State of Wisconsin
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

801 W Badger Road
PO Box 7931
Madison WI 53707-7931

1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

Correspondence Memorandum

Date: June 19, 2017

To: Audit Committee

From: Yikchau Sze, Director
Office of Internal Audit

Subject: 2017 – 2019 Internal Audit Plan

Staff requests that the Audit Committee approve the Audit Plan for Fiscal Years 2018 – 2019.

The Audit Plan was prepared in accordance with the Charter of the Office of Internal Audit. The Charter requires the Office of Internal Audit to prepare a flexible biennial audit plan that addresses key risk areas in cooperation with Department of Employee Trust Funds (ETF) administrators and office directors. The plan has been reviewed and approved by the Office of the Secretary of ETF.

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

Attachment: 2017 -2019 Internal Audit Plan

Reviewed and approved by Robert J. Conlin, Secretary

Electronically signed 6/19/17

Board	Mtg Date	Item #
AUD	6.22.17	5

Internal Audit Plan - Draft

2017 - 2019

Office of Internal Audit

WISCONSIN DEPARTMENT OF EMPLOYEE TRUST FUNDS

Board	Mtg Date	Item #
AUD	6.22.17	5

Executive Summary

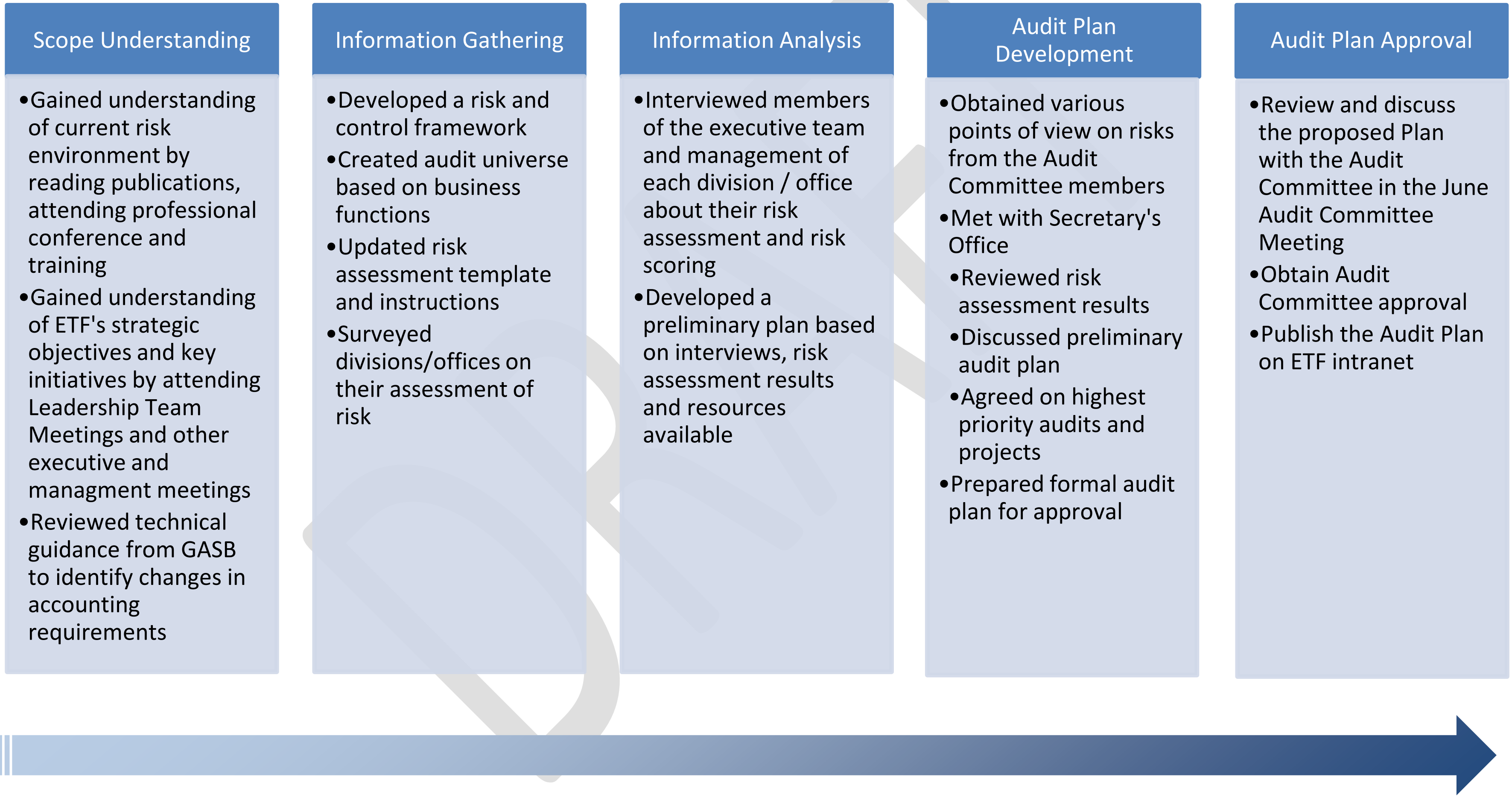
The Office of Internal Audit (OIA) is submitting this Audit Plan (Plan) for biennial period FY2018 and FY2019, as required by the Internal Audit Charter and by the Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing.

