Segregation of duties is either systematically enforced via branch protection policies or access to promote changes is governed by policies that prevent promotion of code by an individual without appropriate approvals.
CM-31	On a monthly basis, all changes to the production environment related to BOLI application, BOLI application's code, and related databases are reviewed by a member of management to verify that each change was authorized and that no changes were developed and promoted by the same individual.
LS-71	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function.
LS-75	Valid user IDs and passwords are required to access the network, in-scope applications, website and related databases.
LS-76	Administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers is restricted to appropriate individuals based on job function.
CC5.3 — COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
COM-8	On an annual basis, penetration testing is performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
COM-9	On a monthly basis, internal network scans are performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.

Common Criteria to Security and Availability	
CC5: Control Activities	
Control ID	**Control Activity Description**
PP-38	On an annual basis, performance reviews are completed as part of the employee compensation review process to help ensure that each employee's skill set matches his/her job responsibilities.
PP-39	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.
PP-40	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.
PP-41	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.
PP-42	The Company has a documented and published organizational structure which is available to internal users via the Company's intranet.
PP-46	A CISO role is maintained and is responsible for changes to security practices and commitments. A formal process is documented to communicate these changes and is made available to applicable internal and external users, related parties, and vendors.

Common Criteria to Security and Availability	
CC6: Logical and Physical Access Controls	
Control ID	**Control Activity Description**
CC6.1 — The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	
DBR-18	Access to the backup tool is restricted to appropriate individuals based on job function.
DS-12	Laptops, desktops, and hard drives are configured to enforce hard drive encryption.
LS-69	Non-Qualified, Qualified, RPS, and AGS: A tracking ticket to revoke access is automatically created when Human Resources approves an employee termination entered by a manager in the Workday application. Access is revoked within two business days following notification of termination from HR and is documented in a tracking ticket.
LS-71	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function.
LS-72	Password parameters for the in-scope applications are configured to require, at minimum: • Length of 8 characters • Complexity requirements
LS-73	Password parameters for the network, operating systems, and databases related to the in-scope applications are configured to require, at minimum: • Length of 6 characters • Complexity requirements
LS-74	External user account passwords for AGS must be changed upon initial login.
LS-75	Valid user IDs and passwords are required to access the network, in-scope applications, website and related databases.
LS-76	Administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers is restricted to appropriate individuals based on job function.
LS-78	Remote access to Ascensus's internal network is restricted through the use of secure VPN and multi-factor authentication.
LS-80	Build standards are documented to provide consistency when building and implementing servers supporting the in-scope applications. Servers are approved by a member of the Infrastructure team prior to use in production.
LS-85	Multi-factor authentication is required to access servers and databases that support the AGS in-scope applications.
LS-86	Client data is logically segregated, and access is systematically restricted based on client organization.

Common Criteria to Security and Availability	
CC6: Logical and Physical Access Controls	
Control ID	**Control Activity Description**
LS-77	Requests to add and or modify access to the network, in-scope applications, and the related databases and infrastructure are approved by a manager prior to access being granted.
LS-25	Access to the Network, BOLI application and related databases, and the Benefits Administration Application is removed or disabled within two business days of the employee's/contractor's termination date.
CC6.2 — Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
LS-69	Non-Qualified, Qualified, RPS, and AGS: A tracking ticket to revoke access is automatically created when Human Resources approves an employee termination entered by a manager in the Workday application. Access is revoked within two business days following notification of termination from HR and is documented in a tracking ticket.
LS-70	On a periodic basis, Ascensus performs a review of access to the network, in-scope applications, and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.
LS-77	Requests to add and or modify access to the network, in-scope applications, and the related databases and infrastructure are approved by a manager prior to access being granted.
LS-81	Requests to add, modify, and/or remove AGS external user accounts must be completed by Production Support with approval documented in a tracking ticket.
LS-25	Access to the Network, BOLI application and related databases, and the Benefits Administration Application is removed or disabled within two business days of the employee's/contractor's termination date.
CC6.3 — The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
LS-69	Non-Qualified, Qualified, RPS, and AGS: A tracking ticket to revoke access is automatically created when Human Resources approves an employee termination entered by a manager in the Workday application. Access is revoked within two business days following notification of termination from HR and is documented in a tracking ticket.
LS-70	On a periodic basis, Ascensus performs a review of access to the network, in-scope applications, and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.

Common Criteria to Security and Availability	
CC6: Logical and Physical Access Controls	
Control ID	**Control Activity Description**
LS-77	Requests to add and or modify access to the network, in-scope applications, and the related databases and infrastructure are approved by a manager prior to access being granted.
LS-81	Requests to add, modify, and/or remove AGS external user accounts must be completed by Production Support with approval documented in a tracking ticket.
LS-25	Access to the Network, BOLI application and related databases, and the Benefits Administration Application is removed or disabled within two business days of the employee's/contractor's termination date.
CC6.4 — The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
PS-10	The ability to implement changes to physical access rights to sensitive areas and locations is limited to authorized system administrators to prevent unauthorized changes.
PS-11	Terminated employee or contractor physical access to sensitive areas and locations is revoked automatically when Active Directory account is disabled or upon notification from the manager of the terminated associate or contractor.
PS-12	On a semi-annual basis, physical access to sensitive areas and locations is reviewed by management to validate that employee access is commensurate with job responsibilities. Any issues identified are researched and resolved.
PS-13	All external access points to sensitive areas and locations are controlled through an electronic key-card system or restricted to emergency exit only. Key-card access is limited to appropriate individuals.
PS-1	Security badge access requests are approved by Management prior to access being granted.
CC6.5 — The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
DS-10	On an annual basis, Ascensus' data classification policy, is reviewed, updated, and approved by management and outlines the handling, communication, destruction, maintenance, storage, distribution, identification, and classification of confidential information. Processes and supporting policies are in place that identify related processes, systems, and third parties involved in the handling of such information. If the classification of the data is not defined, the default data classification is confidential.
DS-11	A data loss prevention (DLP) software solution is implemented to prevent users from storing confidential data on unencrypted physical media devices. The DLP software solution is configured to automatically enforce Ascensus's DLP configurations on all workstations and laptops on the Ascensus network.

Common Criteria to Security and Availability	
CC6: Logical and Physical Access Controls	
Control ID	**Control Activity Description**
DS-14	The Encryption Policy requires that all media (including backup media) leaving Ascensus's offices and containing sensitive information must be encrypted.
CC6.6 — The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
DBR-18	Access to the backup tool is restricted to appropriate individuals based on job function.
LS-69	Non-Qualified, Qualified, RPS, and AGS: A tracking ticket to revoke access is automatically created when Human Resources approves an employee termination entered by a manager in the Workday application. Access is revoked within two business days following notification of termination from HR and is documented in a tracking ticket.
LS-76	Administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers is restricted to appropriate individuals based on job function.
LS-79	Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Ascensus environment.
LS-71	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function.
LS-25	Access to the Network, BOLI application and related databases, and the Benefits Administration Application is removed or disabled within two business days of the employee's/contractor's termination date.
CC6.7 — The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
DBR-18	Access to the backup tool is restricted to appropriate individuals based on job function.
DS-11	A data loss prevention (DLP) software solution is implemented to prevent users from storing confidential data on unencrypted physical media devices. The DLP software solution is configured to automatically enforce Ascensus's DLP configurations on all workstations and laptops on the Ascensus network.
DS-12	Laptops, desktops, and hard drives are configured to enforce hard drive encryption.
DS-13	Mobile device management software is deployed to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.
LS-69	Non-Qualified, Qualified, RPS, and AGS: A tracking ticket to revoke access is automatically created when Human Resources approves an employee termination entered by a manager in the Workday application. Access is revoked within two business days following notification of termination from HR and is documented in a tracking ticket.

Common Criteria to Security and Availability	
CC6: Logical and Physical Access Controls	
Control ID	**Control Activity Description**
LS-76	Administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers is restricted to appropriate individuals based on job function.
LS-78	Remote access to Ascensus's internal network is restricted through the use of secure VPN and multi-factor authentication.
LS-84	All transmissions of electronic information from/to processing center are encrypted as the default setting over public networks via secure transmission protocols (e.g., HTTPS, SFTP, VPN, and TLS).
LS-85	Multi-factor authentication is required to access servers and databases that support the AGS in-scope applications.
LS-25	Access to the Network, BOLI application and related databases, and the Benefits Administration Application is removed or disabled within two business days of the employee's/contractor's termination date.
CC6.8 — The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CM-25	The version control system is configured to automatically scan Non-Qualified, Qualified, AGS and RPS application source code for vulnerabilities as source code is checked in to the library.
CM-27	Access to make configuration and/or business rule changes to the production environment related to the in-scope applications and related databases is restricted to appropriate users based on job function.
CM-30	Segregation of duties is either systematically enforced via branch protection policies or access to promote changes is governed by policies that prevent promotion of code by an individual without appropriate approvals.
CM-31	On a monthly basis, all changes to the production environment related to BOLI application, BOLI application's code, and related databases are reviewed by a member of management to verify that each change was authorized and that no changes were developed and promoted by the same individual.
LS-69	Non-Qualified, Qualified, RPS, and AGS: A tracking ticket to revoke access is automatically created when Human Resources approves an employee termination entered by a manager in the Workday application. Access is revoked within two business days following notification of termination from HR and is documented in a tracking ticket.
LS-71	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function.
LS-76	Administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers is restricted to appropriate individuals based on job function.

Common Criteria to Security and Availability	
CC6: Logical and Physical Access Controls	
Control ID	**Control Activity Description**
LS-80	Build standards are documented to provide consistency when building and implementing servers supporting the in-scope applications. Servers are approved by a member of the Infrastructure team prior to use in production.
LS-82	Antivirus is automatically deployed to workstations and company hosted servers related to the in-scope applications. Static machine learning and dynamic behavioral analysis are performed to protect against malware.
LS-83	The ability to install software on workstations and laptops is restricted to appropriate users based on job roles.
LS-86	Client data is logically segregated, and access is systematically restricted based on client organization.
LS-25	Access to the Network, BOLI application and related databases, and the Benefits Administration Application is removed or disabled within two business days of the employee's/contractor's termination date.

Common Criteria to Security and Availability	
CC7: Systems Operations	
Control ID	**Control Activity Description**
CC7.1 — To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
COM-8	On an annual basis, penetration testing is performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
COM-9	On a monthly basis, internal network scans are performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
COM-10	On a quarterly basis, future processing demand is forecasted and compared to scheduled capacity. Change requests are initiated as needed.
CC7.2 — The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
COM-7	A centralized logging solution is implemented to collect system and application logs for monitoring and alerting purposes. Only appropriate individuals have access to the logs to help ensure that they are protected from alteration.
COM-8	On an annual basis, penetration testing is performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
COM-9	On a monthly basis, internal network scans are performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.
CC7.3 — The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented.

Common Criteria to Security and Availability	
CC7: Systems Operations	
Control ID	**Control Activity Description**
CC7.4 — The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	
IR-29	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.
CC7.5 — The entity identifies, develops, and implements activities to recover from identified security incidents.	
DBR-14	On an annual basis, a business continuity and disaster recovery plan is documented and is tested, and any issues are documented and resolved.
DBR-15	On a daily basis, incremental backups of the Non-Qualified, Qualified, and RPS applications and related databases are configured to be performed. The backup system is configured to alert Application Technology of any backup failures, and any repeated backup failures are investigated and resolved.
DBR-16	On a daily basis, full backups of the AGS application and related databases are configured to be performed. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved on a weekly basis.
DBR-17	On an annual basis, data restore testing is performed to verify the integrity of the backup data.
DBR-19	Ascensus maintains a program within the BCP to conduct tabletop exercises to practice responses to potential incident scenarios.
DBR-3	Backups to the BOLI applications and related databases are configured to be performed daily. The backup system is configured to alert Application Technology of any backup failures, and any repeated backup failures are investigated and resolved.

Common Criteria to Security and Availability	
CC8: Change Management	
Control ID	**Control Activity Description**
CC8.1 — The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
CM-23	Changes to the in-scope applications and related databases, including emergency changes, are tested and approved by a member of management prior to promotion into the production environment.
CM-24	Ascensus follows a documented SDLC workflow that addresses how program changes and system enhancement projects are initiated, authorized, defined, documented in requirements, programmed, tested, approved for implementation, and promoted into production.
CM-25	The version control system is configured to automatically scan Non-Qualified, Qualified, AGS and RPS application source code for vulnerabilities as source code is checked in to the library.
CM-26	Ascensus utilizes development regions that are logically separate from the production environments.
CM-27	Access to make configuration and/or business rule changes to the production environment related to the in-scope applications and related databases is restricted to appropriate users based on job function.
CM-29	Access to update key system parameters that control compliance restrictions is limited to authorized associates based on job function.
CM-30	Segregation of duties is either systematically enforced via branch protection policies or access to promote changes is governed by policies that prevent promotion of code by an individual without appropriate approvals.
CM-31	On a monthly basis, all changes to the production environment related to BOLI application, BOLI application's code, and related databases are reviewed by a member of management to verify that each change was authorized and that no changes were developed and promoted by the same individual.
LS-80	Build standards are documented to provide consistency when building and implementing servers supporting the in-scope applications. Servers are approved by a member of the Infrastructure team prior to use in production.

Common Criteria to Security and Availability	
CC9: Risk Management	
Control ID	**Control Activity Description**
CC9.1 — The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
DBR-14	On an annual basis, a business continuity and disaster recovery plan is documented and is tested, and any issues are documented and resolved.
DBR-15	On a daily basis, incremental backups of the Non-Qualified, Qualified, and RPS applications and related databases are configured to be performed. The backup system is configured to alert Application Technology of any backup failures, and any repeated backup failures are investigated and resolved.
DBR-16	On a daily basis, full backups of the AGS application and related databases are configured to be performed. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved on a weekly basis.
DBR-17	On an annual basis, data restore testing is performed to verify the integrity of the backup data.
DBR-19	Ascensus maintains a program within the BCP to conduct tabletop exercises to practice responses to potential incident scenarios.
OTH-6	Ascensus maintains insurance coverages designed to insulate the organization from the effects of a large-scale loss event.
PP-43	Ascensus has an independent Board of Directors that meets quarterly to oversee the control environment, allocate resources to key security functions, review key risks impacting organizational objectives and corporate culture, and authorize consulting resources as needed.
RA-6	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.
RA-7	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.

Common Criteria to Security and Availability	
CC9: Risk Management	
Control ID	**Control Activity Description**
CC9.2 — The entity assesses and manages risks associated with vendors and business partners.	
RA-6	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.
RA-7	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.
TPM-6	Ascensus has an established Vendor Management Program to review and evaluate third-party relationships and ensure that vendors are adhering to contractual service delivery requirements and information security obligations.
TPM-7	Acceptable use and limits of use for user entities and external third parties (including vendors and SSOs) are documented within the standard contract template.

