



STATE OF WISCONSIN
Department of Employee Trust Funds
A. John Voelker
SECRETARY

Wisconsin Department
of Employee Trust Funds
PO Box 7931
Madison WI 53707-7931
1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

Correspondence Memorandum

Date: June 10, 2021
To: Audit Committee
From: Yikchau Sze, Director
Office of Internal Audit
Subject: FY2022 – FY2023 Internal Audit Plan

The Department of Employee Trust Funds (ETF) requests the Audit Committee approve the draft internal audit plan for fiscal year 2022 through fiscal year 2023.

The draft internal audit plan was prepared in accordance with the Charter of the Office of Internal Audit and the Internal Audit Standards promulgated by the Institute of Internal Auditors. The Charter requires the Office of Internal Audit to submit a risk based biennial audit plan to the Audit Committee for its review and approval.

Staff will be available at the Audit Committee meeting to answer questions.

Attachment: The Draft Internal Audit Plan for FY2022 – FY2023

Board	Mtg Date	Item #
AUD	6.24.21	3

Internal Audit Plan - Draft

FY 2022 – FY 2023

Office of Internal Audit

May 21, 2021



Board	Mtg Date	Item #
AUD	6.24.21	3

EXECUTIVE SUMMARY

The Office of Internal Audit (OIA) is submitting this audit plan (Plan) for biennial period FY2022 and FY2023, as required by the Internal Audit Charter and by the Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing.

The Plan is a critical document that ensures internal audit resources are used efficiently and effectively to fulfill its mission of enhancing and protecting ETF value through risk-based and objective assurance, advice and insight.

This Plan includes 17+ projects that will be performed by the OIA and 7 information technology (IT) projects that will be performed by a consulting firm specialized in IT auditing and consulting services. Third party administrator (TPA) audits during the planning cycle are also included to provide a full picture of audit coverage of ETF. (See Appendix C)

The Plan is a dynamic document that changes during the planning cycle in response to the changes in business risks, timing of ETF initiatives, and resource availability. Any significant deviation from the approved Plan will be communicated to the Audit Committee of the ETF Board through quarterly activity reports. An annual status update of the Plan will be provided to the Audit Committee prior to each fiscal year end.



Audit Plan

A RISK BASED AUDIT PLANNING APPROACH

The OIA used a systematic approach in identifying critical risks to develop the Plan. The risk assessment results were summarized and prioritized into an overall audit plan that addresses critical risks while taking into consideration ETF's operational needs and available resources. (See Appendix A for Budget.) The following was the approach taken in developing the Plan:

Scope Understanding	Information Gathering	Information Analysis	Audit Plan Development	Audit Plan Approval
<ul style="list-style-type: none"> • Gained understanding of current risk environment by reading publications, attending professional conference and training • Gained understanding of ETF's strategic objectives and key initiatives by attending Agency Management Council and other executive and management meetings 	<ul style="list-style-type: none"> • Updated audit universe based on revised Business Capability Model of Enterprise Architecture • Updated risk assessment template and instructions • Surveyed divisions/offices on their assessment of risks 	<ul style="list-style-type: none"> • Gathered and assessed input from members of management team, and subject matter experts • Developed a preliminary Plan based on interviews, risk assessment results and available resources 	<ul style="list-style-type: none"> • Discussion with the Secretary's Office on: <ul style="list-style-type: none"> • Risk assessment results • Concerns and priorities of the Executive Team • Potential audit focus areas • Gathered input from the Audit Committee members and made necessary adjustments to the Plan • Finalized draft audit plan for approval 	<ul style="list-style-type: none"> • Review and discuss the proposed Plan with the Audit Committee in the June Audit Committee Meeting • Obtain Audit Committee approval • Publish the Audit Plan on ETF intranet



TYPES OF PROJECTS TO COVER RISK AREAS

The OIA considered the risk profile of the agency when identifying and prioritizing projects. (See Appendix B for Risk Assessment and Audit Planning.) Different functions and processes will receive different levels of review based on their importance and perceived risks. For example, consulting services will be provided to reduce high residual risk; independent audit and/or agreed upon procedures will be performed to provide reassurance that management identified internal controls are adequate and operating effectively. There are four levels of review that the OIA will use to cover risk areas:

Audit

Responding to high and medium risks with assurance provided



- Provide assurance
- Issue audit report
- Estimated effort of each audit: 320 - 400 hours