The OIA is independent of management and provides risk based, objective assurance and consulting services designed to enhance and protect ETF value. The Plan, including twenty three projects, is designed to provide coverage of key risks, given the existing staff and available budget. The OIA consists of the Director and three full-time audit professional staff. (See Appendix A for the detailed budget.)

Interim changes to the Plan will occur due to changes in business risks, timing of ETF's initiatives, and staff availability. Any significant deviation from the approved Plan will be communicated to the Secretary's Office and the Audit Committee of the ETF Board through quarterly activity reports.

A Risk-Based Audit Planning Approach

The OIA used a systematic approach to identify critical risks to develop the Plan. The risk assessment results of major business functions were summarized and prioritized into an overall audit plan that addresses critical risks while taking into consideration ETF's operational needs. The following was the approach taken in developing the Plan:



Scope Understanding

- 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 Leadership Team Meetings and other executive and managment meetings
- Reviewed technical guidance from GASB to identify changes in accounting requirements

Information Gathering

- Developed a risk and control framework
- Created audit universe based on business functions
- Updated risk assessment template and instructions
- Surveyed divisions/offices on their assessment of risk

Information Analysis

- Interviewed members of the executive team and management of each division / office about their risk assessment and risk scoring
- Developed a preliminary plan based on interviews, risk assessment results and resources available

Audit Plan Development

- Obtained various points of view on risks from the Audit Committee members
- Met with Secretary's Office
  - Reviewed risk assessment results
  - Discussed preliminary audit plan
  - Agreed on highest priority audits and projects
- Prepared formal audit plan for approval

Audit Plan 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 intranet

Types of Projects to Cover Risk Areas

The OIA considered the risk profile of the agency when identifying and prioritizing projects. 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:

Consulting

Responding to high inherent and high residual risks with a quicker turn around time

- Formal assessment with recommendations; no assurance provided
- 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: 240 - 320 hours

Audit

Responding to high inherent and medium residual risks with reassurance provided

- Provide assurance
- Issue audit report
- Estimated effort of each audit: 320 - 640 hours

Agreed-upon Procedures

Routine testing of specific data, transactions and calculations

- Perform specific testing procedures agreed to with management
- Report on results by issuing brief memo to managment
- Estimated effort of each project: 40 - 160 hours

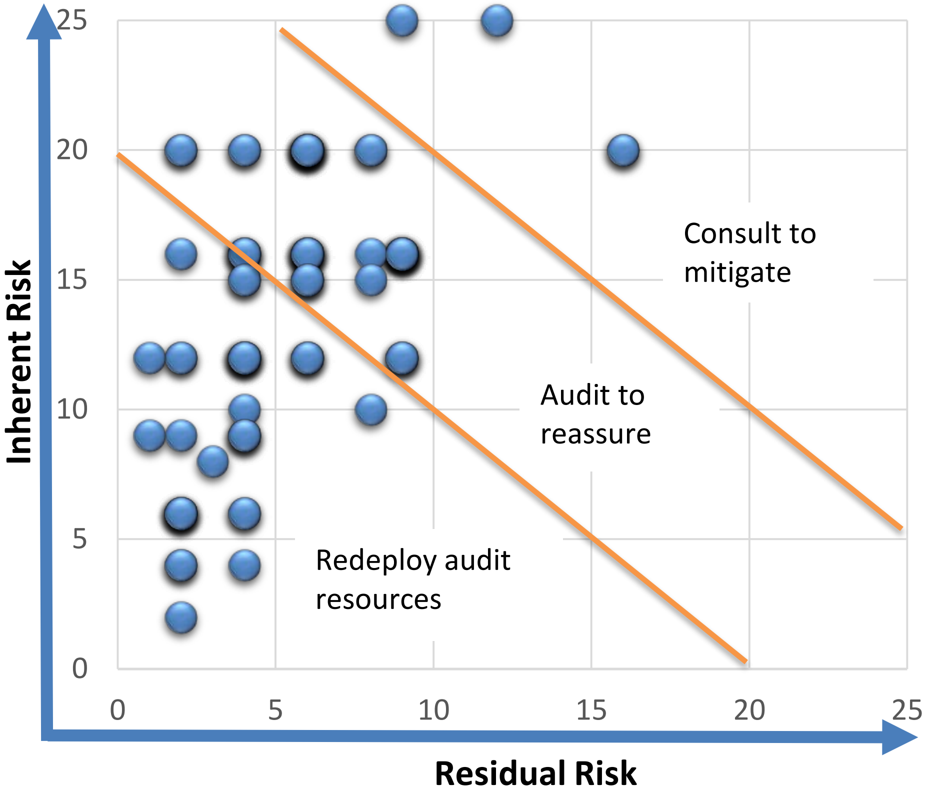
Advisory

- Participate in activities in a non-voting member capacity
- Provide verbal comments or a brief memo to management
- Estimated effort of each advisory service: 10 - 80 hours