Availability	
A1: Additional Criteria for Availability	
Control ID	**Control Activity Description**
A1.1 — The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	
COM-10	On a quarterly basis, future processing demand is forecasted and compared to scheduled capacity. Change requests are initiated as needed.
COM-11	The Company's production environment related to the in-scope applications and related databases is monitored for uptime, latency, utilization, and active services on an ongoing basis, and IT personnel are automatically notified in the event of an incident. Any actionable incidents are researched and resolved.
DBR-20	The Company maintains a recovery site to permit the resumption of full IT operations in the event of a disaster at its primary Data Center. The site undergoes annual testing to assess its effectiveness and verify the organization's ability to restore critical operations.
A1.2 — The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	
DBR-20	The Company maintains a recovery site to permit the resumption of full IT operations in the event of a disaster at its primary Data Center. The site undergoes annual testing to assess its effectiveness and verify the organization's ability to restore critical operations.
DBR-15	On a daily basis, incremental backups of the Non-Qualified, Qualified, and RPS applications and related databases are configured to be performed. The backup system is configured to alert Application Technology of any backup failures, and any repeated backup failures are investigated and resolved.
DBR-16	On a daily basis, full backups of the AGS application and related databases are configured to be performed. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved on a weekly basis.
DBR-17	On an annual basis, data restore testing is performed to verify the integrity of the backup data.
A1.3 — The entity tests recovery plan procedures supporting system recovery to meet its objectives.	
DBR-20	The Company maintains a recovery site to permit the resumption of full IT operations in the event of a disaster at its primary Data Center. The site undergoes annual testing to assess its effectiveness and verify the organization's ability to restore critical operations.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
CM-23	CC5.2 CC8.1	Changes to the in-scope applications and related databases, including emergency changes, are tested and approved by a member of management prior to promotion into the production environment.	**Inspection:** Inspected the change tickets for a sample of changes related to the in-scope applications and related databases to determine that each change was tested and approved by a member of management prior to promotion into the production environment.	No exceptions noted.
CM-24	CC5.2 CC8.1	Ascensus follows a documented SDLC workflow that addresses how program changes and system enhancement projects are initiated, authorized, defined, documented in requirements, programmed, tested, approved for implementation, and promoted into production.	**Inspection:** Inspected the SDLC workflow document to determine that Ascensus followed documented policies that addressed how program changes and system enhancement projects were initiated, authorized, defined, documented in requirements, programmed, tested, approved for implementation, and promoted into production.	No exceptions noted.
CM-25	CC6.8 CC8.1	The version control system is configured to automatically scan Non-Qualified, Qualified, AGS and RPS application source code for vulnerabilities as source code is checked in to the library.	**Inspection:** Inspected the version control tool and static scan tool configurations to determine that the systems were configured to automatically scan Non-Qualified, Qualified, AGS and RPS application source code for vulnerabilities as source code is checked in to the library.	No exceptions noted.
CM-26	CC5.2 CC8.1	Ascensus utilizes development regions that are logically separate from the production environments.	**Inspection:** Inspected the separate development and production environments for the Qualified and Non-Qualified Applications to determine that the development regions that were logically separate from the production environments.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
			Inspection: Inspected the separate development and production environments for the BOLI Applications to determine that the development regions that were logically separate from the production environments.	No exceptions noted.
			Inspection: Inspected the separate development and production environments for the RPS Applications to determine that the development regions that were logically separate from the production environments.	No exceptions noted.
			Inspection: Inspected the separate development and production environments for the AGS Applications to determine that the development regions that were logically separate from the production environments.	No exceptions noted.
			Inspection: Inspected the separate development and production environments related to the in-scope application's databases to determine that the development regions were logically separated from the production environments.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
CM-27	CC6.8 CC8.1	Access to make configuration and/or business rule changes to the production environment related to the in-scope applications and related databases is restricted to appropriate users based on job function.	**Inspection:** Inspected the listing of users with access to make configuration and/or business rule changes to the Qualified and Non-Qualified Applications and related databases and the corresponding job titles for all users to determine that access to make configuration and/or business rule changes to the production environment related to the in-scope applications and related databases was restricted to appropriate users based on job function.	No exceptions noted.
			Inspection: Inspected the listing of users with access to make configuration and/or business rule changes to the BOLI Application and related database and the corresponding job titles for all users to determine that access to make configuration and/or business rule changes to the production environment related to the in-scope applications and related databases was restricted to appropriate users based on job function.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
			Inspection: Inspected the listing of users with access to make configuration and/or business rule changes to the RPS Applications and related databases and the corresponding job titles for all users to determine that access to make configuration and/or business rule changes to the production environment related to the in-scope applications and related databases was restricted to appropriate users based on job function.	No exceptions noted.
			Inspection: Inspected a sample of users with access to make configuration and/or business rule changes to the AGS Applications and related databases and the corresponding job titles for all users to determine that access to make configuration and/or business rule changes to the production environment related to the in-scope applications and related databases was restricted to appropriate users based on job function.	No exceptions noted.
CM-28	CC2.2	Ascensus's release calendar describes the in-scope application and related database changes to be implemented, is posted on the intranet, and is available to internal users within the IT department.	**Inspection:** Inspected the release calendar and the Company's intranet to determine that Ascensus's release calendar described the in-scope application and related database changes to be implemented, was posted on the intranet, and was available to internal users within the IT department.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
CM-29	CC5.2 CC8.1	Access to update key system parameters that control compliance restrictions is limited to authorized associates based on job function.	**Inspection:** Inspected the listing of users with access to update key system parameters that control compliance restrictions and the corresponding job titles for all users to determine that access to update key system parameters that control compliance restrictions was limited to authorized associates based on job function.	No exceptions noted.
CM-30	CC5.2 CC6.8 CC8.1	Segregation of duties is either systematically enforced via branch protection policies or access to promote changes is governed by policies that prevent promotion of code by an individual without appropriate approvals.	**Inspection:** Inspected the deployment tool configurations related to the Non-Qualified and Qualified applications and related databases to determine that segregation of duties was systematically enforced via branch protection policies.	No exceptions noted.
			Inspection: Inspected the deployment tool configurations related to the RPS application and related databases to determine that segregation of duties was systematically enforced via branch protection policies.	No exceptions noted.
			Inspection: Inspected the listing of individuals with access to promote changes into the production environment for the Non-Qualified, Qualified, RPS applications and related databases and the corresponding job titles for all users to determine that access to promote changes into the production environment was restricted to appropriate individuals based on job function.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
			Inspection: Inspected the listing of users with the ability to edit the source code, the listings of users with access to promote changes into the production environment related to the AGS Applications and related databases, and the corresponding job titles for all users on the listings of users with access to promote changes into the production environment related to the AGS Applications and related databases to determine that each user on the listing of users with access to promote changes into the production environment related to the AGS Applications and related databases was appropriate to have this access based on job function and did not have the ability to edit the source code.	No exceptions noted.
			Inspection: Inspected the listing of individuals with access to promote changes into the production environment for the BOLI application and related database and the corresponding job titles for all users to determine that access to promote changes into the production environment was restricted to appropriate individuals based on job function.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
CM-31	CC5.2 CC6.8 CC8.1	On a monthly basis, all changes to the production environment related to BOLI application, BOLI application's code, and related databases are reviewed by a member of management to verify that each change was authorized and that no changes were developed and promoted by the same individual.	**Inspection:** Inspected the code comparison reports related to a selected sample of months to determine that, changes to the BOLI Application, BOLI Application's configurations, and related database were reviewed by a member of management to verify that each change was authorized and that no changes were developed and promoted by the same individual.	No exceptions noted.
COM-7	CC2.1 CC5.1 CC7.2	A centralized logging solution is implemented to collect system and application logs for monitoring and alerting purposes. Only appropriate individuals have access to the logs to help ensure that they are protected from alteration.	**Inspection:** Inspected the centralized logging solution configurations to determine that a centralized logging solution was implemented to collect system and application logs for monitoring and alerting purposes.	No exceptions noted.
			Inspection: Inspected a sample of potential security incidents raised by the SIEM tool to determine that identified risks were investigated and monitored through resolution.	No exceptions noted.
			Inspection: Inspected the listing of users with access to the logs and the corresponding job titles for all users to determine that only appropriate individuals had access to the logs to ensure they were protected from alteration.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
COM-8	CC2.1 CC4.1 CC4.2 CC5.1 CC5.3 CC7.1 CC7.2	On an annual basis, penetration testing is performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.	**Inspection:** Inspected the penetration test and results to determine that testing was performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities.	No exceptions noted.
			Inspection: Inspected the tracking ticket related to a sample of critical/high vulnerabilities to determine that vulnerabilities were tracked within a ticketing system and remediation was completed within the parameters of the remediation schedule.	The Service Auditor noted that this portion of the control activity did not operate during the specified period, as there were no critical or high-risk vulnerabilities identified within the annual penetration test. Therefore, this portion of the control activity could not be tested for operating effectiveness.
			Inspection/Inquiry: Inspected the test results within the penetration to determine that there were no critical or high vulnerabilities related to the penetration testing for all internet-facing infrastructure performed during the specified period. Further, inquired of the Risk Management Director to determine that there were no critical or high vulnerabilities related to the penetration testing for all internet-facing infrastructure performed during the specified period.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
COM-9	CC2.1 CC4.1 CC4.2 CC5.1 CC5.3 CC7.1 CC7.2	On a monthly basis, internal network scans are performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system and is completed within the parameters of the remediation schedule.	**Inspection/Inquiry:** Inspected the internal network scans related to a sample of months to determine that for each selected month an internal network scan was performed to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the Director of Risk Management to determine that there were no critical/high vulnerabilities identified during the sampled months; however, if there had been any critical/high vulnerabilities, each vulnerability would have been tracked within a ticketing system and completed within the parameters of the remediation schedule	No exceptions noted.
COM-10	CC7.1 A1.1	On a quarterly basis, future processing demand is forecasted and compared to scheduled capacity. Change requests are initiated as needed.	**Inspection:** Inspected the forecast and demand documentation related to a sample of quarters to determine that future processing demand was forecasted and compared to scheduled capacity for each selected quarter. Further, inspected the forecast and demand documentation related to each selected quarter and the corresponding change management tickets to determine that change requests were initiated as needed based on the forecast for each selected quarter.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
COM-11	A1.1	The Company's production environment related to the in-scope applications and related databases is monitored for uptime, latency, utilization, and active services on an ongoing basis, and IT personnel are automatically notified in the event of an incident. Any actionable incidents are researched and resolved.	**Observation:** Observed the monitoring tool configurations for the production environment related to the in-scope applications and related databases to determine that the Company's production environment was monitored for uptime, latency, utilization, and active services on an ongoing basis and that IT personnel were automatically notified in the event of an incident.	No exceptions noted.
			Inspection: Inspected the incident ticket related to a sample of actionable incidents to determine that each selected incident was researched and resolved.	No exceptions noted.
DBR-3	CC7.5	Backups to the BOLI applications and related databases are configured to be performed daily. The backup system is configured to alert Application Technology of any backup failures, and any repeated backup failures are investigated and resolved.	**Inspection:** Inspected the Oracle backup schedules to determine that backups to the in-scope applications and related databases are configured to be performed daily.	No exceptions noted.
			Inspection: Inspected the daily backup status email related to a sample of days to determine that, for each sampled day, backups to the in-scope applications and related databases were performed daily, and any repeated backup failures were investigated and resolved.	No exceptions noted.
			Inspection: Inspected the backup notification settings for the BOLI application and related database to determine that the backup system was configured to alert Application Technology of any backup failures.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
DBR-14	CC7.5 CC9.1	On an annual basis, a business continuity and disaster recovery plan is documented and is tested, and any issues are documented and resolved.	**Inspection:** Inspected the Business Continuity and Disaster Recovery Plan to determine that Ascensus had established policies and procedures for business continuity and disaster recovery.	No exceptions noted.
			Inspection: Inspected the results for the annual BCP/DR test to determine that the plan was tested and any issues were documented and resolved.	No exceptions noted.
DBR-15	CC7.5 CC9.1 A1.2	On a daily basis, incremental backups of the Non-Qualified, Qualified, and RPS applications and related databases are configured to be performed. The backup system is configured to alert Application Technology of any backup failures, and any repeated backup failures are investigated and resolved.	**Inspection:** Inspected the backup configurations related to the Non-Qualified and Qualified applications and related databases to determine that backups were configured to be performed daily, and that Application Technology was notified of any backup failures.	No exceptions noted.
			Inspection: Inspected the backup reports and associated tickets for a sample of days to determine that any backup failures and repeated backup failures were investigated and resolved.	No exceptions noted.
			Inspection: Inspected the backup configurations related to the RPS application and related databases to determine that backups were configured to be performed daily, and that Application Technology was notified of any backup failures.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
DBR-16	CC7.5 CC9.1 A1.2	On a daily basis, full backups of the AGS application and related databases are configured to be performed. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved on a weekly basis.	**Inspection:** Inspected the AGS backup schedule and notification configurations to determine that full backups of the AGS application and related databases were configured to be performed on a daily basis and alert IT personnel of any backup failures.	No exceptions noted.
			Inspection: Inspected the backup reports for a sample of weeks to determine that, for each selected week, full backups were performed, and any repeated backup failures were investigated and resolved.	No exceptions noted.
DBR-17	CC7.5 CC9.1 A1.2	On an annual basis, data restore testing is performed to verify the integrity of the backup data.	**Inspection:** Inspected the annual data restore test results to determine that data restore testing was performed to verify the integrity of the backup data.	No exceptions noted.
DBR-18	CC6.1 CC6.6 CC6.7	Access to the backup tool is restricted to appropriate individuals based on job function.	**Inspection:** Inspected the listing of users with access to the backup tool and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function.	No exceptions noted.
DBR-19	CC7.5 CC9.1	Ascensus maintains a program within the BCP to conduct tabletop exercises to practice responses to potential incident scenarios.	**Inspection:** Inspected the Business Continuity Program Overview and the tabletop test plans to determine that Ascensus maintained a program within the BCP to conduct tabletop exercises to practice responses to potential incident scenarios.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
DBR-20	A1.1 A1.2 A1.3	The Company maintains a recovery site to permit the resumption of full IT operations in the event of a disaster at its primary Data Center. The site undergoes annual testing to assess its effectiveness and verify the organization's ability to restore critical operations.	**Inspection:** Inspected the contract with the recovery site to determine that the Company maintained a recovery site to permit the resumption of full IT operations in the event of a disaster at its primary Data Center.	No exceptions noted.
			Inspection: Inspected the most recent failover testing determine that recovery site underwent annual testing to assess its effectiveness and verify the organization's ability to restore critical operations.	No exceptions noted.
DS-10	CC6.5	On an annual basis, Ascensus' data classification policy, is reviewed, updated, and approved by management and outlines the handling, communication, destruction, maintenance, storage, distribution, identification, and classification of confidential information. Processes and supporting policies are in place that identify related processes, systems, and third parties involved in the handling of such information. If the classification of the data is not defined, the default data classification is confidential.	**Inspection:** Inspected the Ascensus Data Classification policy to determine that it was reviewed, updated and approved by management and outlined the handling, communication, destruction, maintenance, storage, distribution, identification, and classification of confidential information, further that processes and supporting policies were in place that identify related processes, systems, and third parties involved in the handling of such information and If the classification of the data was not defined, the default data classification was confidential.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
DS-11	CC6.5 CC6.7	A data loss prevention (DLP) software solution is implemented to prevent users from storing confidential data on unencrypted physical media devices. The DLP software solution is configured to automatically enforce Ascensus's DLP configurations on all workstations and laptops on the Ascensus network.	**Inspection:** Inspected the DLP software solution configurations to determine that a DLP solution was implemented to prevent users from storing confidential data on unencrypted physical media devices.	No exceptions noted.
			Inspection: Inspected the DLP software solution configurations and an example device to determine that the solution was configured to automatically enforce Ascensus's DLP configurations on all workstations and laptops on the Ascensus network.	No exceptions noted.
DS-12	CC6.1 CC6.7	Laptops, desktops, and hard drives are configured to enforce hard drive encryption.	**Inspection:** Inspected the BitLocker encryption configurations enforced via Intune to determine that encryption was enforced for laptops, desktops, and hard drives.	No exceptions noted.
			Inspection: Inspected the encryption status for a sample of laptops, desktops, and hard drives to determine that each selected sample was configured to enforce hard drive encryption.	No exceptions noted.
DS-13	CC6.7	Mobile device management software is deployed to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.	**Inspection:** Inspected the Mobile Device Management Software configurations to determine that mobile device management software was deployed to protect mobile devices (such as laptops, smart phones, and tablets) that served as information assets.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
DS-14	CC6.5	The Encryption Policy requires that all media (including backup media) leaving Ascensus's offices and containing sensitive information must be encrypted.	**Inspection:** Inspected the Encryption Policy in the Policy Manual to determine that the Encryption Policy required that all media (including backup media) leaving Ascensus's offices and containing sensitive information must be encrypted.	No exceptions noted.
			Inspection: Inspected the DLP encryption configurations to determine that media leaving Ascensus's offices and containing sensitive information was encrypted.	No exceptions noted.
IR-29	CC1.1 CC1.3 CC1.4 CC1.5 CC2.1 CC2.2 CC3.1 CC3.4 CC5.1 CC5.3 CC7.3 CC7.4	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis, and the corrective actions implemented.	**Inspection:** Inspected the Escalation and Incident Response Policy to determine that the policy outlined incident response procedures, including escalation, notification, alerting, affected individuals, documenting the incident and actions taken, and post-incident analysis.	No exceptions noted.
			Inspection: Inspected the incident ticket related to a sample of security incidents to determine that a defined incident management process was initiated for each selected incident which included a root cause analysis, and corrective actions implemented.	The Service Auditor noted that this portion of the control activity did not operate during the specified period, as there were no security incidents during the specified period. Therefore, this portion of the control activity could not be tested for operating effectiveness.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
			Inspection: Inspected the listing of potential system security incidents and the parameters used to generate the listing and the list of noted incidents to determine that the parameters were accurate to result in a complete population and that there were no system security incidents detected or reported during the specified period. Further, inquired of the Risk Management Director to determine that there were no system security incidents detected or reported during the specified period.	No exceptions noted.