Consulting

Responding to request for formal study or assessment of high-risk areas with relative quicker turnaround time



- Provide no assurance but provide formal recommendations
- Issue consulting report or memo as deliverable; significant deficiency identified would be reported to senior management and the Audit Committee as required by professional auditing standard
- Estimated effort of each consulting service: 280 - 360 hours

Agreed-upon Procedures (AUP)

Routine testing of specific data, transactions and calculations



- Perform specific testing procedures agreed to with management
- Report on results by issuing brief memo to management
- Estimated effort of each project: 40 – 80 hours

Advisory



- Participate in activities in a non-voting member capacity
- Provide verbal comments or a brief memo to management

The OIA will continue to explore Computer Assisted Auditing Techniques to enhance Agreed-upon Procedures and data analytical capacity for continuous auditing.

RISK THEMES

The OIA compiled risks from all the interview sessions and aggregated them to remove redundancies. The risks were then categorized into the following four “Risk Theme.” This process, by its nature, is subjective and based on the auditor’s experience and professional judgement.

1

Data Quality and Protection

Inaccurate and/or incomplete data can lead to poor customer service, inaccurate financial reporting, error in actuarial estimates, and ineffective or incorrect decision making. Failure to properly protect sensitive data may cause unauthorized use and/or disclosure.

2

Change Management

Failure to effectively manage and execute changes may result in inefficiency, increased cost, delayed project timeline, low employee morale and poor service delivery.

3

Third Party

Inadequate third-party risk management may increase ETF’s exposure to regulatory, financial, operational and reputational risks.

4

Transaction Processing

Increased difficulty in supporting legacy applications may result in incorrect, incomplete or untimely transaction processing.

AUDIT FOCUS AREAS

There are a number of discrete risk areas that support the broader Risk Themes identified on the preceding page, as showcased in the table below. These risk areas have been subjectively placed on a heat map on the following page.

1

Data Quality and Protection

- WRS Member Contact Information
- Health Plan Enrollment
- Sick Leave Reporting
- WRS Data Integrity
- System Interface (IT)
- Legacy Application General Controls (IT)
- Breach Response (IT)
- Data Loss Prevention (IT)
- Equipment and Data Protection (IT)

2

Change Management

- Resources Management
- Portfolio Intake Process
- ECM Record Processing
- Open Record Request
- System Development Life Cycle (IT)

3

Third Party

- Department Terms and Conditions
- TPA Contract Compliance
- SOC1 Reporting
- Chapter 40 Procurement
- Vendor Management (IT)

