Internal Audit Plan - Draft

FY 2024 – FY 2025

Office of Internal Audit

May 19, 2023

WISCONSIN DEPARTMENT OF EMPLOYEE TRUST FUNDS

Board	Mtg Date	Item #
AUD	06.22.23	7

EXECUTIVE SUMMARY

The Office of Internal Audit (OIA) is submitting this audit plan (Plan) for biennial period FY2024 and FY2025, 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 engagements covering 12 audit focus areas that will be performed by the OIA and three information technology (IT) projects that will be outsourced to IT auditing and consulting firm(s) specialized in IT and Security services. Third-party administrator (TPA) contract compliance audits, including both insourced and outsourced audits, are 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

• 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
	• Updated the risk assessment template and the survey questionnaires
	• Conducted interviews with division administrators, office directors, and other senior management and key staff
		• Assessed input from members of management team, and subject matter experts
		• Developed a preliminary Plan based on interviews, risk assessment results and available OIA resources
			• Discussed with the Secretary's Office on:
			  • Risk assessment results
			  • Concerns and priorities of the Executive Team
			  • Potential audit focus areas
			• Gathered input from the Audit Committee members
			• Made necessary adjustments to finalize the Plan for approval
				• 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 Connect OIA page

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 medium to 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 medium to hig 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 standards
- 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

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 Themes.” 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 oversight and risk management may increase ETF’s exposure to regulatory, financial, operational and reputational risks.

4 Transaction Processing

Increased difficulty in supporting legacy applications and poor data migration, and system integration and process re-engineering of the new system may result in incorrect, incomplete, or untimely transaction processing.

AUDIT FOCUS AREAS

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

1 Data Quality and Protection

- Data Lake and Reporting
- IAS Employer Compliance
- GASB 96
- Penetration Testing (IT)

2 Change Management

- IAS Implementation Readiness
- Project Scoping and Handoff
- System Development Life Cycle (IT)