LS-25	CC6.1 CC6.2 CC6.3 CC6.6 CC6.7 CC6.8	Access to the Network, BOLI application and related databases, and the Benefits Administration Application is removed or disabled within two business days of the employee's/contractor's termination date.	**Inspection:** Inspected the removal request for a sample of terminated employees/contractors with access to the network, BOLI application and related databases, and the Benefits Administration Application to determine that access to the network, BOLI application and related databases, and the Benefits Administration Application was removed within two business days of the employee's/contractor's termination date.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
LS-69	CC6.1 CC6.2 CC6.3 CC6.6 CC6.7 CC6.8	Non-Qualified, Qualified, RPS, and AGS: A tracking ticket to revoke access is automatically created when Human Resources approves an employee termination entered by a manager in the Workday application. Access is revoked within two business days following notification of termination from HR and is documented in a tracking ticket.	**Observation:** Observed the HR Director approve an employee termination within Workday to determine that a tracking ticket to revoke access was automatically created when Human Resources approved an employee termination entered by a manager in the Workday application.	No exceptions noted.
			Inspection: Inspected the termination ticket related to a sample of terminated employees to determine that each selected employee's access was removed within two business days of termination date and was documented in a tracking ticket.	No exceptions noted.
LS-70	CC6.2 CC6.3	On a periodic basis, Ascensus performs a review of access to the network, in-scope applications, and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.	**Inspection:** Inspected the access review documentation related to the network, Non-Qualified, Qualified, RPS and AGS applications and related databases to determine that user access, including associate and administrative accounts, was reviewed at least annually to ensure that access to the network, Non-Qualified, Qualified, RPS and AGS applications and related databases was appropriate and any identified access discrepancies were communicated and resolved.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
			Inspection: Inspected the Access Removal Tickets related to a sample of changes identified during the network, Non-Qualified, Qualified, RPS and AGS applications and related databases access reviews to determine that each selected user's access was removed as requested.	No exceptions noted.
			Inspection: Inspected the access review documentation related to a sample of quarters to determine that the Company performed a quarterly review of access to the BOLI Application, BOLI database, and the Benefit Administration Application for each selected quarter to help ensure that user access was appropriate. Further, inspected supporting review documentation and inquired of the SVP of Operations and Director Programing & Analysis to determine that no issues were identified as a result of the selected reviews; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
LS-71	CC5.2 CC6.1 CC6.6 CC6.8	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function.	**Inspection:** Inspected the listing of users with administrative access to the Qualified and Non-Qualified production applications and related databases and the corresponding job titles to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.
			Inspection: Inspected the listing of users with administrative access to the BOLI production applications and related databases and the corresponding job titles to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.
			Inspection: Inspected the listing of users with administrative access to the RPS production applications and related databases and the corresponding job titles to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.
			Inspection: Inspected the listing of users with administrative access to the AGS production applications and related databases and the corresponding job titles to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
LS-72	CC6.1	Password parameters for the in-scope applications are configured to require, at minimum: • Length of 8 characters • Complexity requirements	**Inspection:** Inspected password parameters for the Qualified and Non-Qualified applications to determine that passwords were configured to have a minimum length of 8 characters and complexity required.	No exceptions noted.
			Inspection: Inspected password parameters for the BOLI applications to determine that passwords were configured to have a minimum length of 8 characters and complexity required.	No exceptions noted.
			Inspection: Inspected password parameters for the RPS applications to determine that passwords were configured to have a minimum length of 8 characters and complexity required.	No exceptions noted.
			Inspection: Inspected password parameters for the AGS applications to determine that passwords were configured to have a minimum length of 8 characters and complexity required.	No exceptions noted.
LS-73	CC6.1	Password parameters for the network, operating systems, and databases related to the in-scope applications are configured to require, at minimum: • Length of 6 characters • Complexity requirements	**Inspection:** Inspected password parameters for the Qualified and Non-Qualified network, operating systems, and databases to determine that passwords were configured to have a minimum length of 6 characters and complexity required.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
			Inspection: Inspected password parameters for the BOLI network, operating systems, and databases to determine that passwords were configured to have a minimum length of 6 characters and complexity required.	No exceptions noted.
			Inspection: Inspected password parameters for the RPS network, operating systems, and databases to determine that passwords were configured to have a minimum length of 6 characters and complexity required.	No exceptions noted.
			Inspection: Inspected password parameters for the AGS network, operating systems, and databases to determine that passwords were configured to have a minimum length of 6 characters and complexity required.	No exceptions noted.
LS-74	CC6.1	External user account passwords for AGS must be changed upon initial login.	**Observation:** Observed the user registration process for the AGS applications to determine that user account passwords must be changed upon initial login.	No exceptions noted.
LS-75	CC5.2 CC6.1	Valid user IDs and passwords are required to access the network, in-scope applications, website and related databases.	**Observation:** Observed an internal user attempt to gain access to the network to determine that a valid user ID and password was required.	No exceptions noted.
			Observation: Observed an internal user attempt to gain access to the website to determine that a valid user ID and password was required.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
			Observation: Observed a user attempt to gain access to Qualified and Non-Qualified Services applications and related databases to determine that valid user IDs and passwords were required to access the Qualified and Non-Qualified Services applications and related databases.	No exceptions noted.
			Observation: Observed an internal user attempt to gain access to BOLI applications, websites, and related databases to determine that valid user IDs and passwords were required.	No exceptions noted.
			Observation: Observed an internal user attempt to gain access to the AGS applications, websites, and related databases to determine that valid user IDs and passwords were required.	No exceptions noted.
			Observation: Observed an internal user attempt to gain access to the RPS applications, websites, and related databases to determine that valid user IDs and passwords were required.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
LS-76	CC5.2 CC6.1 CC6.6 CC6.7 CC6.8	Administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers is restricted to appropriate individuals based on job function.	**Inspection:** Inspected the list of users with administrative access to the network, operating systems, and in-scope utilities, including access to firewalls and routers and the corresponding job titles for all users on the listing to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.
LS-77	CC6.1 CC6.2 CC6.3	Requests to add and or modify access to the network, in-scope applications, and the related databases and infrastructure are approved by a manager prior to access being granted.	**Inspection:** Inspected the access request tickets for a sample of requests to grant or modify access to the network, in-scope applications, related databases and infrastructure to determine that each selected access request was approved by a manager prior to access being granted.	No exceptions noted.
LS-78	CC6.1 CC6.7	Remote access to Ascensus's internal network is restricted through the use of secure VPN and multi-factor authentication.	**Observation:** Observed a user access the Ascensus internal network by logging successfully into VPN and confirming multi-factor authentication to determine that remote access to Ascensus's internal network required the use of VPN and multi-factor authentication.	No exceptions noted.
			Observation: Observed a user attempt to access the Ascensus internal network without logging into VPN and confirming multi-factor authentication to determine that access to Ascensus's internal network was restricted through the use of VPN and multi-factor authentication.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
LS-79	CC6.6	Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Ascensus environment.	**Inspection:** Inspected the Ascensus network diagram to determine that network devices were deployed to detect and prevent threats to the Ascensus environment.	No exceptions noted.
			Inspection: Inspected network device configurations to determine that Ascensus deployed and maintained network devices to detect and prevent threats to Ascensus's environment	No exceptions noted.
LS-80	CC6.1 CC6.8 CC8.1	Build standards are documented to provide consistency when building and implementing servers supporting the in-scope applications. Servers are approved by a member of the Infrastructure team prior to use in production.	**Inspection:** Inspected the Virtual Machine process document to determine that build standards were documented to provide consistency when building and implementing servers supporting the in-scope applications.	No exceptions noted.
			Inspection: Inspected the change ticket and supporting documentation related to a sample of new servers to determine that servers were approved by a member of the Infrastructure team prior to use in production.	No exceptions noted.
LS-81	CC6.2 CC6.3	Requests to add, modify, and/or remove AGS external user accounts must be completed by Production Support with approval documented in a tracking ticket.	**Inspection:** Inspected the access tracking ticket related to a sample of external access changes to determine that each selected change to access for external users was approved and documented in a tracking ticket and completed by a member of production support.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
LS-82	CC6.8	Antivirus is automatically deployed to workstations and company hosted servers related to the in-scope applications. Static machine learning and dynamic behavioral analysis are performed to protect against malware.	**Observation:** Observed the anti-virus software global configurations and a sample of one workstation and one server to determine that antivirus software was automatically deployed, and that static machine learning and dynamic behavioral analysis were performed to protect against malware for workstations and company hosted servers related to the in-scope applications.	No exceptions noted.
LS-83	CC6.8	The ability to install software on workstations and laptops is restricted to appropriate users based on job roles.	**Inspection:** Inspected the listing of users with the ability to install software on workstations and laptops and the corresponding job titles related to the users on the listing to determine that the ability to install software on workstations and laptops was restricted to appropriate users based on job roles.	No exceptions noted.
LS-84	CC6.7	All transmissions of electronic information from/to processing center are encrypted as the default setting over public networks via secure transmission protocols (e.g., HTTPS, SFTP, VPN, and TLS).	**Inspection:** Inspected the TLS certificates for the external networks to determine that all transmissions of electronic information from/to processing center were encrypted as the default setting over public networks via secure transmission protocols (e.g., HTTPS, SFTP, VPN, and TLS).	No exceptions noted.
LS-85	CC6.1 CC6.7	Multi-factor authentication is required to access servers and databases that support the AGS in-scope applications.	**Observation:** Observed the remote sign-in process for the AGS in-scope platform servers and databases to determine multi-factor authentication was required to access servers and databases that support the AGS in-scope applications.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
LS-86	CC6.1 CC6.8	Client data is logically segregated, and access is systematically restricted based on client organization.	**Inspection:** Inspected the database schema structures to determine that client data was logically segregated, and access was systematically restricted based on client organization.	No exceptions noted.
OTH-6	CC9.1	Ascensus maintains insurance coverages designed to insulate the organization from the effects of a large-scale loss event.	**Inspection:** Inspected the active insurance policy to determine that Ascensus maintained insurance coverage designed to insulate the organization from the effects of a large-scale loss event.	No exceptions noted.
PP-35	CC1.1 CC1.4 CC2.2	On an annual basis, Ascensus communicates the code of conduct, security policies and practices, and procedures for submitting complaints and/or unethical behavior to Ascensus personnel. On an annual basis, Ascensus personnel must complete Annual Security Awareness Training confirm their understanding of and compliance with the Ascensus's code of conduct and security policies.	**Inspection:** Inspected the Ascensus Security Awareness Training Subjects, the Associate Handbook, and Policy Manual to determine that, on an annual basis, Ascensus communicated the code of conduct, security policies and practices, and procedures for submitting complaints and/or unethical behavior to Ascensus personnel.	No exceptions noted.
			Inspection: Inspected the results of the annual security awareness training for a sample of employees to determine that employees confirmed their understanding of and compliance with Ascensus's code of conduct and security policies, on an annual basis.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
PP-36	CC1.4	Before starting, each employee and contractor is subjected to a background check in accordance with the Ascensus hiring procedures.	**Inspection:** Inspected background checks related to a sample of new employees and contractors to determine each new hire was subjected to a background check in accordance with the Ascensus hiring procedures.	No exceptions noted.
			Inspection: Inspected the Background Check Process Document to determine that Ascensus had hiring procedures in place related to background checks for employees and contractors.	No exceptions noted.
PP-37	CC1.1 CC1.4 CC2.2	Within 30 days of hire date, new employees and contractors must sign a non-disclosure agreement that indicates they understand the confidential nature of the data that they will interact with, and they also electronically acknowledge that they are aware of and bound to follow the information security policies and the Company's code of conduct as outlined in the Company's Policy Manual and the Code of Conduct Handbook.	**Inspection:** Inspected new hire acknowledgements for a sample of new employees and contractors to determine that, within 30 days of hire, each new employees and contractor signed a non-disclosure agreement and electronically acknowledged information security policies and the Company's code of conduct as outlined in the Company's Policy Manual and the Code of Conduct Handbook.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
PP-38	CC1.1 CC1.4 CC1.5 CC5.3	On an annual basis, performance reviews are completed as part of the employee compensation review process to help ensure that each employee's skill set matches his/her job responsibilities.	**Inspection:** Inspected the performance review completion date for a sample of employees to determine that at least annually, each selected employee had their performance review completed as part of the employee compensation review process to help ensure that each employee's skill set matched his/her job responsibilities.	No exceptions noted.
PP-39	CC1.1 CC1.3 CC1.4 CC1.5 CC2.1 CC2.2 CC3.1 CC3.4 CC5.1 CC5.3	Information security policies are maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.	**Inspection:** Inspected the Ascensus organizational charts and the Associate Handbook and Policy Manual to determine that information security policies were maintained that document organizational structures, reporting lines, authorities, and responsibilities related to the design, development, implementation, operation, maintenance, and monitoring of Ascensus's systems.	No exceptions noted.
PP-40	CC1.1 CC1.3 CC1.4 CC1.5 CC2.1 CC2.2 CC3.1 CC3.4 CC5.1 CC5.3	The Company maintains a Policy Manual Ownership Index that identifies ownership of key security, compliance, data management, and third-party risk management policies. Further, each key policy is reviewed annually within the Ascensus Policy Manual and updated as appropriate.	**Inspection:** Inspected the Policy Ownership Index to determine that the Company maintained a Policy Manual Ownership Index that identified ownership of key security, compliance, data management, and third-party risk management policies.	No exceptions noted.
			Inspection: Inspected the Ascensus Policy Manual to determine that key policies were reviewed annually and updated as appropriate.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
PP-41	CC1.1 CC1.3 CC1.4 CC1.5 CC2.1 CC2.2 CC3.1 CC5.3	Ascensus has written job descriptions specifying the responsibilities of and professional requirements for job positions.	**Inspection:** Inspected the job profile overview for a sample of job descriptions to determine that each selected job description included the job responsibilities and the professional requirements for job positions.	No exceptions noted.
PP-42	CC1.3 CC2.2 CC2.3 CC5.3	The Company has a documented and published organizational structure which is available to internal users via the Company's intranet.	**Inspection:** Inspected the organizational chart available on the intranet to determine that Ascensus had a documented and published organizational structure which was available to internal users via the intranet.	No exceptions noted.
PP-43	CC1.2 CC9.1	Ascensus has an independent Board of Directors that meets quarterly to oversee the control environment, allocate resources to key security functions, review key risks impacting organizational objectives and corporate culture, and authorize consulting resources as needed.	**Inspection:** Inspected the Board of Directors quarterly meeting agenda for a sample of quarters to determine that the Board of Directors met during each selected quarter to oversee the control environment, allocate resources to key security functions, review key risks impacting organizational objectives and corporate culture, and authorize consulting resources as needed.	No exceptions noted.
PP-44	CC2.2 CC2.3	Ascensus has provided a description of the in-scope applications and its services, including applicable information related to the boundaries of the System and its processing integrity, on internal repositories and are accessible as needed.	**Inspection:** Inspected the Ascensus intranet to determine that Ascensus provided a description of the in-scope applications and services, including applicable information related to the boundaries of the System and its processing integrity, on internal repositories that were accessible as needed.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
PP-45	CC1.2	The Ascensus Security Council (ASC) is a cross-functional committee that meets on a monthly basis to review potential security-related issues or concerns.	**Inspection:** Inspected the ASC meeting minutes and list attendees related to a sample of months to determine that the Ascensus Security Council (ASC) was a cross-functional committee, and for each selected month, the council met to review potential security-related issues or concerns.	No exceptions noted.
PP-46	CC1.3 CC2.2 CC2.3 CC5.3	A CISO role is maintained and is responsible for changes to security practices and commitments. A formal process is documented to communicate these changes and is made available to applicable internal and external users, related parties, and vendors.	**Inspection:** Inspected the CISO job description to determine that the role was maintained and was responsible for changes to security practices and commitments.	No exceptions noted.
			Inspection: Inspected the Ascensus Policy Manual available on the Company's intranet and the Ascensus Security Overview available on the client portal to determine that a formal process was documented to communicate these changes and was made available to applicable internal and external users, related parties, and vendors.	No exceptions noted.
PP-47	CC1.2	Ascensus has reporting mechanisms for associates in place for reporting operational failures, security incidents, problems, and compliance concerns through an anonymous hotline, and both identified and anonymous reporting mechanisms are available. This anonymous hotline is communicated to all stakeholders via the Policy Manual.	**Inspection:** Inspected the Associate Policy and Handbook Manual to determine that Ascensus had reporting mechanisms for associates in place for reporting operational failures, security incidents, problems, and compliance concerns through an anonymous hotline, and both identified and anonymous reporting mechanisms were available and communicated.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
PS-1	CC6.4	Security badge access requests are approved by Management prior to access being granted.	**Inspection:** Inspected the corresponding tracking tickets and supporting documents for a sample of new users granted physical access to secure areas at the Newton, MA and Kansas City, MO locations to determine that, for each selected new user granted physical access to secure areas, the corresponding tracking tickets were authorized by management.	No exceptions noted.
PS-10	CC6.4	The ability to implement changes to physical access rights to sensitive areas and locations is limited to authorized system administrators to prevent unauthorized changes.	**Inspection:** Inspected the listing of users with the ability to implement changes to physical access rights and the corresponding job titles related to the users on the listing to determine that the ability to implement changes to physical access rights to sensitive areas and locations was limited to authorized system administrators to prevent unauthorized changes.	No exceptions noted.
PS-11	CC6.4	Terminated employee or contractor physical access to sensitive areas and locations is revoked automatically when Active Directory account is disabled or upon notification from the manager of the terminated associate or contractor.	**Inspection:** Inspected the termination ticket for a sample of terminated employees and contractors to determine that access to sensitive areas and locations was revoked automatically when Active Directory account was disabled or upon notification from the manager of the terminated associate or contractor.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
PS-12	CC6.4	On a semi-annual basis, physical access to sensitive areas and locations is reviewed by management to validate that employee access is commensurate with job responsibilities. Any issues identified are researched and resolved.	**Inspection:** Inspected the semi-annual physical access review and supporting documentation to determine that physical access to sensitive areas and locations was reviewed by management to validate employee access was commensurate with job responsibilities and that any issues identified were researched and resolved.	No exceptions noted.
PS-13	CC6.4	All external access points to sensitive areas and locations are controlled through an electronic key-card system or restricted to emergency exit only. Key-card access is limited to appropriate individuals.	**Observation:** Observed the external access points to the Newton, MA and Kansas City, MO secure locations to determine that access was restricted via electronic key-card system or restricted to emergency exit only.	No exceptions noted.
			Inspection: Inspected the listing of users with key-card access to sensitive areas and locations and the corresponding job titles related to the users on the listing to determine that access was limited to appropriate individuals.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
RA-6	CC2.1 CC3.1 CC3.2 CC3.3 CC3.4 CC5.1 CC9.1 CC9.2	On an annual basis, Ascensus performs a risk assessment that includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services). As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.	**Inspection:** Inspected the annual risk assessments to determine that Ascensus performed a risk assessment that included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services); and that these threats were formally assessed, and mitigation strategies were documented and revised as needed.	No exceptions noted.
RA-7	CC2.1 CC3.1 CC3.2 CC3.3 CC3.4 CC5.1 CC9.1 CC9.2	On a monthly basis, risk and control meetings are held to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.	**Inspection:** Inspected retirement risk and control meeting agendas for a sample of months to determine that risk and control meetings were held during each selected month to help identify potential sources of fraud and identify processes to effectively address identified fraud risks.	No exceptions noted.