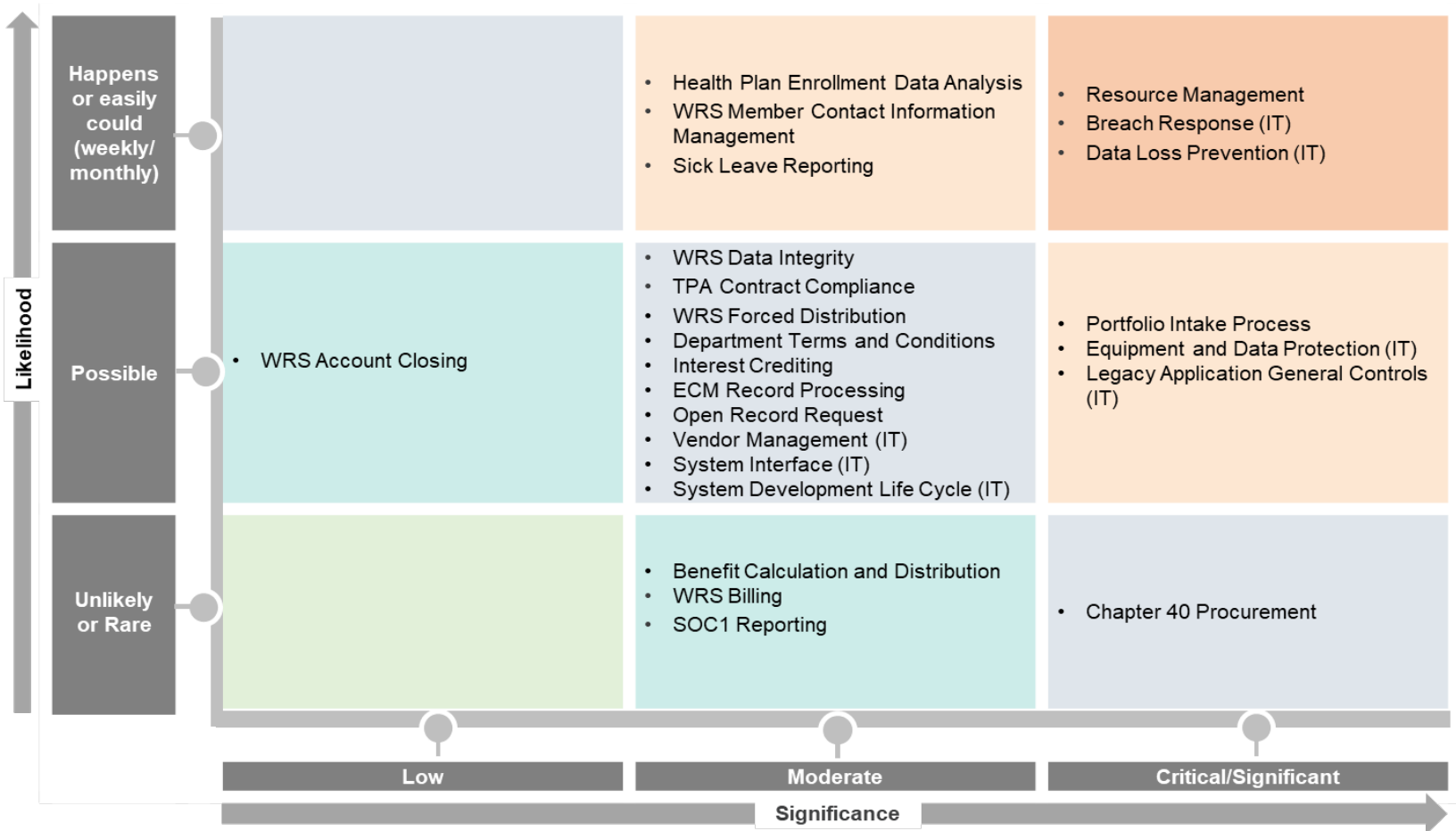
4

Transaction Processing

- WRS Account Closing
- Interest Crediting
- WRS Forced Distribution
- Benefit Calculation and Distribution
- WRS Billing