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

Agency Risk Profile

In developing the Plan, the Director of the OIA surveyed and discussed with management about the likelihood and impact of risks pertaining to their divisions / offices. (See Appendix B for the detailed instructions of risk assessment.) The identified inherent risks, assessed without consideration of internal controls, and their corresponding residual risks, assessed with consideration of internal controls, were brought together in the form of a heat map (see below). The Plan focuses on the risks in the areas to the right of the first orange line on the heat map (areas of “Audit to reassure” and “Consult to mitigate”).



The following represents key business processes that warrant either consulting work or an audit:

- Information Security
- WRS Earnings Allocation
- WRS Member Account Maintenance
- Third Party Administrator Monitoring
- WRS Employer Reporting
- Cash Receipts and Cash Disbursements
- Benefit Payments

Audit Plan

The tables on this page and the following pages summarize the audit projects to be performed during the biennial period FY2018 and FY2019. Objectives and scopes will be finalized in each project's formal planning phase.

Benefits

Title	Type	Preliminary Objective	7/1/17 - 12/31/17	2018	1/1/2019-6/30/2019
Member Account Maintenance	Audit	Determine whether members' information is maintained accurately in ETF's systems		X	
Employer Reporting	Audit/Follow-up Audit	Determine whether the new employer reporting process of Rollout 2 is working as intended and confirm that management responses to prior audit findings were implemented		X	
Long-Term Disability Insurance (LTDI) Processing	Audit	Determine whether LTDI benefit payment are processed correctly in the Benefit Payment System		X	
Third Party Administrator (TPA) Oversight	Consulting	Facilitate the review of service organization control reports, the assessment of user entity controls and oversee TPA audits to enhance ETF's TPA monitoring (See Appendix C for listing of TPA audits)	X	X	X
Benefits Calculation and Distribution	Agreed-upon Procedures	Semi-annual sample testing of data and transactions to gain additional assurance on WRS benefits' calculation and distribution	X	X	X
Pension Estimates	Advisory	Assess the accuracy of pension estimates			X

Trust Finance

Title	Type	Preliminary Objective	7/1/17 - 12/31/17	2018	1/1/2019-6/30/2019
Cash Receipts and Disbursements	Audit	Evaluate the adequacy and effectiveness of internal controls over cash receipts and disbursements, in particular, WRS contributions, benefit deposits and payments made to TPAs and Vendors for accuracy and appropriate recording	X		
Earnings Allocation	Consulting	Assess and advise on the earnings allocation process for efficient processing and effective internal controls		X	
Effective Rate Calculation	Agreed-upon Procedures	Perform agreed-upon testing procedures to verify the accuracy of the effective rate calculation		X	

Procurement and Contract Administration

Title	Type	Preliminary Objective	7/1/17 - 12/31/17	2018	1/1/2019-6/30/2019
Contract Administration	Audit	Assess the administration of contracts for effective performance monitoring and oversight		X	
Purchasing Delegation	Audit	Ensure that ETF is in compliance with the Department of Administration's Purchasing Delegation Agreement			X
Invoice Processing	Audit	Determine whether the invoice review and approval process is working as intended	X		

Business Continuity and Information Technology

Title	Type	Preliminary Objective	7/1/17 - 12/31/17	2018	1/1/2019-6/30/2019
BAS Data Conversion	Audit	Determine the accuracy of data conversion from legacy systems to the Business Administration System (BAS) for Rollout 2	X	X	
COOP Plan	Audit	Determine whether the business continuity plan is current and adequate in keeping ETF's essential lines of business functioning during an event that disrupts ETF's normal operations			X
Information Security Incidents Response	Audit	Assess whether the information security incidents response plan is effective in supporting ETF’s critical functions and reducing ETF’s risk exposure during an information security incident/breach			X
IT Asset Management	Audit/Follow-up Audit	Evaluate the adequacy and effectiveness of internal controls over IT assets (including software) and confirm prior audit findings were mitigated by management	X		