Control ID	Associated Criteria	Control Activity Description	Tests Performed by Service Auditor	Results of Testing
TPM-6	CC1.3 CC3.2 CC3.4 CC9.2	Ascensus has an established Vendor Management Program to review and evaluate third-party relationships and ensure that vendors are adhering to contractual service delivery requirements and information security obligations.	**Inspection:** Inspected the Ascensus Vendor Compliance Program overview to determine that Ascensus had an established Vendor Management Program to review and evaluate third-party relationships and ensure that vendors were adhering to contractual service delivery requirements and information security obligations.	No exceptions noted.
			Inspection: Inspected the status of the vendor questionnaire for a sample of vendors to determine that a vendor questionnaire was completed by each selected vendor annually to help ensure that vendors were adhering to contractual service delivery requirements and information security obligations.	No exceptions noted.
TPM-7	CC1.3 CC3.2 CC9.2	Acceptable use and limits of use for user entities and external third parties (including vendors and SSOs) are documented within the standard contract template.	**Inspection:** Inspected the Ascensus contract template for user entities and external third parties to determine that the contract templates included acceptable use and limits of use clauses.	No exceptions noted.

V. Other Information Provided by Ascensus, LLC; Ascensus College Savings Recordkeeping Services, LLC; Ascensus Broker Dealer Services, LLC; and Newport Group, Inc.

The information in this section is presented by the Company to provide additional information to its user entities, business partners, and other specified parties and is not part of the Company's description of its system and controls included in Section III. The information in Section A, "SPARK Data Security Control Objectives" has not been subjected to the procedures applied in the examination of the description of the Company's Retirement and Government Savings Systems and suitability of design and operating effectiveness of controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, and accordingly, Grant Thornton LLP expresses no opinion on it.

A. SPARK Data Security Control Objectives

In 2017, the SPARK Institute, a Retirement Industry consortium, announced the development of new Industry Best Practices for how recordkeepers should report their cyber-security capabilities to plan sponsors and plan consultants.

The following summary of Ascensus's compliance with this standard applies to the Ascensus Retirement business only.

In order to comply with the new Industry Best Practices, the SPARK Institute formed a Data Security Oversight Board (DSOB), comprising recordkeepers and members of the plan consultant community. The DSOB determined that when a member firm, such as Ascensus, uses SPARK's Industry Best Practices to describe their overall data security capabilities, they should use the 17 identified critical data security control objectives defined by the DSOB and that a review should be performed by an independent third party.

Ascensus's compliance with this SPARK standard is detailed below in the mapping of the existing SOC 2 controls to the 17 SPARK control objectives:

	SPARK Control Objective	Description	Criteria in SOC 2
1	Risk Assessment and Treatment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals.	CC 1.0 CC 3.0
2	Security Policy	Organizational information security policy is established.	CC 1.0 CC 2.0 CC 3.0 CC 5.0
3	Corporate / Organizational Security	Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.	CC 1.0 CC 2.0 CC 3.0 CC 5.0
4	Asset Management	The data, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed.	CC 3.0 CC 4.0 CC 5.0 CC 6.0 CC 8.0
5	Human Resource Security	The organization's personnel and partners are suitable for the roles they are considered for, are provided cybersecurity awareness education, and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	CC 1.0 CC 2.0 CC 3.0
6	Physical and Environmental Security	Physical access to assets is managed and protected.	CC 6.0
7	Communications and Operations Management	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	CC 5.0 CC 6.0 CC 7.0

	SPARK Control Objective	Description	Criteria in SOC 2
8	Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	CC 6.0
9	Information Systems Acquisition Development	An SDLC to manage systems is implemented, a vulnerability management plan is developed and implemented, and vulnerability scans are performed.	CC 8.0
10	Incident and Event Communications Management	Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events.	CC 2.0 CC 7.0 CC 9.0
11	Operational Business Resiliency	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and DR) are in place and managed.	CC 7.0 CC 9.0
12	Compliance	Legal requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	CC 2.0 CC 3.0 CC 4.0
13	Mobile	A formal policy is in place and appropriate security measures have been adopted to protect against the risks of using mobile computing and communication facilities.	CC 6.0
14	Encryption	Data-at-rest and data-in-transit are protected.	CC 6.0
15	Supplier Risk	The organization ensures protection of its assets that are accessible by suppliers.	CC 1.0 CC 3.0 CC 4.0

	SPARK Control Objective	Description	Criteria in SOC 2
16	Cloud Security	The organization ensures protection of its assets that are stored or processed in cloud environments.	N/A – The use of cloud technologies is not applicable as the services that are the subject of this section is strictly limited to the Ascensus Retirement business only, and the related service requirements, commitments, and obligations, do not rely upon the use of cloud environments.
17	Ransomware	Processes and controls are in place to detect and respond to ransomware events.	CC 1.0 CC 3.0 CC 4.0 CC 6.0 CC 7.0



© Grant Thornton LLP
All rights reserved.
A U.S. member firm of Grant Thornton International Ltd.

This report is confidential. Unauthorized use of this report in whole or in part is strictly prohibited.

Ascensus® and the Ascensus logo are registered trademarks of Ascensus, LLC.



Report on the Description of the Transaction Processing System and the Suitability of the Design and Operating Effectiveness of Controls for Qualified Plan Services and Individual Retirement Arrangements

SOC 1 Type 2 Examination
For the Period October 1, 2024
Through September 30, 2025

Ascensus Trust Company

Qualified Plan Services and
Individual Retirement Arrangements



Section I – Independent Service Auditor's Report 1

Section II – Managements Assertion Provided by Ascensus Trust Company 5

Section III – Description of Transaction Processing System for Qualified Plan Services and Individual Retirement Arrangements 7

- Complementary Subservice Organization Controls (CSOC) 15
- Complementary User Entity Controls 18

Section IV – Control Objectives and Related Controls, Tests of Operating Effectiveness and Results of Tests Provided by the Independent Service Auditor and Ascensus Trust Company 21

- Account Set-up and Maintenance – Qualified Plan Services 23
- Account Set-up and Maintenance – Individual Retirement Accounts 23
- Account Set-up and Maintenance- Individual Retirement Accounts 25
- Account Fees and Maintenance – Qualified Plan Services 26
- Account Fees and Maintenance – Individual Retirement Accounts 27
- Keying/Processing of Investment Transactions – Qualified Plan Services 29
- Keying/Processing of Investment Transactions – Individual Retirement Accounts 29
- Keying/Processing of Investment Transactions – Qualified Plan Services 31
- Keying/Processing of Investment Transactions – Qualified Plan Services 32
- Keying/Processing of Investment Transactions – Qualified Plan Services 33
- Keying/Processing of Distribution Transactions – Qualified Plan Services 34
- Keying/Processing of Distribution Transactions – Qualified Plan Services 35
- Keying/Processing of Distribution Transactions – Qualified Plan Services 36
- Keying/Processing of Distribution Transactions – Individual Retirement Accounts 37
- Keying/Processing of Distribution Transactions – Individual Retirement Accounts 39
- Reconciliations 41
- State Tax Filings and Withholdings 42
- Federal Tax Filings and Withholdings 43
- Organization and Administration 44
- Application Development 45
- Risk Management 47
- Security Controls to the Computer Facilities 49

Section V – Other Information Provided by Ascensus Trust Company 50

- Ascensus Trust Company Business Continuity Planning 50

Section I

Independent Service Auditor's Report

Independent Service Auditor's Report

The Board of Directors
Ascensus Trust Company
Fargo, North Dakota

Scope

We have examined management of Ascensus Trust Company's description of its Transaction Processing System for processing user entities' transactions for Qualified Plan Services and Individual Retirement Arrangements throughout the period October 1, 2024 to September 30, 2025 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in management of Ascensus Trust Company's Assertion (assertion). The controls and control objectives included in the description are those that management of Ascensus Trust Company believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Transaction Processing System that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section V, "Other Information Provided by Ascensus Trust Company," is presented by management of Ascensus Trust Company to provide additional information and is not a part of Ascensus Trust Company's description of its Transaction Processing System for processing user entities' transactions for Qualified Plan Services and Individual Retirement Arrangements made available to user entities during the period October 1, 2024 to September 30, 2025. Information about Ascensus Trust Company's business continuity planning has not been subjected to the procedures applied in the examination of the description of the Transaction Processing System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Transaction Processing System and, accordingly, we express no opinion on it.

Ascensus Trust Company uses a subservice organization for qualified and individual retirement plan setup, ongoing plan maintenance, fee administration, and IT general controls including physical security, logical access, disaster recovery and backups, network administration, application development, and environment controls related to the data center. The description includes only the control objectives and related controls of Ascensus Trust Company and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Ascensus Trust Company can be achieved only if complementary subservice organization controls assumed in the design of Ascensus Trust Company's controls are suitably designed and operating effectively, along with the related controls at Ascensus Trust Company. Our examination did not extend to controls of the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

eidebailly.com
4310 17th Ave. S. • P.O. Box 2545 • Fargo, ND 58108-2545 • **T** 701.239.8500 • **F** 701.239.8600 • EOE

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Ascensus Trust Company's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section II, management of Ascensus Trust Company has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Ascensus Trust Company is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2024 to September 30, 2025. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related objectives stated in the description, based on the criteria referenced previously;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved;
- Evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in section IV of our report titled "Control Objectives and Related Controls, Tests of Operating Effectiveness and Results of Tests Provided by the Independent Service Auditor and Ascensus Trust Company."

Opinion

In our opinion, in all material respects, based on the criteria described in management of Ascensus Trust Company's assertion:

a. The description fairly presents the Transaction Processing System that was designed and implemented throughout the period October 1, 2024 to September 30, 2025.
b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2024 to September 30, 2025, and the subservice organization and user entities applied the complementary controls assumed in the design of Ascensus Trust Company's controls throughout the period October 1, 2024 to September 30, 2025.
c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2024 to September 30, 2025, if complementary subservice organization and user entity controls assumed in the design of Ascensus Trust Company's controls operated effectively throughout the period October 1, 2024 to September 30, 2025.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV is intended solely for the information and use of management of Ascensus Trust Company, user entities of Ascensus Trust Company's Transaction Processing System during some or all of the period October 1, 2024 to September 30, 2025, and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.