3 Third Party

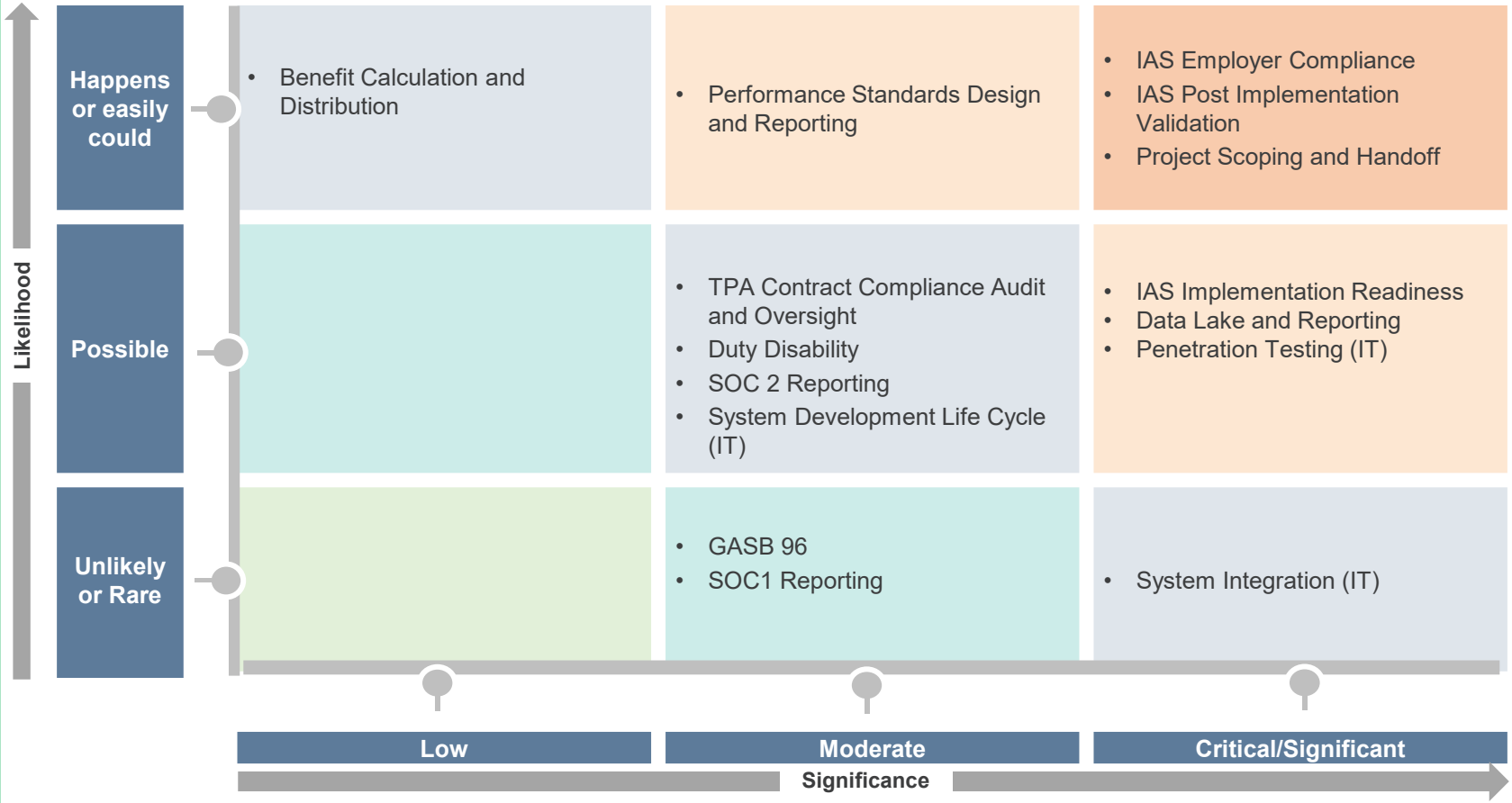
- TPA Contract Compliance Audit and Oversight
- Performance Standards Design and Reporting
- SOC2 Reporting
- SOC1 Reporting Oversight

4 Transaction Processing

- IAS Post Implementation Validation
- WRS Benefit Calculation and Distribution
- Duty Disability
- System Integration (IT)