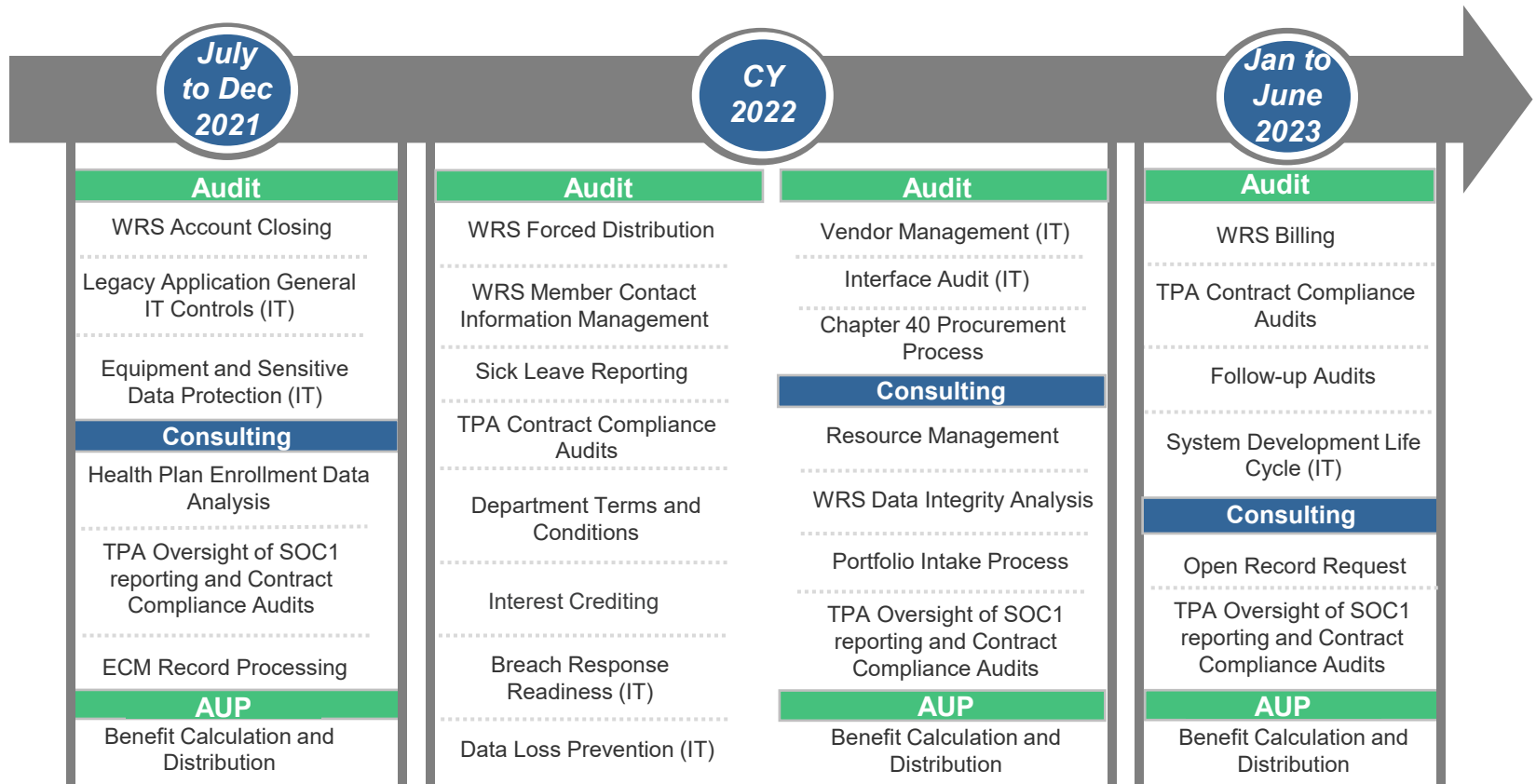
HEAT MAP

Based on interviews performed, OIA subjectively mapped the residual risks identified based on Likelihood and Significance to ETF. The results of this mapping exercise plays a role in the prioritization and scheduling of proposed engagements.



PROPOSED AUDIT PLAN

OIA developed the Plan based on the risk assessment results, audit coverage across ETF for the past five years, timing of ETF initiatives, and available resources. This plan will be refreshed annually, via inquiry with a select group of leadership / stakeholders, to confirm accuracy based on changing risk conditions and external factors that may impact ETF.



ENGAGEMENT DESCRIPTIONS

The tables on this page and the following pages summarize the audit projects, by business processes, defined by the Business Capability Model. Objectives and scopes will be finalized in each project's formal planning phase.

Provide and Administer Benefits

Engagement Focus	Timing	Description
Health Plan Enrollment Data	FY22	Conduct a pilot enrollment data analysis for eligibility and determine whether an audit on a larger scale is beneficial
Member Contact Information Management	FY22	Determine the extent to which ETF has processes in place to ensure member contact information is appropriately maintained
Benefit Calculation and Distribution	FY22 & FY23	Periodic sample testing of data and transactions to gain additional assurance on WRS benefits' calculation and distribution
Forced Distribution	FY23	Determine whether ETF has processes in place to ensure compliance with IRS Required Minimum Distribution for retirement benefits
Interest Crediting	FY23	Determine whether internal controls are adequately designed and operating as intended for the annual interest crediting process
WRS Account Closing	FY22	Review WRS account closing process and determine the extent to which the non-compare process is working as intended
WRS Data Integrity Analysis	FY23	Perform data analysis on WRS accounts to ensure data integrity, and develop data analysis scripts for future automated tests
WRS Billing	FY23	Review WRS employer invoicing process for adequate controls, specifically the process for over and under contributions by employers
Sick Leave Reporting	FY22	Review sick leave hours reported by employers to ensure accuracy and appropriateness

ENGAGEMENT DESCRIPTIONS

Manage Programs and Policy		
Engagement Focus	Timing	Description
Department Terms and Conditions	FY23	Determine whether ETF has processes in place to ensure Department Terms and Conditions are appropriately maintained and applied
TPA Contract Compliance Audits and Audit Oversight	FY22 & FY23	Facilitate the review of service organization control reports, oversee TPA contract compliance audits and perform contract compliance audits (see Appendix C for benefit programs administered by the TPAs)
Develop, Align and Deploy Strategy		
Engagement Focus	Timing	Description
Resource Management	FY22	Determine whether the resource management tool is being used effectively to support organization initiatives
ECM Record Processing	FY22	Conduct before and after ECM implementation reviews to ensure appropriate processing procedures and adequate controls
Portfolio Intake Process	FY22	Determine the extent to which the portfolio intake process is operating as designed