Fargo, North Dakota
December 15, 2025

Section II

Management's Assertion Provided by

Ascensus Trust Company

Ascensus Trust Company's Assertion

We have prepared the description of Ascensus Trust Company's Transaction Processing System for processing user entities' transactions for Qualified Plan Services and Individual Retirement Arrangements throughout the period October 1, 2024 to September 30, 2025 (description) for user entities of the system during some or all of the period October 1, 2024 to September 30, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities, when assessing the risks of material misstatements of user entities' financial statements.

Ascensus Trust Company uses a subservice organization for qualified and individual retirement plan setup, ongoing plan maintenance, fee administration, and IT general controls including physical security, logical access, disaster recovery and backups, network administration, application development, and environment controls related to the data center. The description includes only the control objectives and related controls of Ascensus Trust Company and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Ascensus Trust Company's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

1. The description fairly presents the Transaction Processing System made available to user entities of the system during some or all of the period October 1, 2024 to September 30, 2025 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description.
    a. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:
        i. The types of services provided including, as appropriate, the classes of transactions processed.
        ii. The procedures, within both automated and manual systems, by which those services are provided, including as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

iii. The information used in the performance of the procedures, including, if applicable, related accounting records, when electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
iv. How the system captures and addresses significant events and conditions other than transactions.
v. The process used to prepare reports and other information for user entities.
vi. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
vii. The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.
viii. Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b. Includes relevant details of changes to the service organization's system during the period covered by the description.
c. Does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Transaction Processing System that each individual user entity of the system and its auditor may consider important in its own particular environment.

2. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2024 to September 30, 2025 to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of Ascensus Trust Company's controls throughout the period October 1, 2024 to September 30, 2025. The criteria we used in making this assertion were that:
   a. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization;
   b. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
   c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section III

Description of Transaction Processing System
for Qualified Plan Services and
Individual Retirement Arrangements

Ascensus Trust Company

General Description of the Organization

Ascensus Trust Company (ATC) is principally involved in processing the investment of contributions and the payment of distributions for Qualified Plan Clients (Clients) through "alliance" arrangements with third-party recordkeepers and investment providers. In these alliances, ATC receives instructions from a recordkeeper and processes data for the investment provider to properly invest Clients' funds and process distributions.

ATC provides services for Individual Retirement Arrangements (IRAs), SEP and SIMPLE IRA's and a force out IRA product. The services provided include setting up new IRAs, accepting contributions and processing distributions for IRA owners.

ATC also provides fiduciary services for irrevocable and rabbi trusts.

This report has been prepared to provide information on ATC's controls that may be relevant to ATC's Qualified Plan Services and IRAs processing activities. As a result, this report is not intended to address controls that may be relevant to other clients of ATC (i.e., irrevocable and rabbi trusts, state facilitated retirement plan IRA's).

Control Environment

Management Controls and Organizational Structure

ATC's control environment reflects the overall attitude, awareness and actions of management, the Board of Directors, and committees concerning the importance of controls and the emphasis given to controls in its policies, procedures and organizational structure. ATC's control environment includes, among other things, policy and procedural guidelines which are reviewed and updated on an ongoing basis and provide guidance by which administrative and client reporting activities are conducted. In addition, formal information and reporting systems exist which permit monitoring by management of key control and performance measurements.

Management reviews operational and financial information on a regularly scheduled basis. Financial information is prepared monthly; detailed reconciliations are prepared daily and monthly.

Board of Directors

The Board of Directors oversees ATC's activities. The Board, as a whole, functions as the Audit Committee and a Trust Committee to oversee ATC's activities. The Board is charged with monitoring the activities under its oversight.

Personnel Policies and Procedures

Training of personnel is accomplished through supervised on-the-job training.

Assignment of Authority and Accountability

The assignment of authority and responsibility within ATC includes establishing relationships and authorization levels necessary to execute specific business decisions and objectives. ATC's Qualified and Individual Retirement Plans processing activities are conducted in accordance with established procedure manuals and checklists. The responsibilities are allocated among personnel so as to segregate the following functions:

- Account set-up and maintenance
- Keying/processing of investment transactions
- Keying/processing of distribution transactions
- Tax filings
- Information systems environment

Operating and financial reconciliations are subject to review by supervisory personnel.

Risk Assessment

An entity's risk assessment is its identification, analysis, and management of risks relevant to the preparation of its financial statements and to user organizations. ATC recognizes that risk management is a critical component of its operations that helps to ensure corporate assets are properly managed and user organizations are properly served. ATC management has incorporated risk management throughout its processes at both the corporate and business unit levels. The management of each business unit is responsible for implementing procedures to identify the risks inherent in the unit's operations and implement procedures to monitor and mitigate the risks. The foundation of this process is management's knowledge of its operations, its close working relationship with its user organizations, and its understanding of the industries in which it operates. For any significant risks identified, management is responsible for implementing appropriate measures to monitor and manage these risks.

Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achieve the entity's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in conditions. Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities.

Information and Communication

Information and communication systems support the identification, capture, and exchange of information in a form and timeframe that enable associates to carry out their responsibilities. The information system consists of the procedures, whether automated or manual, and records established to initiate, record, process, and report entity transactions to maintain accountability. The quality of system generated information affects management's ability to make appropriate decisions in controlling the entity's activities and to prepare reliable financial reports.

Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting. Communication systems exist from the entity-level to the department-level. Multiple communication paths exist to help ensure that processes function as designed and issues are identified and resolved in a timely manner. These include voice mail, email, instant message and regularly scheduled meetings and teleconferences.

Reporting Provided to User Entities

The service agreements with user entities provide for reporting that is in scope of the controls in the system description. The reporting is based on the type of service provided (i.e., Qualified Plan or IRA). For Qualified Plans this includes required tax filings and information. For IRA's this includes quarterly statements, fair market value statements, required minimum distribution (RMD) notification, and tax filing information.

Other Considerations

ATC is subject to regulation by the North Dakota Department of Financial Institutions (NDDFI).

ATC'S financial statements are audited by an independent auditor.

Scope of Report

The report and system description cover transaction processing for qualified plans and IRAs. Ascensus, LLC is a carved-out subservice organization related to IRA and Qualified plan setup, ongoing plan maintenance, fee administration, and General IT controls. The systems in scope of the report are Trust Services, an internal support system designed specifically for qualified and IRA plans trust processing, and ARK, a Recordkeeping platform, and other ancillary systems.

Account Set-up and Maintenance - Qualified Plan Services

There are two methods to establish a new client in ATC's system. One method is that Ascensus, LLC (Ascensus), ATC's parent company, assigns the new client a client number and this information is included in the daily download from Ascensus and is imported by ATC. The account setup forms can also be obtained directly from the recordkeeper. A client number is assigned to these plans when the documents are received. The last step in the client account set up process is complete when the required documentation is received at ATC and an Office of Foreign Asset Control (OFAC) review is completed to verify the individual or company is not included on the OFAC list. An ATC employee searches the Ascensus imaging system for completed agreements. When an agreement is received, the agreement is reviewed for completeness. When the agreement is complete, the agreement information is entered into the system and the plan is considered fully set up. Certain clients have agreements on a Source level or mass conversion and are, therefore, automatically considered fully set up.

An ATC employee bills annual fees quarterly and in accordance with the ATC fee schedule. The employee in charge of billing is not allowed to approve the fee account reconciliations.

Account Set-up and Maintenance - IRAs

The IRA department receives requests to add new IRA participants for each of the IRA products. The process to add a new IRA participant is different for each of the IRA product types.

ATC Force Out IRAs do not require signed IRA applications at the time of account establishment as these are opened by the plan sponsor. Each plan sponsor signs an IRA Service Agreement with ATC that allows the plan sponsor to open IRA accounts on their participants' behalf. Customer Identification Program (CIP) is performed at the time the IRA owner returns the IRA Acceptance Agreement, initiates their first withdrawal request or transacts on the participant website.

The IRA and ATC SEP/SIMPLE IRA products require applications be sent in for any new IRA participants. The only new accounts are SEP/SIMPLE IRAs. IRA application(s) are retained electronically in CLIFF. Applications are worked through several stages of processing inside of IMPACT and/or Chorus and IRA Services. Some Plan Sponsors also have the ability to add participants via the Sponsor Website. If a Plan Sponsor adds the participant directly, an IRA associate will follow up with the plan until an application is received. If ATC is unable to obtain an application signed by the IRA owner, the Plan Sponsor is able to sign on their employee's behalf.

Account changes can originate as a result of the IRA holder calling into the IRA Service Center, a form being received or notification from the post office. All calls are recorded and retained for 7 years. Any form received by the IRA department is retained through CLIFF, Chorus, daily backup, or Web Comments.

Before any personal account information can be provided to a caller or be updated in our system the information provided (Social Security Number (SSN), Date of Birth (DOB) and address of record) must be verified against the information in the Ascensus recordkeeping system (ARK) and/or IRA Services. If the IRA associate is able to establish that the person is who they say they are, an address update can be made. If there is a discrepancy with the DOB or SSN, additional verification or documentation may be required prior to the update being made.

Account fees vary by product and are disclosed to the IRA holders via Financial Disclosures which are part of the Force Out Welcome Packet and the SEP/SIMPLE IRA Employee Kits. New ATC Forceout quarterly fees are taken shortly after account opening and then again, every quarter thereafter. The employee in charge of billing is not allowed to approve the fee account reconciliations. ATC also sends withholding notices for IRA plans semi-annually And SIMPLE notices to active plans annually.

Keying/Processing of Investment Transactions - Qualified Plan Services

ATC processes Client contributions for Qualified Plans. Third party recordkeepers do all the participant recordkeeping for the Qualified Plans and provide contribution processing and investment instructions to ATC. Most Client contribution data is imported on a composite report from a third party recordkeeper sent via an electronic transfer process that is initiated by the recordkeeper. The composite report details the amount of funds to be invested for each Client and the investment provider to which the funds are to be remitted.

Contribution checks are received in a secure mailroom at ATC via USPS and Express mail and given to an ATC associate for processing. An ATC associate keys the deposit information daily. The manually keyed amount is also independently verified by another ATC associate. If exceptions to the contribution balances are discovered, they are investigated and cleared before the check can be deposited.

Incoming wire transfers are initiated by the client and the amounts are entered manually by an employee. The cash amount and the amount to post to each account must be equal. A second employee verifies the data and agrees the total dollar amount, client number and other information.

The recordkeepers final investment file is imported into the ATC system to review the availability of funding for the trades that will need settlement the following day. Finalized trade amounts are confirmed with Investment partners prior to funds being sent for trading. Daily settlement reports for each trading partner’s net trades are reconciled to the days bank activity. Any differences are monitored or investigated for resolution and resolved within the same day. Daily bank reconciliations are prepared and reviewed for the contribution and distribution accounts. Monthly reviews are performed of the reconciled bank balances.

Recurring wire transfers are prepared to settle the trades that were the result of investment file processing from the previous night. Templates are created for recurring wire transfers based on instructions received from the third parties. An employee enters the amounts and the code for each trading partner or settlement entity based off the reports prepared from the investment file processing reports. A second employee verifies the wire transfers.

ATC determines that each Client has available funds to complete the investment transactions per the composite report by daily reconciliations. All reconciliations are reviewed by an independent employee on a monthly basis. The composite report is adjusted for any special requests and for any contribution funds that were not received by ATC. If the Client has an adequate balance by money type to complete the investment transactions per the composite report, a wire transfer request is completed and electronically communicated to the bank for the next day settlement of the trades. The bank's wire codes are preprogrammed. If any wire instructions are other than those preprogrammed, the wire is verified by another ATC employee. Authorization for nonrecurring wire transfers to an investment provider is received from an approved third party.

Wire transfer instructions for sending trade settlement to Investment Providers from the ATC account are prepared and verified. Wire transfer instructions are submitted electronically.

Client funds for which investment instructions have not yet been received are invested in a group trust which earns a rate comparable to a money market rate. Interest earned on the group trust may be allocated to the Clients or ATC as part of their trust/custodial agreement through system calculations, which are reviewed on a monthly basis. The collective fund account is audited annually by an independent auditor.

Keying/Processing of Investment Transactions - IRAs

IRA contribution checks are given to the IRA department. The instruction as well as the processing of contribution checks is different for each of the IRA products. ATC Forceouts typically require an excel spreadsheet that contains all of the necessary instructions for investment. The IRA and ATC SEP/SIMPLE products require a Contribution Investment form (or some form or documentation in writing). If all information is not received, a call may be made to obtain the necessary information on a recorded line. However, the majority of the ATC SEP/SIMPLE plans process their own contributions via the plan website and do not require processing from the IRA department, other than depositing the check. Any contributions keyed by an IRA associate are verified by another IRA associate. The contribution form/backup is scanned and retained in Chorus or IRA backup.

Keying/Processing of Distribution Transactions - Qualified Plan Services

ATC facilitates distributions for Clients in response to instructions from third-party recordkeepers and the receipt of funds from the investment provider or National Securities Clearing Corporation (NSCC). The third-party recordkeepers process all distribution requests from the Clients and participants and calculates the proper liquidation amounts. ATC imports this data via electronic transfer. The investment provider receives trade files from the third-party recordkeepers. Special instructions are keyed by an ATC associate and are independently verified by another associate.

Distribution funds are received directly by ATC from the investment provider or NSCC net settlement to the ATC contribution account or are sent by check. Physical checks are received by ATC mailroom personnel and are restrictively endorsed. An electronic file of the amounts of the incoming funds is imported electronically into the system and a report is created of all distribution data, including cash availability, and matching electronic notification from the recordkeeper. Electronic transfer of distribution requests from and/or to the third party recordkeeper is completed using secured internal network drives. An OFAC screening is performed on all pending checks and wire transfers before the transactions are processed. The computer system will generate a check trial balance, including the associated tax withholdings, which independent ATC personnel verify. After totals are verified, the checks are printed and forwarded to the plan administrator for distribution to the plan participants or are sent directly to the participant, or third party, by ATC if ATC is instructed to do so directly by the recordkeeper. Distributions that are sent by wire or ACH are also created at this time.

The distribution account is reconciled on a daily basis. The preparer and reviewer of the reconciliation are separate. ATC tracks funds received for which they have yet to receive distribution instructions. ATC also tracks the instructions received for which no funds have been received. Exception listings are provided to third party recordkeeper that provide the distribution request. The Pending Check/Check History Audit Log is printed and reviewed daily. The Outgoing Wire Audit Log is printed and reviewed daily.

Terminating Clients are required to provide a corporate resolution that is notarized or has the corporate seal affixed to ATC when ATC is the trustee. Terminating clients may provide a letter from the plan sponsor and successor trustee in lieu of a corporate resolution. If ATC is custodian, a corporate resolution is not needed. Uninvested cash is forwarded to the successor trustee or custodian and securities could be registered under the successor party. Activity reports are reviewed for terminating Clients to verify the cash and investment balances of the terminating plan to ensure the Client receives the correct amount.

Keying/Processing of Distribution Transactions IRAs - Paper IRA Distributions

All of the ATC IRA products require a distribution form to be completed. Each IRA product may have additional requirements (i.e., driver's license, passport, or notary) that need to be submitted along with the withdrawal form. IRA holders do have the option to set up recurring payments on a monthly, quarterly, semiannually, or annual basis where subsequent forms would not be necessary unless a one-time distribution is requested. IRA withdrawal forms are retained via CLIFF, Chorus or in IRA backup and distributions are processed within 7 business days of receipt of request.

The Transmission report is run and compared to the IRA withdrawal forms in Chorus. Corrections can be made within ARK and would need to be reviewed when the Transmission report is rerun.