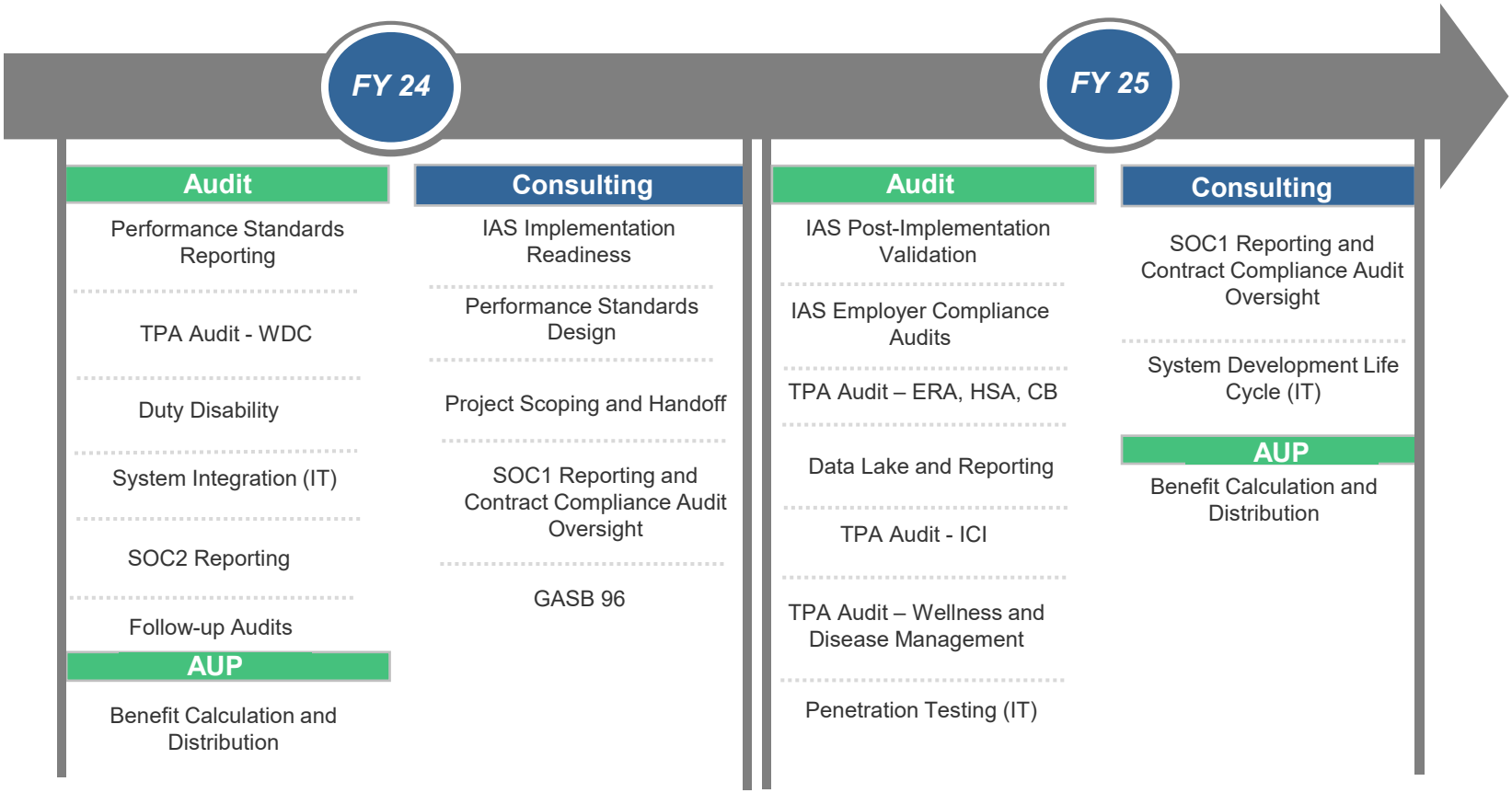
HEAT MAP

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 and 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 engagement 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	Description	Estimated Hours
Duty Disability Benefits Audit	Conduct an audit on the Duty Disability Benefits program to ensure the design and operating effectiveness of internal controls	320
IAS Employer Compliance Audits	Determine the extent to which WRS participating employers submit correct and accurate information to the Insurance Administration System for processing	960
Benefit Calculation and Distribution	Periodic sample testing of data and transactions to gain additional assurance on calculation and distribution of WRS benefits	200
IAS Implementation Readiness Review	Consult on the organizational readiness for the IAS implementation, including but not limited to, proper definition of roles and responsibilities, updates to position descriptions and procedures, action plan for prioritized issues	360

In addition to the audit projects, OIA has delegated 2,200 hours in the audit plan to develop a data analytic program that will enhance the effectiveness of the planned engagements and identify targeted reviews and continuous monitoring opportunities to be included in the audit plan. The development of the data analytics program, including additional projects, will be reported to the Audit Committee through the quarterly audit plan status update.

ENGAGEMENT DESCRIPTIONS (CONT.)

Manage Programs and Policy

Engagement Focus	Description	Estimated Hours
TPA Contract Compliance Audits	Perform contract compliance audit on benefit programs administered by the TPAs, including: - Pre-tax savings account programs by Optum Financial - Income Continuation Insurance program by the Hartford - Wellness and Disease Management program by WebMD - Wisconsin Deferred Compensation by Empower	2120
SOC 1 Reporting & TPA Contract Compliance Audit Oversight	Facilitate the review of service organization control reports and oversee TPA contract compliance audits performed by independent auditors	140
Performance Standards Design	Evaluate the design of performance measures and reporting standards in the health and other supplemental benefit plan contracts for the alignment of desired outcomes	280
Performance Standards Reporting	Assess performance standards reports submitted by health plans for adequate support and proper computation	280

ENGAGEMENT DESCRIPTIONS (CONT.)