ENGAGEMENT DESCRIPTIONS

Support Relationships

Engagement Focus	Timing	Description
Open Record Request	FY23	Evaluate the Open Record Request process for adequate documentation, appropriate controls and identify potential process improvement opportunities

Enable Delivery

Engagement Focus	Timing	Description
Chapter 40 procurement process	FY22	Assess Chapter 40 procurement process for adequate documentation, transparency and appropriate controls

ENGAGEMENT DESCRIPTIONS

Enable Delivery – Information Technology

Engagement Focus	Timing	Description
IT General Control	FY22	Confirm the operating effectiveness of IT general controls for a sample of legacy applications related to security, change management/system development, batch scheduling, and backup and recovery
System Development Life Cycle (SDLC)	FY23	Evaluate the following of SDLC methodology and the utilization of sound project management and change management disciplines
Breach Response Readiness	FY22	Review the breach response plan for appropriate steps regarding incident containment, eradication, recovery and follow-up, and evaluate the processes in place to react to a data breach or security incident
Data Loss Prevention	FY23	Identify where sensitive data is located and determine how sensitive data is controlled to effectively manage risks associated with data transfer / data transmission
Equipment and Sensitive Data Protection	FY22	Evaluate anti-theft security measures for effective protection of sensitive data on ETF mobile computing devices
Vendor Management	FY23	Evaluate the vendor management processes including due diligence, security, contract compliance and quality of and ability to rely on vendor's attestation regarding internal controls
IT Interfaces	FY23	Evaluate controls between interfaces to confirm that data transmissions are complete and accurate



APPENDIX A - Budget

ESTIMATED OIA HOURS

	Audit Director	Internal Auditors	Summary	
Total Hours - Biennial	4,160	12,480	16,640	100%
Less		-		
Meetings	500	450	950	6%
General Administration	354	824	1,178	7%
Training	100	240	340	2%
Holidays and Personal	216	648	864	5%
Vacation and Sick Leave	400	1,650	2,050	12%
	1,570	3,812	5,382	32%
Internal Audit Activities				
Audit Recommendation Follow-up	20	60	80	
Audit Manual and Charter Update	40	-	40	
Biennial Audit Planning	280	-	280	
Data Analysis Buildout	20	200	220	
Audit Management Software Upgrade	80	80	160	
Internal Quality Assurance Review	300	100	400	
Fraud Program Oversight and Hotline Monitoring	80	40	120	
	820	480	1,300	
Total Available Audit Hours	1,770	8,188	9,958	60%
Project Hours				
Planned	1,144	5,911	7,055	71%
Reserved*	626	2,278	2,903	29%

* Hours available to conduct TPA audits and Follow-up Audits



APPENDIX B - Risk Assessment And Audit Planning

RISK ASSESSMENT AND AUDIT PLANNING

Risk Definition

Risk is defined as “the possibility that an event will occur and adversely affect the achievement of objectives.”

Overall Risk Assessment (Risk Scores)

OIA took each of the auditable areas from the Business Capability Model and assigned an overall risk score based on the following weighted risk factors: Dollar Size or Transaction Volume (15%), Program Complexity (15%), Maturity Level of Business Capability (25%), Control Environment (35%), and Time Since Last Audit (10%). The risk scores were used as an indicator to determine whether detailed risk assessment needed to be performed.

Detailed Risk Assessment (*Likelihood and Impact*)

OIA interviewed Bureau Directors and subject matter experts to confirm the likelihood and impact assessment of specific risks identified of business functions with a risk score of 3 or above. Financial risk, operational risk, reputational risk, compliance risk and strategic risk were considered and analyzed; although fraud risk is generally discussed at this biennial planning phase, typical risk assessment has always been performed at the engagement level. OIA sought input from Division Administrators, Secretary’s Office, and Audit Committee to ensure that significant risks or major concerns were captured at this detailed risk assessment phase.

Please refer to **Figure 1** Risk Assessment Guidance for definitions and examples.