Upon approval, the process is moved to and becomes part of the distribution department process. The process is the same whether it is a qualified plan or an IRA.

Keying/Processing of Distribution Transactions IRAs - Online IRA distributions

During the period, there was a significant change in the distribution allocation (electronic vs paper form request), with a large increase in the mix of electronically requested distributions compared to paper-based distributions. This shift necessitated the identification and evaluation of the controls implemented to govern the electronic distribution process.

For electronically initiated IRA distributions a system verification of online distributions occurs to review any items that require manual adjustment prior to the distribution. All manual adjustments require an independent review prior to processing the distribution. An audit log is also maintained to track all changes made to online distribution instructions. Distributions requests must undergo customer identification program (CIP) processes and any discrepancies in data are resolved prior to the distribution. Distributions are to be processed within 7 business days of the receipt of the online withdrawal request and will be processed in accordance with the online distribution instructions.

Keying/Processing of Distribution Transactions IRAs

IRA account holders are required to take an RMD from their IRA by April 1 of the year following the year they reach the required age and by the end of each year thereafter. A notice is sent to each IRA holder in January notifying them of their RMD amount. It is the IRA owner's responsibility to satisfy their RMD. ATC does not automatically process RMD's as RMDs can be satisfied from any IRA that is held by the IRA holder.

Based on IRS rules, if the IRA owner does not reply, Ascensus is not required to distribute the RMD. Ascensus is only required to communicate the amount of the RMD. The IRA owner can also take the RMD out of another IRA account that is not held at ATC to satisfy their requirement.

Reconciliations

The bank accounts used for distributions and contributions are reconciled daily and reviewed monthly by ATC personnel. The reconciliations are reviewed by an independent employee.

State and Federal Tax Filings and Withholdings

The respective federal tax withholdings are submitted to the federal tax authorities electronically. State tax withholdings are submitted to the state tax authorities using electronic filing or appropriate forms. An independent ATC employee reviews the tax payments. An IRS confirmation is obtained for all electronic federal tax payments and scanned into the system. If necessary, 1099s and 5498s are prepared. Quarterly and annual state tax reports are filed at the appropriate time.

Form 5498 is only prepared for IRA account holders that contributed to their IRA for the tax year being reported to the IRS. While the form allows for the reporting of the IRA market value, ATC has elected to communicate that to the IRA owner via the year end statements and thus does not report the market value on the Form 5498. The IRS does not require the market value be reported on Form 5498.

Data for the preparation of Form 5498 comes from ARK. Data is reviewed for exceptions. Upon approval, the data is uploaded to an ATC system application which produces the form to be sent to the IRA owners and to allow for electronic transmission to the IRS.

Carved-Out Subservice Organization and Complementary Subservice Organization Controls (CSOC)

ATC uses Ascensus, LLC to provide qualified and individual retirement plan setup, ongoing plan maintenance, fee administration, and Information Technology (IT) general controls including physical security, logical access, disaster recovery and backups, network administration, application development, and environmental controls related to the data center services. The subservice organization is carved out; therefore, the description includes only policies, procedures and control objectives of the service organization and does not include policies, procedures, and control objectives at the service organization described below. The examination of the independent service auditors did not extend to policies and procedures at the subservice organization.

Monitoring of Subservice Organizations

ATC management receives and reviews the SOC report for the subservice organization on an annual basis. Additionally, there are ongoing meetings and discussions related to services provided by the subservice organization. They review the reports for areas of concern and complementary user entity controls (CUEC), as applicable.

Complementary Subservice Organization Controls (CSOC)

ATC's controls related to the Transaction Processing System only cover a portion of overall internal control for each user entity of ATC. It is not feasible for the control objectives related to the Transaction Processing System to be achieved solely by ATC. The achievement of certain control objectives related to ATC is dependent upon controls, known as complementary subservice organization controls (CSOC) that are performed by our subservice provider. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with ATC's controls and related tests and results described in Section IV of this report.

Complementary subservice organization controls (CSOC) are the controls management of ATC assumes in the design of the service organizations system. These controls will be implemented at the subservice organization and are necessary to achieve certain control objectives, as described in the table below. The scope of this report does not include controls at the external subservice organization. Through the performance of the control activities described herein, including obtaining and evaluating available SOC reports for subservice providers, ATC monitors subservice provider's adherence to policies and procedures.

Types of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls (CSOC)	Relevant Applicable CA or CO
IRA and Qualified plan setup, ongoing plan maintenance, fee administration, and IT general controls including physical security, logical access, disaster recovery and backups, network administration, application development, and environmental controls related to the data center.	Ascensus, LLC	Responsible for completeness and accuracy of new plan setup and ongoing plan maintenance. Responsible for logical security, including but not limited to assigning and removing logical user access. Responsible for fee administration. Responsible for governance of application development and network administration. Responsible for disaster recovery and backups. Responsible for assigning, removing, and monitoring physical access to facilities and environmental controls related to the data center.	CO 1 - Controls provide reasonable assurance that the new plans are processed completely and accurately. CO 2 - Controls provide reasonable assurance that IRA modifications and additions to Client master files are processed completely, accurately and retained electronically. CO 3A - Controls provide reasonable assurance that account fees are processed completely and accurately and on a quarterly basis. CO 3B - Controls provide reasonable assurance that account fees are processed completely and accurately and on a quarterly basis and required notices are sent. CO 10B - Controls provide reasonable assurance that paper initiated distribution transactions are properly authorized, accurate, and timely. CO 10C - Controls provide reasonable assurance that electronically initiated distribution transactions are properly authorized, accurate, and timely. CO 15 - Controls provide reasonable assurance that the application development changes are approved, tested, made by the appropriate individual, and reviewed prior to implementation into production.

Types of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls (CSOC)	Relevant Applicable CA or CO
			CO 16 - Controls provide reasonable assurance that Logical Access is maintained in a manner consistent with appropriate rights and restrictions. CO 17 - Controls provide reasonable assurance that access to the physical facilities is limited to authorized personnel.

Information Systems Environment

The following describes the information systems environment at Ascensus and the general controls surrounding its system and network implementations. Information System controls are those which define and establish the control environment in which ATC's client information is processed. How these controls are designed, implemented, managed, maintained and monitored have a significant impact on the effectiveness of internal control at ATC.

Organization and Administration

Annual Information Technology Security Plan and Reporting is reviewed and approved by the Board of Directors annually. ATC's maintains separation of IT and operational business units. The active directory permissions are established based on roles.

A majority of the Board of Directors is independent of management.

As part of the IT environment Ascensus, LLC has an IT employee accessible to ATC. This allows for ongoing monitoring discussions related to the IT environment and related areas of concern, or complementary control required by ATC.

Application and Development

ATC's implemented controls provide reasonable assurance that software development activities follow a prescribed method. This is accomplished by peer reviews, standard testing procedures, and deployment procedures once development has been completed.

Daily meetings are held to review and approve sprints. Emergency sprints are also reviewed and approved prior to implementation into production which may occur separately from the daily meetings.

Access to source code is limited to authorized members of the IT staff.

Security Controls to the Computer Facilities

Controls provide reasonable assurance that access to the physical facilities is limited to authorized personnel. External access points are controlled by key locks with internal access points controlled by keypads opened with individually assigned FOBs. Exterior doors are alarmed and monitored by security cameras. Access to all internally controlled doors is logged by the security software. Access to internally controlled doors in the ATC building are logged by the security software and are available to be reviewed. Ascensus, LLC is notified of ATC employees who have been terminated within one business day.

Risk Management

Logical Access is maintained in a manner consistent with appropriate rights and restrictions. Management approval is required to grant new users application user access. Ascensus, LLC is notified of Ascensus Trust employees who have been terminated within one business day and user access is disabled. Employees are cross-trained, where practical, to provide sufficient backup in the event of unexpected termination, resignation, or promotion. Password security levels have been established at the operating system, network, and application levels, including:

- Minimum requirement of 14 characters (20+ is preferred).
- Alphanumeric and special characters are required if less than 20 characters.
- Passwords are required to be changed once a year.

Customer accounts are locked out after eight invalid attempts. Once an account is locked, it will remain disabled until no invalid attempts are made for 30 minutes. Employee accounts are locked after eight unsuccessful login attempts, and they can unlock their profile using a self-service website. Client's session times out after 15 minutes of idle time.

Complementary User Control Considerations

ATC's processes were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the applications of specific controls at user organizations are necessary to achieve certain control objectives included in this report. The following are the type of controls that ATC expects each party to have in place within their respective organization.

Information Technology

- The user organization limits access to apply system updates to authorized personnel. (Control Objective 14 & 16)
- The user organization restricts access to production and source code to authorized personnel. (Control Objective 16)

- The user organization applies security patches to network infrastructure. (Control Objective 14 & 16)
- The user organization performs daily backups of data to be utilized in instances of system failure. (Control Objective 14)
- The user organization installs and maintains antivirus software across all machines that are part of the network. (Control Objective 14 & 16)
- The user organization configures antivirus software to automatically scan and remove threats from network devices. (Control Objective 14 & 16)
- The user organization adds/removes user access upon requests submitted by ATC. (Control Objective 16)
- The user organization engages third party to perform annual vulnerability scans and web ethical hack assessments. (Control Objective 14 & 16)

Recordkeepers

- The Recordkeeper is responsible for providing accurate and authorized data pertaining to all distributions and loan disbursements. This includes the proper name, address, and distribution type, gross and net amount of the distribution along with any state and federal tax withholding. (Control Objective 8 & 10)
- The Recordkeeper is responsible for providing updates of plan sponsor contact and addresses. (Control Objective 2)
- The Recordkeeper is responsible for providing accurate information for transferring assets on service terminations. (Control Objective 8)
- The Recordkeeper is responsible for providing accurate ACH/bank account information for each plan sponsor. (Control Objective 1 & 2)
- The Recordkeeper is responsible for ensuring that all trade activity provided is accurate and true. (Control Objectives 4, 5, 8, & 10)
- The Recordkeeper is responsible for providing data in a consistent, electronic format approved by both parties. (All Control Objectives)
- Protect passwords that are in conjunction with Ascensus' websites. (All Control Objectives)
- The Recordkeeper is responsible for identifying plans by the proper type and use the correct corresponding Ascensus agreement. (Control Objectives 1, 2, & 3)

Plan Sponsors

- The Plan Sponsor is responsible for establishing control procedures to ensure employee payroll information sent to Recordkeepers for contributions (employee and employer), loan repayments are accurate, complete and match the funds sent to ATC. (Control Objective 4)
- Prompt notification to Ascensus of any change in the Sponsor's contact person or address. (Control Objectives 1, 2, 3, 8, 9, & 10)
- The Plan Sponsor is responsible for submitting participant contributions to ATC consistent with DOL guidelines. (Control Objective 4)
- The Plan Sponsor is responsible for the authorization to ATC's website and password. (All Control Objectives)
- Prompt notification to ATC upon the termination of ATC's services or the termination of the plan. (Control Objective 8)

- The Plan Sponsor is responsible to promptly reply to any correspondence received by ATC regarding outstanding distribution checks. (Control Objective 10)
- The Plan Sponsor is responsible for beneficiary information concerning participants of the plan. (Control Objective 1 & 2)
- The Plan Sponsor is responsible for performing due diligence on any investment or mutual funds that it anticipates offering inside of their qualified plans. (Control Objectives 1, 2, 3, 4, 5, 6, & 7)
- The Plan Sponsor is responsible for development and approval of fee schedules and for changes to participating plans/individuals. (Control Objective 3)

Section IV

Control Objectives and Related Controls,
Tests of Operating Effectiveness and Results of Tests

Provided by the Independent Service Auditor and Ascensus Trust Company

Purpose and Objectives of the Independent Service Auditor's Examination

This report on the controls placed in operation and tests of operating effectiveness applicable to Ascensus Trust Company is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of Ascensus Trust Company's controls that may be relevant to a user entity's internal controls over financial reporting. This report, when coupled with an understanding of internal controls in place at user entities and the subservice organization, is intended to assist in the assessment of the total internal controls applicable to the transactions processed by Ascensus Trust Company for user entities.

Our examination was restricted to the selected services, control objectives and related procedures specified by Ascensus Trust Company in the controls and testing in Section IV, and were not extended to procedures in effect at user entities and the subservice organization. Ascensus Trust Company specified its control objectives and is responsible for identifying its controls to meet those objectives.

The examination was conducted in accordance with the Statements on Standards for Attestation Engagements, Reporting on Controls at a Service Organization (Type 2), of the American Institute of Certified Public Accountants. It is each interested party's responsibility to evaluate this information in relation to internal controls in place at each user entity to obtain an overall understanding of internal controls to assess control risk. The user entity and Ascensus Trust Company's portions of the control structure must be evaluated together. If effective user entity internal controls are not in place, Ascensus Trust Company's controls may not compensate for such weaknesses.

A system of internal control is intended to provide reasonable, but not absolute, assurance that the control objectives are achieved. The concept of reasonable assurance recognizes that the cost of a system of internal control should not exceed the benefits expected to be derived and also recognizes that the evaluation of the cost-benefit relationship requires estimates and judgments by management.

Our tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved throughout the period from October 1, 2024 to September 30, 2025. Our tests of the operational effectiveness of controls were designed to cover a representative number of events for each of the controls listed in Section IV which are designed to achieve the specific control objectives, also listed in Section IV. In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items tested, (b) the types and competence of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk and (e) the expected efficiency and effectiveness of the test.

Description of Testing Procedures

Test procedures performed in connection with determining the operational effectiveness of controls detailed in the matrices in Section IV are described below:

Test	Description
Inquiry	Inquired of appropriate personnel to ascertain their knowledge and understanding of the compliance of the controls. Inquiries were performed on all controls. However, the test is not listed individually for every control shown in the accompanying matrices.
Observation	Observed application of specific control activity.
Inspection	Inspected documents and reports indicating performance of the specific control activity.
Reperformance	Reperformed application of the specific control activity.

Within the testing procedures, sampling refers to non-statistical sampling methods and techniques. Likewise, when referring to a selection of items, such selection was not based on sampling methods and techniques.

Exceptions, if any, noted by Eide Bailly LLP, regarding the adequacy of the controls identified to achieve the stated objective or the level of compliance with the controls are presented in this section under the caption “Results of Testing”.