Accounts for Trust Funds

Engagement Focus	Description	Estimated Hours
IAS Post Implementation Validation	Evaluation of the implementation of key business processes to ensure outcome are delivered as expected	400
GASB 96	Consult on the implementation plan and review the reporting of GASB Standards for the Subscription-Based Information Technology Arrangements	60

Develop and Deploy Vision and Strategy

Engagement Focus	Description	Estimated Hours
Project Scoping and handoff	Review project scoping and handoff to assess the extent to which the project objectives are achieved, and the outcomes are maintained	360

ENGAGEMENT DESCRIPTIONS (CONT.)

Enable Delivery

Engagement Focus	Description	Estimate Hours
Data Lake and Reporting	Review data lake and its reporting function for integrity, quality, and security	320
SOC2 Reporting	Evaluate the review and monitoring process for SOC2 reporting to ensure adequate internal controls	320
System Development Life Cycle Management	Evaluate whether the SDLC methodology is followed, and sound project management and change management disciplines are utilized	Outsourced to JANUS
System Integration Review	Evaluate the process and controls with regard to the data transmissions through integrated ETF internal IT systems for the completeness, accuracy, and security	Outsourced to JANUS
Penetration Testing	Identify security vulnerabilities in ETF's systems and applications through penetration test to ensure a reasonable protection against malicious attacks	TBD
Follow-up Audits	Conduct follow-up audits to ensure the completion of corrective actions of audit findings with a significance rating equal to or above Medium	240

APPENDIX A - Budget

ESTIMATED OIA HOURS

	Director	Staff	Team Total	
Total Hours - Biennial	**4,160**	**12,480**	**16,640**	**100%**
		-		
Less		-		
Meetings	500	450	950	
General Administration	284	638	921	
Training	100	240	340	
Holidays and Personal	216	648	864	
Vacation and Sick Leave	400	1,200	1,600	
	1,500	3,176	4,675	28%
Internal Audit Activities				
Audit Manual and Charter Update	20	-	20	
Biennial Audit Planning	320	-	320	
Data Analytics Project	120	2,080	2,200	
Fraud Program Oversight and Hotline Monitoring	40	40	80	
IT Audits & Penetration Testing RFPs	520		520	
TeamMate+ Functionality Buildout	120	160	280	
	1,140	2,280	3,420	21%
Total Available Project Hours for Audit Plan Completion	**1,520**	**7,024**	**8,545**	**51%**

Available Project Hours - Audit Plan Allocation				
Planned Projects	1,272	6,360	7,632	**89%**
Contingent Projects	248	664	913	**11%**
	1,520	**7,024**	**8,545**	

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 Division Administrators, Office Directors, and subject matter experts to gain further understanding on general and specific risks identified for 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 the Secretary’s Office, and Audit Committee members 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								
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	- Program Complexity - Regulatory Environment - Estimates Used - Susceptibility to Change - Historical Experience - Frequency/volume of activity - External Oversight - Number of processes and systems involved	- Overall control environment: culture and ethical value; organization structure; oversight and accoutability - 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 tipically discussed at the planning stage, but further assessed at the engagement level

RISK ASSESSMENT AND AUDIT PLANNING (CONT.)