Audit Planning

The result of the detailed risk assessment, played a significant role in the prioritization and scheduling of proposed engagements. Also being considered, was the overall audit coverage. OIA analyzed audit coverage across ETF for the past five years when developing the new biennial audit plan to ensure that the new audit plan provides appropriate audit coverage that aligns with the Audit Frequency Guideline of auditing high-risk rating areas within three years, moderate risk rating areas every 4 to 5 years, and low risk areas every 6 to 7 years.

Please refer to **Figure 2** Audit Coverage for the details.

RISK ASSESSMENT AND AUDIT PLANNING (CONT.)

Figure 1. Risk Assessment Guidance – Assessment Criteria and Examples

Impact / Significance Scale		Financial*		Reputation*	Operational*	Compliance*	Strategic*	Description	Example of Operational Risk
IMPACT	Financial*		Reputation*	Operational*	Compliance*	Strategic*	Description	Example of Operational Risk	
	Statements	Other							
(5) Critical	> \$1BLN	Greater than 15% of operating budget or program assets	Irreversible damage to ETF reputation and credibility; Irreversible loss of member confidence	Complete stoppage of business services for foreseeable future	Violation(s) resulting in widespread data loss, monetary fines, regulatory intervention, etc.	Failure to meet ETF's strategic goals	The risk will cause the objective to not be achieved	No training can be provided to users before the deployment of the new system	
(4) High	\$100M - \$1BLN	Between 10% and 15% of operating budget or program assets	Adverse media exposure is persistent and in multiple publications; Increase in member inquiries	Widespread disruption to service levels, business activities, and/or critical processes	Significant violation(s) of laws, guidelines, or breach of fiduciary duty	Significant delays or reductions in scope of ETF's goals	The risk will cause major elements of objectives to be delayed or not be achieved	Limited training will be provided to some users before the deployment of the new system	
(3) Moderate	\$1M - \$100M	Between 5% and 10% of operating budget or program assets	Media exposure includes criticism from several sources; Members remain confident	Temporary disruption to service levels and/or business activities; Minor impact on critical processes	Moderate violation, potentially leading to increased scrutiny	Delays or revisions to ETF's strategic goals	The risk will cause some elements of objectives to be delayed or not be achieved	Adequate training will be provided to critical users before the deployment of the new system	
(2) Low	\$100K - \$1M	Between 1% and 5% of operating budget or program assets	Local/limited media exposure having minimal impact on reputation	Minor/temporary impact to service levels and/or business activities; No impact to critical processes	Minor legal/compliance violations	Minor delays or revisions to goals	The risk will cause some minor elements of objective to be delayed	Adequate training will be provided to the majority of users before the deployment of the new system	
(1) Incidental	<\$100K	Less than 1% of operating budget or program assets	No impact to ETF's reputation	No impact to service levels, business activities or critical processes	No legal/compliance violations	No impact to achievement of goals	The risk will not substantively impede the achievement of the objective	Adequate training will be provided to all users before the deployment of the new system	

Likelihood/Probability Scale		Description		Example of Operational Risk	CONSIDERATIONS	
PROBABILITY	Within the time horizon contemplated by the objective			Objective: adequate training is provided to all users before the deployment of the new IT system	Inherent	Residual
(5) Expected	The risk is expected to occur			No resource is attainable to provide required training	<ul style="list-style-type: none"> - Program Complexity - Regulatory Environment - Estimates Used - Susceptibility to Change - Historical Experience - Frequency/volume of activity - External Oversight - Number of processes and systems involved 	<ul style="list-style-type: none"> - Overall control environment: culture and ethical value; organization structure; oversight and accountability - Risk identification and analysis - Internal control activities - Policies and procedures - Skills and competencies of staff performing control activities
(4) Likely	The risk is seen as likely to occur			Resource is very limited to provide required training		
(3) Possible	The risk is seen as probable to occur			Additional resource needs to be brought in to provide required training		
(2) Unlikely	The risk is seen as unlikely to occur			Current resource can be re-arranged to provide required training		
(1) Remote	The risk is seen as very rare to occur			Current resource is almost certain to be able to provide required training		

*Financial Risk - Risk that could result in a negative financial impact to the organization in term of waste or loss of assets / financial statement material misstatement/misrepresentation
 *Reputational Risk - Risk that could expose the organization to negative publicity
 *Operational Risk - Risk that could disrupt operations or prevent the organization from operating in the most effective and efficient manner
 *Compliance Risk - Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations
 *Strategic Risk - Risk that would prevent an organization from accomplishing its mission and strategic goals
 Fraud Risk is typically discussed at the planning stage, but further assessed at the engagement level

RISK ASSESSMENT AND AUDIT PLANNING (CONT.)