In certain situations, the application of specific controls at the user entities and the subservice organization are necessary to achieve certain control objectives included in this report.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Account Set-up and Maintenance – Qualified Plan Services		
1A	Controls provide reasonable assurance that the new plans are processed completely and accurately upon receiving appropriate documentation.		
1A.1	All plans setup on ATC's system are reviewed during setup to ensure trust date and agreement type per the system match information on the signed trust/custodial agreement or other notice.	1. Inspected the signed trust/custodial agreement and supporting documentation for a sample of new plans setup to evidence that all plans setup on ATC's system are reviewed during setup to ensure trust date and agreement type per the system match information on the signed trust/custodial agreement or other notice.	No exceptions noted.
1A.2	The Office of Foreign Assets Control (OFAC) listing is run and reviewed weekly.	1. Inspected the OFAC listing for a sample of weeks to evidence that the OFAC listing is run and reviewed weekly.	No exceptions noted.
1A.3	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes in which management discussed the SOC report to evidence that management monitors the subservice organization on an ongoing basis.	No exceptions noted.
	Account Set-up and Maintenance – Individual Retirement Accounts		
1B	Controls provide reasonable assurance the new accounts are processed completely and accurately.		
1B.1	IRA accounts are set up in the system only after required documents are received from IRA owners, Plan Sponsors, or Ascensus, LLC.	1. Inspected the signed IRA application for a sample of new IRA accounts to evidence that the account was set up after an application was received from IRA owners, Plan Sponsors, or Ascensus, LLC.	No exceptions noted.
1B.2	New IRA accounts that are set up in the system are checked for accuracy by an individual independent from the IRA set up process.	1. Inspected supporting documentation for a sample of new IRA accounts to evidence that the accounts were reviewed for accuracy by an individual independent from the IRA set up process.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
1B.3	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Account Set-up and Maintenance – Individual Retirement Accounts		
2	Controls provide reasonable assurance that IRA modifications and additions to client master files are processed completely, accurately, and retained electronically.		
2.1	Documentation of modifications to an IRA account is retained electronically.	1. Inspected supporting documentation for a sample of IRA account modifications to evidence that documentation of modifications to an IRA account is retained electronically for future reference.	No exceptions noted.
2.2	Telephone requests for IRA account modifications are received on a recorded line and retained for 7 years. Verification of the caller as an IRA account owner is required.	1. Observed the backup location on the Application Extender system to evidence that telephone requests for IRA account modifications are received on a recorded line and retained for 7 years. 2. Inspected a recording to evidence that verification of the caller as an IRA account owner is required.	No exceptions noted.
2.3	Modifications to IRA account information are completed after required documentation or approval received.	1. Inspected a sample of IRA account modifications to evidence that changes are completed after required documentation or approval is received.	No exceptions noted.
2.4	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Account Fees and Maintenance – Qualified Plan Services		
3A	Controls provide reasonable assurance that account fees are processed completely and accurately and on a quarterly basis.		
3A.1	Account fees are billed quarterly and according to the approved fee schedule.	1. Inspected account fees billed and the approved fee schedule for a sample of plans to evidence that account fees are billed quarterly and according to the approved fee schedule.	No exceptions noted.
3A.2	The approval of the daily fee account reconciliation is independent of the recurring billing of account fees.	1. Inspected fee account reconciliations for a sample of days to evidence the approval of the fee account reconciliation and that it was performed by an individual independent of the recurring billing of account fees.	No exceptions noted.
3A.3	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Account Fees and Maintenance – Individual Retirement Accounts		
3B	Controls provide reasonable assurance that account fees are processed completely, accurately and on a quarterly basis and required notices are sent.		
3B.1	Account fees are billed quarterly and according to the approved fee schedule.	1. Inspected account fees billed and a bank statement, for force-out plans, for a sample of quarters to evidence that account fees are billed quarterly and according to the approved fee schedule. 2. Inspected the approved fee schedule and account fees billed, for force-out plans, for one individual for a sample of quarters to evidence that account fees are billed quarterly and according to the approved fee schedule. 3. Inspected the approved fee schedule and account fees billed, for non-force-out plans, for a sample of participants by quarter to evidence that account fees are billed quarterly and according to the approved fee schedule.	No exceptions noted.
3B.2	The review of the daily fee account reconciliation is independent of the recurring billing of account fees.	1. Inspected the fee account reconciliations for a sample of days to evidence the approval of the fee account reconciliation and that it was performed by an individual independent of the recurring billing of account fees.	No exceptions noted.
3B.3	Withholding notices are sent to applicable IRA owners semi-annually.	1. Inspected withholding notices for a sample of IRA plans that qualify for withholding notices to evidence that withholding notices are sent semi-annually.	No exceptions noted.
3B.4	SIMPLE notices are sent annually to applicable plans.	1. Inspected supporting documentation to evidence that SIMPLE notices are sent annually to applicable plans.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
3B.5	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Keying/Processing of Investment Transactions – Qualified Plan Services		
4A	Controls provide reasonable assurance that cash contributions are adequately safeguarded upon receipt, properly authorized and processed accurately and completely.		
4A.1	Contribution checks are received at ATC in a secure mailroom. The checks are given to the Trust Associates for processing.	1. Observed mailroom and procedures performed by ATC personnel regarding contributions to evidence that contribution checks are received at ATC in a secure mailroom and given to the Trust Associates for processing.	No exceptions noted.
4A.2	The keyed contribution information is verified and processed by independent individuals or autokey system verification.	1. Inspected a sample of keyed contributions to evidence that the keyed contribution information is verified and processed by independent individuals or autokey system verification.	No exceptions noted.
4A.3	Exceptions to contribution balances received are investigated and cleared before further processing is allowed and prior to the check deposit.	1. Inspected supporting documentation for an exception that has been cleared to evidence that exceptions to contribution balances received are investigated and cleared before further processing is allowed and prior to the check deposit.	No exceptions noted.
4A.4	Contributions received, including check deposits, ACH and wire transfers, are processed for transmittal to investment providers upon receipt.	1. Inspected supporting documentation for a sample of contributions to evidence that contributions received, including check deposits, ACH and wire transfers, are processed for transmittal to investment providers upon receipt.	No exceptions noted.
	Keying/Processing of Investment Transactions – Individual Retirement Accounts		
4B	Controls provide reasonable assurance that cash contributions are adequately safeguarded upon receipt, properly authorized and processed accurately, completely, and timely.		
4B.1	IRA contribution checks are received at ATC in a secure mailroom and routed to the IRA associate.	1. Observed procedures performed by ATC personnel regarding contributions to evidence that IRA contribution checks are received at ATC in a secure mailroom and routed to the IRA associate.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
4B.2	IRA contributions are keyed based on an IRA Contribution/Investment form signed by the IRA owner or other approved correspondence timely.	1. Inspected the IRA Contribution/Investment form or other approved correspondence for a sample of IRA contributions to evidence that IRA contributions are keyed based on an IRA Contribution/Investment form signed by the IRA owner or other approved correspondence and processed within 5 business days. 2. Observed a daily force out contribution to evidence that IRA contributions are keyed based on an IRA Contribution/Investment form signed by the IRA owner or other approved correspondence.	No exceptions noted.
4B.3	IRA contributions are reviewed for accuracy by another member of the IRA team.	1. Inspected supporting documentation for a sample of IRA contributions to evidence that IRA contributions are reviewed for accuracy by another member of the IRA team.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Keying/Processing of Investment Transactions – Qualified Plan Services		
5	Controls provide reasonable assurance that client investment transactions are applied to the appropriate account and are processed completely, accurately, and on a timely basis.		
5.1	Electronic transfer of contribution investment instructions and transaction information from and/or to third-party recordkeepers is completed using secure communication.	1. Observed the use of secure communication to evidence that the electronic transfer of contribution investment instructions and transaction information from and/or to third party recordkeepers is completed using secure communication.	No exceptions noted.
5.2	Recordkeepers Final Investment File is imported to the ATC system to prepare fund for investment purchases.	1. Inspected a sample of daily Final Investment Files to evidence that the recordkeepers Final Investment File is imported to the ATC system to prepare fund for investment purchases.	No exceptions noted.
5.3	Finalized trade amounts are confirmed with Investment Partners prior to funds being sent for trading.	1. Inspected a sample of daily settlement reports to evidence that investment amounts are confirmed, through positive or negative confirmation, with trading partners prior to funds being sent for trading.	No exceptions noted.
5.4	Daily settlement reports for each trading partners net trades are reconciled to bank activity. Any differences are investigated and resolved daily, unless further support needed for proper resolution.	1. Inspected a sample of daily settlement reports to evidence that daily settlement reports for each trading partners net trades are reconciled to bank activity, and differences are investigated and resolved.	No exceptions noted.
5.5	Daily bank reconciliations are prepared and reviewed for the contribution/distribution accounts. A monthly review is performed of the reconciled account balances.	1. Inspected the reconciliation for a sample of days to evidence that reconciliations of the investment bank accounts are performed and reviewed on a daily basis. 2. Inspected the monthly review of the reconciled account balances for a sample of months to evidence the review is performed monthly.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Keying/Processing of Investment Transactions – Qualified Plan Services		
6	Controls provide reasonable assurance that client contribution investment requests delivered to an investment provider are complete and accurate.		
6.1	Recurring wire templates are setup based on third party instructions and approval.	1. Inspected supporting documentation for a sample of new or modified recurring wire templates to evidence they are based on third party instructions and approval.	No exceptions noted.
6.2	Authorization for nonrecurring wire transfers to an investment provider is received from an approved third party.	1. Inspected supporting documentation for a sample of nonrecurring wire transfers to evidence that the authorization was proper.	No exceptions noted.
6.3	Non-recurring wire transfer instructions for sending contributions to investment providers from the ATC account are prepared, verified and submitted.	1. Inspected a sample of nonrecurring wire transfers to evidence that wire instructions for sending contributions to investment providers from the ATC account are prepared, verified and submitted.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Keying/Processing of Investment Transactions – Qualified Plan Services		
7	Controls provide reasonable assurance that funds for which proper investment or distribution requests have not been delivered are invested in short-term investments and the investment income is properly allocated.		
7.1	A monthly report indicating the collected balance of funds invested in a money market account (Collective Fund) is received and reviewed by an associate on a monthly basis.	1. Inspected reports for a sample of months to evidence that a report indicating the collected balance of funds invested in a money market account is received and reviewed by an associate on a monthly basis.	No exceptions noted.
7.2	Reconciliations of the bank accounts for contributions and distributions are performed on a daily basis.	1. Inspected the reconciliation for a sample of days to evidence that reconciliations of the bank accounts for contributions and distributions are performed on a daily basis.	No exceptions noted.
7.3	Reconciliations of the bank accounts for contributions and distributions that are performed on a daily basis are reviewed by an individual independent of the preparation. Account balances are reviewed on a monthly basis.	1. Inspected the reconciliation for a sample of days to evidence that reconciliations of the bank accounts for contributions and distributions that are performed on a daily basis are reviewed by an individual independent of the preparation. 2. Inspected the account balance review for a sample of months to evidence that account balances are reviewed on a monthly basis.	No exceptions noted.
7.4	The interest earned on the Collective Fund is properly allocated monthly to client accounts and ATC through system calculations. The calculation is reviewed by an associate for reasonableness.	1. Inspected interest allocations for a sample of clients by month to evidence that the interest earned on the Collective Fund is properly allocated monthly to the accounts and ATC through system calculations. 2. Inspected review by an associate for a sample of months to evidence that the calculation is reviewed by an associate for reasonableness.	No exceptions noted.
7.5	The Collective Fund is audited annually by an independent auditor.	1. Inspected the audit report to evidence that the Collective Fund is audited annually by an independent auditor.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Keying/Processing of Distribution Transactions – Qualified Plan Services		
8	Controls provide reasonable assurance that client distribution requests received from a third-party recordkeeper for terminating clients are completely and accurately recorded.		
8.1	Terminating clients, for whom ATC is the trustee, must provide proper notice from an authorized individual prior to distribution of the clients' funds.	1. Inspected proper notice for terminations in which ATC is trustee, for a sample of terminating clients to evidence that each client, for whom ATC is the trustee, must provide proper notice from an authorized individual prior to distribution of the clients' funds.	No exceptions noted.
8.2	Activity reports are reviewed for terminating clients to verify the cash and investment balances of the terminating plan.	1. Inspected the liquidation report and outgoing wire history for a sample of terminated plans to evidence that activity reports are reviewed for terminating clients to verify the cash and investment balances of the terminating plan.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Keying/Processing of Distribution Transactions – Qualified Plan Services		
9	Controls provide reasonable assurance that remittances from third parties are received securely by ATC prior to a distribution check being processed.		
9.1	The funds for each distribution must be received by ATC prior to ATC distributing the checks to participants.	1. Inspected a sample of distributions to evidence that the funds for each distribution are received by ATC prior to ATC distributing the checks to participants.	No exceptions noted.
9.2	A cash receipt distribution comparison report is prepared for all distribution requests for which no funds have been received from third parties and all cash received but for which no distribution instructions have been received. This report is sent to the third-party recordkeeper daily.	1. Inspected the cash receipt distribution comparison report and daily email to third-party recordkeeper for a sample of days to evidence that a cash receipt distribution comparison report is prepared for all distribution requests for which no funds have been received from third parties and all cash received but for which no distribution instructions have been received and that this report is sent to the third-party recordkeeper daily.	No exceptions noted.
9.3	Physical checks are received by ATC mailroom personnel and restrictively endorsed.	1. Observed the mailroom process to evidence that physical checks are received by ATC mailroom personnel and restrictively endorsed.	No exceptions noted.
9.4	Electronic transfer of distribution requests from and/or to the third party recordkeeper is completed using secured internal network drives.	1. Observed the distribution process to evidence that electronic transfer of distribution requests from and/or to the third party recordkeeper is completed using secured internal network drives.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Keying/Processing of Distribution Transactions – Qualified Plan Services		
10A	Controls provide reasonable assurance that cash distribution transactions are properly authorized and executed.		
10A.1	Reconciliations of the bank accounts for contributions and distributions that are performed on a daily basis are reviewed by an individual independent of the preparation.	1. Inspected the reconciliation for a sample of days to evidence that reconciliations of the bank accounts for contributions and distributions that are performed on a daily basis are reviewed by an individual independent of the preparation.	No exceptions noted.
10A.2	The check processed report and the check trial balance is agreed before the system allows distribution checks to be processed.	1. Inspected supporting documentation of the check distribution process to evidence that the check processed report and the check trial balance must agree before the system allows distribution checks to be processed.	No exceptions noted.
10A.3	The check register, positive pay exports, Office of Foreign Assets Control (OFAC) comparison report and Ascensus check file are verified daily by personnel independent of the check writing and initiating process.	1. Inspected the Distribution Check Paperwork Verification form for a sample of days to evidence that the check register, positive pay exports, Office of Foreign Assets Control (OFAC) comparison report and Ascensus check file are verified daily by personnel independent of the check writing and initiating process.	No exceptions noted.
10A.4	A system report reconciling the cash balance to voided checks, check runs, and deposits is used to monitor daily activity.	1. Inspected supporting documentation of the check distribution process to evidence that a system report reconciling the cash balance to voided checks, check runs, and deposits is used to monitor daily activity.	No exceptions noted.
10A.5	The Pending Check/Distribution Audit Log is printed and reviewed daily.	1. Inspected the Pending Check/Distribution Audit Log for a sample of days to evidence that the Pending Check/Distribution Audit Log is printed and reviewed daily.	No exceptions noted.
10A.6	The Outgoing Wire Audit Log is printed and reviewed daily.	1. Inspected the Outgoing Wire Audit Log for a sample of days to evidence that the Outgoing wire Audit Log was printed and reviewed daily.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
10A.7	Outgoing distribution wires are reviewed by a separate individual from the preparer to verify third party wire instructions are properly entered.	1. Inspected supporting documentation for a sample of distribution wires to evidence that outgoing distribution wires are reviewed by a separate individual from the preparer to verify third party wire instructions are properly entered.	No exceptions noted.
	Keying/Processing of Distribution Transactions – Individual Retirement Accounts		
10B	Controls provide reasonable assurance that paper initiated distribution transactions are properly authorized, accurate, and timely.		
10B.1	An IRA Withdrawal form signed by the IRA owner/authorized individual is required for the processing of a distribution.	1. Inspected the signed IRA Withdrawal form for a sample of distributions to evidence that an IRA Withdrawal form signed by the IRA owner/authorized individual is required for the processing of a distribution.	No exceptions noted.
10B.2	Distributions via paper request must include a copy of a valid government ID or notarized withdrawal form and any discrepancies in data are resolved prior to distribution.	1. Inspected supporting documentation for a sample of distributions to evidence that the distribution request must include a copy of a valid government ID or notarized withdrawal form and any discrepancies in data are resolved prior to distribution.	No exceptions noted.
10B.3	The distribution is reviewed by personnel independent of the preparer prior to processing. The Payment Transmission is run and compared for paper forms to the distribution forms for accuracy.	1. Inspected review signoffs for a sample of distributions to evidence that the distribution is reviewed by personnel independent of the preparer prior to processing. 2. Inspected the Payment Transmission for a sample of distributions to evidence that the Payment Transmission is run and compared to the distribution forms for accuracy.	No exceptions noted.
10B.4	A report is run annually identifying all individuals whom are required to take a required minimum distribution.	1. Inspected the required minimum distribution report to evidence that a report is run annually identifying all individuals whom are required to take a required minimum distribution.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
10B.5	Communication is sent to individuals who have met the required minimum distribution threshold on an annual basis in accordance with IRS regulations.	1. Inspected the required minimum distribution communication to the account owner for a sample of IRA accounts with required minimum distributions to evidence that communication is sent to individuals who have met the required minimum distribution threshold on an annual basis in accordance with IRS regulations.	No exceptions noted.
10B.6	Distribution is processed within 7 business days of receipt of withdrawal request.	1. Inspected the signed IRA Withdrawal form and Payment Transmission for a sample of distributions to evidence that distributions are processed within 7 business days of receipt of the withdrawal request.	No exceptions noted.
10B.7	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedure	Results of Testing
	Keying/Processing of Distribution Transactions – Individual Retirement Accounts		
10C	Controls provide reasonable assurance that electronically initiated distribution transactions are properly authorized, accurate, and timely.		
10C.1	A system verification of online distribution requests occurs to review any items that require manual adjustment prior to the distribution being processed. All manual adjustments require an independent review prior to processing the distribution. An audit log is also maintained to track all changes made to online distribution instructions.	1. Inspected supporting documentation for a sample of distributions to evidence that a system verification of online distribution requests occurs to review any items that require manual adjustment prior to distribution. 2. Inspected supporting documentation for a sample of distributions to evidence that all manual adjustments were independently reviewed prior to processing the distribution. 3. Inspected the audit log for a sample of distributions to evidence that the audit log is maintained.	No exceptions noted.
10C.2	Distributions requests must undergo customer identification program (CIP), if not already done, and any discrepancies in data are resolved prior to the distribution.	1. Inspected supporting documentation for a sample of distributions to evidence that distributions must undergo customer identification program (CIP) prior to the distribution and any discrepancies in data are resolved prior to distribution.	No exceptions noted.
10C.3	Distributions are processed in accordance with the online distribution instructions.	1. Inspected supporting documentation for a sample of distributions to evidence that distributions are processed in accordance with the online distribution instructions.	No exceptions noted.
10C.4	Distributions are processed within 7 business days of receipt of withdrawal request.	1. Inspected supporting documentation for a sample of distributions to evidence that distributions are processed within 7 business days of receipt of the withdrawal request.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedure	Results of Testing
10C.5	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Reconciliations		
11	Controls provide reasonable assurance that bank accounts for contributions and distributions are reconciled completely and accurately.		
11.1	Reconciliations of the bank accounts for contributions and distributions are performed on a daily basis.	1. Inspected the reconciliation for a sample of days to evidence that reconciliations of the bank accounts for contributions and distributions are performed on a daily basis.	No exceptions noted.
11.2	Reconciliations of the bank accounts for contributions and distributions that are performed on a daily basis are reviewed by an individual independent of the preparation. Account balances are reviewed on a monthly basis.	1. Inspected the reconciliation for a sample of days to evidence that reconciliations of the bank accounts for contributions and distributions that are performed on a daily basis are reviewed by an individual independent of the preparation. 2. Inspected the account balance review for a sample of months to evidence that account balances are reviewed on a monthly basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	State Tax Filings and Withholdings		
12	Controls provide reasonable assurance that all state tax filings are processed completely and accurately and filed in accordance with applicable filing deadlines.		
12.1	ATC has the appropriate system settings in place to provide for accurate filing of state taxes for which ATC is the trustee.	1. Inspected the system settings for a sample of states to evidence that the system settings for the tax payments match state filing requirements.	No exceptions noted.
12.2	Each day a system state taxes due report is generated and reviewed to ensure state tax payments are made in accordance with state requirements.	1. Inspected the state taxes due report for a sample of states by day to evidence that the report is generated and reviewed daily. 2. Inspected payment support for a sample of daily state tax payments to evidence that the amount paid agreed to the state taxes due report. 3. Inspected supporting documentation to evidence that state requirements are monitored for applicable changes.	No exceptions noted.
12.3	Quarterly and annual state tax reports are filed in accordance with state requirements.	1. Inspected supporting documentation for a sample of quarterly and annual reports by state to evidence that they were filed in accordance with state requirements.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Federal Tax Filings and Withholdings		
13	Controls provide reasonable assurance that federal income tax reports are filed accurately and at the appropriate time.		
13.1	Electronic federal tax payment system (EFTPS) withholding payments and ACH transfers are reviewed by personnel independent of the EFTPS program on a daily basis.	1. Inspected the EFTPS withholding payments and ACH transfers for a sample of days to evidence that the payments were reviewed by personnel independent of the EFTPS program.	No exceptions noted.
13.2	EFTPS transmission is verified by confirmation from the Internal Revenue Service.	1. Inspected the EFTPS filings for a sample of days to evidence that the transmissions were verified by confirmation from the Internal Revenue Service.	No exceptions noted.
13.3	1099's and 5498's are prepared for clients with distributions (1099's) and contributions (5498's) during the year. Reconciliation of distributions and contributions to taxes withheld is done annually to determine all necessary filings are complete.	1. Inspected a sample of 1099's and 5498's to evidence that the document agreed to the respective distribution/contribution during the year. 2. Inspected the annual reconciliation of distributions and contributions to taxes withheld to evidence all filings are completed.	No exceptions noted.
13.4	Federal income tax withholding reports (form 945) are prepared accurately and are filed at the appropriate times.	1. Inspected the annual Form 945 filing to evidence that it was prepared accurately and filed at the appropriate time.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Organization and Administration		
14	Controls provide reasonable assurance that adequate segregation of function exists between departments.		
14.1	Annual Information Technology Security Plan and Reporting is reviewed and approved by the Board of Directors annually.	1. Inspected the Board of Directors resolution approving the Information Security Plan and Reporting to evidence that it is approved annually. 2. Inspected the annual Information Security Plan and Reporting to evidence their existence.	No exceptions noted.
14.2	Active Directory permissions are established based on roles.	1. Inspected the use of security groups in Active Directory to evidence that ATC's permissions are established based on roles.	No exceptions noted.
14.3	ATC's maintains separation of IT and operational business units.	1. Inspected the organization chart and Information Security Plan to evidence that reasonable separation of incompatible duties between IT and operation business units exist.	No exceptions noted.
14.4	A majority of the Board of Directors is independent of management.	1. Inspected Board of Directors member listing to evidence that a majority of the Board of Directors is independent of management.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Application Development		
15	Controls provide reasonable assurance that the application development changes are approved, tested, made by the appropriate individual, and reviewed prior to implementation into production.		
15.1	Each user story is created in Azure DevOps where it's assigned a unique ID for tracking documentation in accordance with the Software Development Life Cycle.	1. Inspected the Software Development Life Cycle policy for evidence requiring the use of Azure DevOps for tracking of user stories. 2. Inspected supporting documentation for a sample of user stories to evidence that they are created with a unique change ID for tracking.	No exceptions noted.
15.2	Formal testing procedures check the function of new or modified software prior to implementation.	1. Inspected supporting documentation for a sample of user stories to evidence that formal testing procedures check the function of new or modified software prior to implementation.	No exceptions noted.
15.3	Daily meetings are held to review and approve sprints. Emergency sprints are also reviewed and approved prior to implementation into production which may occur separately from the daily meetings.	1. Inspected the daily recurring meeting invite and supporting documentation to evidence that meetings are held daily to review sprints. 2. Inspected supporting documentation for a sample of emergency releases to evidence they were approved prior to implementation into production.	No exceptions noted.
15.4	Access to source code is limited to authorized members of the IT staff.	1. Inspected a list of users with access to source code to evidence that access to source code is limited to authorized members of the IT staff.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
15.5	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Risk Management		
16	Controls provide reasonable assurance that Logical Access is maintained in a manner consistent with appropriate rights and restrictions.		
16.1	Management approval is required to grant new users application access.	1. Inspected a sample of new user requests to evidence that management approval is required to grant new users application access.	No exceptions noted.
16.2	Ascensus, LLC is notified of ATC employees who have been terminated within one business day.	1. Inspected a sample of terminated ATC employees to evidence that Ascensus, LLC is notified of Ascensus Trust employees who have been terminated within one business day.	No exceptions noted.
16.3	Employees are cross-trained, where practical, to provide sufficient backup in the event of unexpected termination, resignation, or promotion.	1. Inspected the Information Technology Security Plan to evidence that the Plan identifies a backup person responsible for each key IT function.	No exceptions noted.
16.4	Password security requirements have been established as follows: - Minimum 14 characters - Required change every year - Alphanumeric and special characters required if less than 20 characters	1. Inspected the password security settings to evidence that password security requirements have been established that requires a minimum of 14 characters, change every year, and alphanumeric and special characters required if less than 20 characters.	No exceptions noted.
16.5	Employee's accounts are locked out after eight unsuccessful login attempts.	1. Inspected system configurations to evidence that the employee is locked out after eight unsuccessful login attempts. 2. Observed an employee attempt to login unsuccessfully eight times to evidence that employee's accounts are locked out after eight unsuccessful login attempts.	No exceptions noted.
16.6	Client's session times out after 15 minutes of idle time.	1. Observed the timeout after 15 minutes of idle time on the website to evidence that client sessions time out after 15 minutes of idle time.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
16.7	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.