Figure 2. Audit Coverage

		Risk Assessment			Audit Coverage		
		Overal Score	Inherent Risk	Residual Risk	July 2019-June 2021	July 2021 - June 2022	New Audit Plan
Auditable Areas - by Enterprise Architecture Business Capability							
2.4	Manage Employer Reporting and Contributions	3.55	High	Medium	x	x	x
9.1	Develop and Manage Human Resource Planning, Policies, and Strategies	3.50	High	Medium			x
3.1	Train and Educate Members and Employers	3.49	High	Medium	x	x	x
7.3	Execute Strategy	3.43	High	Medium			x
2.2	Manage Employer Benefit Participation	3.43	High	Medium	x	x	x
3.3	Voice of the Customer Feedback	3.26	Medium	Low			x
2.3	Provide Employer Customer Assistance	3.26	High	Medium			x
12.4	Manage Program Compliance	3.25	High	Medium	x	x	x
9.2	Manage Employee Lifecycle	3.24	High	Medium			x
8.3	Manage Change	3.20	High	Medium		x	x
3.2	Member and Employer Communications	3.15	High	Medium		x	x
1.4	Maintain Account After Distribution	3.14	High	Medium	x	x	x
1.3	Distribute Benefits	3.13	High	Medium		x	x
4.2	Manage Enterprise Policy	3.11	High	Medium		x	x
10.4	Manage Data Services	3.11	High	Medium		x	x
1.1	Enroll in Benefit Programs	3.10	High	Medium	x	x	x
8.1	Manage Enterprise Processes, Quality and Performance	3.07	High	Medium		x	x
4.4	Program Oversight and Process Development	3.06	High	Medium	x	x	x
7.2	Develop Business Strategy	3.04	High	Medium			x
1.2	Provide Customer Service	3.01	High	Medium		x	x
8.4	Develop and Manage Enterprise Knowledge	2.97	Medium	Low			
11.1	Manage Agency Budget	2.94	High	Low		x	
2.1	Onboard Employer and Select Benefit Participation	2.94	High	Medium			
9.3	Manage Employee Information and Analytics	2.91	High	Medium	x	x	
4.1	Manage Program Policy and Program Rates	2.91	High	Medium			
6.1	Manage Government and Industry Relationships	2.91	Medium	Low	x	x	
6.3	Manage Media Relations	2.89	Medium	Low			
10.1	Manage Personal Technical Support Services	2.89	High	Medium			
8.2	Manage Portfolio, Programs, and Projects	2.89	High	Medium		x	x
12.2	Manage External Audit	2.86	High	Low	x	x	x
12.3	Manage Information Risk	2.85	High	Medium		x	x
11.3	Manage Contracts and Vendors	2.83	High	Medium	x	x	
10.3	Manage Technology Infrastructure Services	2.82	High	Medium		x	x
10.2	Manage Technology Solution Services	2.73	High	Medium		x	
11.2	Manage Procurement	2.72	High	Medium	x	x	
5.2	Manage Financial Reporting	2.66	High	Low		x	x
7.1	Define the Business Concept and Long-Term Vision	2.65	High	Medium			
9.4	Manage Facilities	2.63	Medium	Low	x	x	
11.4	Pay Agency Expenses	2.58	Medium	Low			
4.3	Manage Board Governance Policy	2.57	Medium	Low			
6.2	Manage Legal Issues	2.53	Medium	Low		x	
5.1	Account for TPA Payments	2.53	High	Medium		x	
12.1	Manage Internal Audit						

APPENDIX C – Third-Party Administrators

TPA CONTRACT COMPLIANCE AUDITS

Program	TPA	ETF Responsible Business Area	Audit Resource	Next Audit Cycle (Calendar Year)
Wisconsin Deferred Compensation Program (WDC)	Empower Retirement	Division of Retirement Services	OIA	2024 for 2023
Income Continuation Insurance (ICI)	The Hartford	Division of Retirement Services	OIA	2025 for 2021, 2022, and 2023
Pharmacy Benefit Manager	Navitus	Office of Strategic Health Policy	Outsource	Annual
Employee Reimbursement Account/Health Savings Accounts/Commuter Benefits (ERA/HSA/CB)	Optum Financial	Office of Strategic Health Policy	OIA	2024 for 2022 and 2023
Life Insurance	Securian	Office of Strategic Health Policy	Outsource	2024 for 2022 and 2023
Uniform Dental	Delta Dental	Office of Strategic Health Policy	Outsource	2025 for 2023 and 2024
Wellness and Disease Management	WebMD	Office of Strategic Health Policy	OIA	2024 for 2022 and 2023