Figure 2. Audit Coverage

		Risk Assessment		
		Overall Score	Inherent Risk	Residual Risk
Auditable Areas - by Enterprise Architecture Business Capability				
1.1	Enroll in Benefit Programs	3.92	High	Medium
8.3	Manage Change	3.83	High	Medium
7.3	Execute Strategy	3.73	High	Medium
11.2	Manage Procurement	3.70	High	Medium
2.2	Manage Employer Benefit Participation	3.69	High	Medium
2.4	Manage Employer Reporting and Contributions	3.66	High	Medium
9.1	Develop and Manage Human Resource Planning, Policies, and Strategies	3.65	High	Medium
4.2	Manage Enterprise Policy	3.62	High	Medium
2.1	Onboard Employer and Select Benefit Participation	3.62	High	Medium
8.2	Manage Portfolio, Programs, and Projects	3.59	High	Medium
8.1	Manage Enterprise Processes, Quality and Performance	3.58	High	Medium
2.3	Provide Employer Customer Assistance	3.49	High	Medium
4.1	Manage Program Policy and Program Rates	3.43	High	Medium
1.4	Maintain Account After Distribution	3.39	High	Medium
1.3	Distribute Benefits	3.36	High	Medium
10.4	Manage Data Services	3.36	High	Medium
12.4	Manage Program Compliance	3.35	High	Medium
7.2	Develop Business Strategy	3.34	High	Medium
7.1	Define the Business Concept and Long-Term Vision	3.30	High	Medium
10.2	Manage Technology Solution Services	3.27	High	Medium
9.2	Manage Employee Lifecycle	3.24	High	Medium
10.3	Manage Technology Infrastructure Services	3.20	High	Medium
10.1	Manage Personal Technical Support Services	3.20	High	Medium
1.2	Provide Customer Service	3.11	High	Medium
11.3	Manage Contracts and Vendors	3.00	High	Medium
12.3	Manage Information Risk	2.87	High	Medium
5.2	Manage Financial Reporting	3.06	High	Low
11.1	Manage Agency Budget	2.98	High	Low
12.2	Manage External Audit	2.41	High	Low
5.1	Account for TPA Payments	2.18	High	Low
3.1	Train and Educate Members and Employers	3.65	Medium	Low
8.4	Develop and Manage Enterprise Knowledge	3.62	Medium	Low
3.3	Voice of the Customer Feedback	3.42	Medium	Low
9.3	Manage Employee Information and Analytics	3.26	Medium	Low
6.2	Manage Legal Issues	3.23	Medium	Low
3.2	Member and Employer Communications	3.22	Medium	Low
6.1	Manage Government and Industry Relationships	3.06	Medium	Low
6.3	Manage Media Relations	3.04	Medium	Low
4.4	Program Oversight and Process Development	2.91	Medium	Low
4.3	Manage Board Governance Policy	2.90	Medium	Low
11.4	Pay Agency Expenses	2.44	Medium	Low
9.4	Manage Facilities	2.43	Medium	Low
12.1	Manage Internal Audit			

Audit Coverage (Calendar Year)					
2016	2017	2018	2019	2020 - June 2021	New Audit Plan
x					x
					x
					x
				x	
x				x	x
					x
				x	
					x
				x	x
x	x		x		x
		x			x
				x	x
					x
				x	x
		x			x
		x			
				x	
					x
					x
x	x	x	x	x	x
		x			
				x	
					x
					x
				x	
					x
	x				
			x		



APPENDIX C – Third-Party Administrators

TPA AUDITS

Program	TPA	Audit Frequency	Calendar Year Last Review Completed
Deferred Compensation Program	Empower Retirement	Biennial (Covers One Year Only)	2019
Income Continuation Insurance (ICI)	The Hartford	Triennial	2017
Pharmacy Benefit Manager	Navitus	Annual	2020
Employee Reimbursement Account/HSA/Commuter Benefits	Connect Your Care	Biennial	2019
Life Insurance	Securian	Biennial	2019
Uniform Dental	Delta Dental	Biennial	2018
Wellness and Disease Management	StayWell	Triennial	2019