Control Number	Controls Specified by the Organization	Test Procedures	Results of Testing
	Security Controls to the Computer Facilities		
17	Controls provide reasonable assurance that access to the physical facilities is limited to authorized personnel.		
17.1	External access to the ATC building is restricted through the use of key locks and key cards. Exterior doors are alarmed and monitored with a camera.	1. Observed that external access to the ATC building is restricted through the use of key locks and key cards and that they are alarmed and monitored by camera.	No exceptions noted.
17.2	Internal access points in the ATC building are controlled by key cards opened with individually assigned key cards.	1. Observed that internal access points in the ATC building are controlled by key cards opened with individually assigned key cards.	No exceptions noted.
17.3	Access/denial to internally controlled doors in the ATC building are logged by the security software and available to be reviewed.	1. Observed the history reports to evidence that access/denial to internally controlled doors are logged by the security system and available for review.	No exceptions noted.
17.4	Management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	1. Inspected the subservice SOC report to evidence that it was obtained by management. 2. Performed corroborative inquiry with management to evidence the ongoing monitoring of the subservice organization. 3. Inspected meeting minutes to evidence that management reviews the subservice SOC report for areas of concern and monitors the subservice organization on an ongoing basis.	No exceptions noted.
17.5	Ascensus, LLC is notified of ATC employees who have been terminated within one business day.	1. Inspected supporting documentation for a sample of terminated ATC employees to evidence that Ascensus, LLC is notified of Ascensus Trust employees who have been terminated within one business day.	No exceptions noted.

Section V

Other Information Provided by

Ascensus Trust Company

The information included in Section V is presented by Ascensus Trust Company to provide additional information to user organizations and is not a part of ATC's description of controls. The information in Section V has not been subjected to the procedures applied in the examination of the aforementioned description of ATC's controls related to its information processing services, and accordingly, we express no opinion on the descriptions contained within Section V.

ATC Business Continuity Planning

ATC's Business Continuity planning focuses on maintaining and/or rapidly recovering critical business functions that provide service to clients. All Business Continuity planning efforts are guided by an extensive business contingency planning program that defines the planning and recovery processes required during an unexpected business interruption and throughout a recovery. A Business Continuity Plan (BCP) is developed for ATC and is evaluated by both IT and management. BCP activation procedures are tested to ensure that communications, vital records, recovery systems, and necessary equipment are available and function correctly. Disaster Recovery (DR) procedures are tested regularly.

ATC's BCP details a comprehensive recovery approach for the technology environment. The plan defines the roles and responsibilities for team members who are responsible for coordinating the response, recovery, and reconstruction phases after a disaster. Plans are maintained electronically and are backed up nightly as part of system backups.

The main components of the BCP include the following:

- ATC's entire Production and QA infrastructure is located in the Ascensus information technology data center in Dresher, PA. The servers are maintained and supported by Ascensus associates. Ascensus backs up their data using a real time replication process to an off-site location which greatly reduces the amount of data loss should a disaster strike prior to the Ascensus nightly backup tape being created.

- In the event the Dresher facility becomes inoperative, the Dresher disaster recovery team would relocate to the backup Core Data Center located in Las Vegas to begin the recovery process. ATC associates will continue to report to work as usual although they will not be able to access the network until the temporary network is restored. Dresher anticipates recovery of ATC's main applications to occur within 12 hours and all other non-critical applications to be recovered within 48 hours.

- If the structure currently housing ATC is destroyed or not fit for human occupancy, the primary plan is to relocate to the Ascensus Brainerd, MN location. This location provides for immediate access to ATC's production, development, and QA servers with no IT setup necessary. The Brainerd location has many workstations that are not assigned to a specific associate which allows for flexible scheduling on short-notice.

- In relocating to Brainerd, ATC has substantially decreased the risks associated with a serious business interruption. While it now becomes necessary to support and test two recovery plans, the risk of data loss has been minimized as physical documents and electronic data are stored in two separate locations. Recovery efforts have also been streamlined as there is no longer a need to worry about recovering data and relocating to a recovery center at the same.

Attachment to 2025 Form 5500
Assets Held at Year End

Plan Name HENDRICKS COMMUNITY HOSPITAL ASSOCIATION 403(B) PLAN
Plan Sponsor Name HENDRICKS COMMUNITY HOSPITAL ASSOCIATION
EIN 41-0307617
PN 001

(a)	(b) Identity of issue, borrower, lessor, or similar party	(c) Description of investment including maturity date, rate of interest, collateral, par, or maturity value	(d) Cost	(e) Current value
	iShares	IShares Core U.S. Aggregate Bond ETF	0	174,871
	iShares	iShares Core S&P Mid-Cap ETF	0	192,656
	iShares	iShares Core S&P 500 ETF	0	404,432
	iShares	iShares Core 1-5 Year USD Bond ETF	0	20,981
	iShares	iShares Core S&P U.S. Growth ETF	0	1,331,501
	iShares	iShares Core MSCI Total Intl Stk ETF	0	160,820
	Schwab	Schwab U.S. Large-Cap Value ETF	0	144,761
	State Street	State Street SPDR S&P 600 SC Growth ETF	0	98,825
	American Funds	American Funds Capital Inc Bldr R6	0	97,690
	American Funds	American Funds American Balanced R6	0	83,919
	Vanguard	Vanguard Target Retirement 2055 Fund	0	532,730
	Vanguard	Vanguard Target Retirement 2050 Fund	0	318,276
	Vanguard	Vanguard Target Retirement 2040 Fund	0	654,430
	Vanguard	Vanguard Federal Money Market Inv	0	216,552
	Vanguard	Vanguard Target Retirement 2030 Fund	0	397,631
	Vanguard	Vanguard Target Retirement 2045 Fund	0	613,486
	Vanguard	Vanguard Target Retirement 2035 Fund	0	410,241
	Vanguard	Vanguard Target Retirement 2060 Fund	0	401,742
	Vanguard	Vanguard Target Retirement 2025 Fund	0	542,828
	Vanguard	Vanguard Target Retirement 2020 Fund	0	208,605
	Vanguard	Vanguard Treasury Money Market	0	199,809
	Vanguard	Vanguard High Yield Corp Adm	0	19,898
	Ascensus Trust Company	Contribution Account	0	847
	Participant's Loan Account	Various Rates and Maturities	0	96,243