Information Security and Privacy

Title	Type	Preliminary Objective	7/1/17 - 12/31/17	2018	1/1/2019-6/30/2019
Identity and Access Management	Consulting (co-source)	Assess user identity and access management and provide recommendation for user account life cycle management; evaluate the onboarding and off-boarding process of the V3 product for BAS		X	
Security Awareness	Social Engineering (outsource)	Assess whether the security awareness training is effective and identify areas for improvement		X	
Data Sharing with Vendor	Audit	Determine whether members' personally identifiable information is effectively protected through the data sharing arrangement with vendors		X	
HIPPA Compliance	Audit	Assess ETF's compliance with HIPPA and the effectiveness of privacy breach management	X		

Follow-up Audit

Title	Type	Preliminary Objective	7/1/17 - 12/31/17	2018	1/1/2019-6/30/2019
Full File Compare	Follow-up Audit	Verify corrective actions have been properly implemented by management		X	
Health Insurance Eligibility	Follow-up Audit	Verify corrective actions have been properly implemented by management			X
Income Continuation Insurance	Follow-up Audit	Verify corrective actions have been properly implemented by management		X	

Office of Internal Audit Other Activities

Title	Preliminary Objective	7/1/17-12/31/17	2018	1/1/2019-6/30/2019
Data Analytics	Leverage ACL to incorporate data analytics into audit programs and develop continuous auditing approach when appropriate	X	X	X
Education Reach-out	Prepare and provide training/education sessions to ETF staff, such as risk and control and other topics to improve staff's overall risk awareness and control understanding	X	X	X
Audit Recommendation Follow-up	Follow-up and report on the status of outstanding audit recommendations to the Audit Committee quarterly	X	X	X
Fraud Hotline	Monitor and report fraud hotline results and coordinate the rollout to WRS members if the internal pilot rollout is successful	X	X	X
Conference & Training	Participate in professional conferences and job related trainings	X	X	X
Audit Management Software	Enhance the configuration of TeamMate to better meet the needs of the OIA	X		
Internal Quality Assurance Review	Conduct self-assessment of the OIA's compliance with professional auditing standards	X		
External Quality Assessment	Engage independent qualified assessor to assess and provide an opinion on OIA's compliance with IIA's auditing standards and code of conduct		X	
Biennial Audit Plan	Perform risk assessment and plan audit activities for the next plan years			X

Appendix A

Budget

Working Hours – Available vs. Planned

		Annual Individual		Biennial Total		
		Staff	Director	Staff	Director	
Project Hours - Available						
Available Working Hours		1,664	1,664	9,984	3,328	
Less:						
Continuing Education		40	40	240	80	
Administration		40	280	240	560	
OIA Activities				1,094	940	
Available Hours				**8,410**	**1,748**	
Project Hours - Planned	Estimated Hours	Number of Projects				
Audits and Consulting	480	16	1	7,680	1,632	*
Agreed Upon Procedures and Advisory	80	3		240	48	*
Follow-up Audits	80	3		240	48	*
Planned Hours				**8,160**	**1,728**	

* Based on 20% review hours per project

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”.

Risk Identification

While all employees are encouraged to make possible risks known to the OIA at any time, the OIA’s formal method for identifying new risks will be a biennial survey of key business staff across the agency. In addition, the risk survey will ask survey recipients to review and update existing risks that were previously identified.

Risk Assessment (*Likelihood and Impact*)

In the survey, ETF management will provide an assessment of the identified risks related to their business area. Risks are assessed based on the likelihood of occurrence and the significance of their impact on the objectives. In general, the assessment of risks takes two steps to evaluate how likely the adverse events will occur and how significant their impact will be. First, one must evaluate the risks on an inherent basis – that is, without consideration of existing controls and risk responses in place; second, one must evaluate the risks on a residual basis – that is, after consideration of the adequacy and effectiveness of existing controls and risk responses.

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

Risk Mapping and Risk Monitoring

The survey document will map risks according to the risks’ corresponding scores of likelihood (X Axis) and impact (Y Axis). Comparison will be made between inherent risks and residual risks on the map, as illustrated by the Risk Map of Figure 2 below. Internal controls/mitigating controls/risk responses must be documented by the business owner when high/medium inherent risks are avoided/reduced to medium/low residual risks. Business owners must review and monitor risk status on an on-going basis to ensure risk exposures are managed at an acceptable level. The OIA will exercise judgment in planning audit activities.

Audit Plan Mapping

The survey document will also map risks according to their inherent score (Y Axis) and residual scores (X Axis). When using the risk assessment results to plan audit activities, the OIA will focus on risks that are in the “Consult” and “Reassure” sections of the Audit Plan Map, as illustrated by the Audit Plan Map of Figure 2 below. The OIA will provide consulting services to reduce high residual risks and conduct audits and/or agreed upon procedures to provide reassurance that controls and risk responses identified by management are adequate and operating effectively to keep the inherent risks at the acceptable level.

Figure 2. Risk Map and Audit Plan Map Illustration

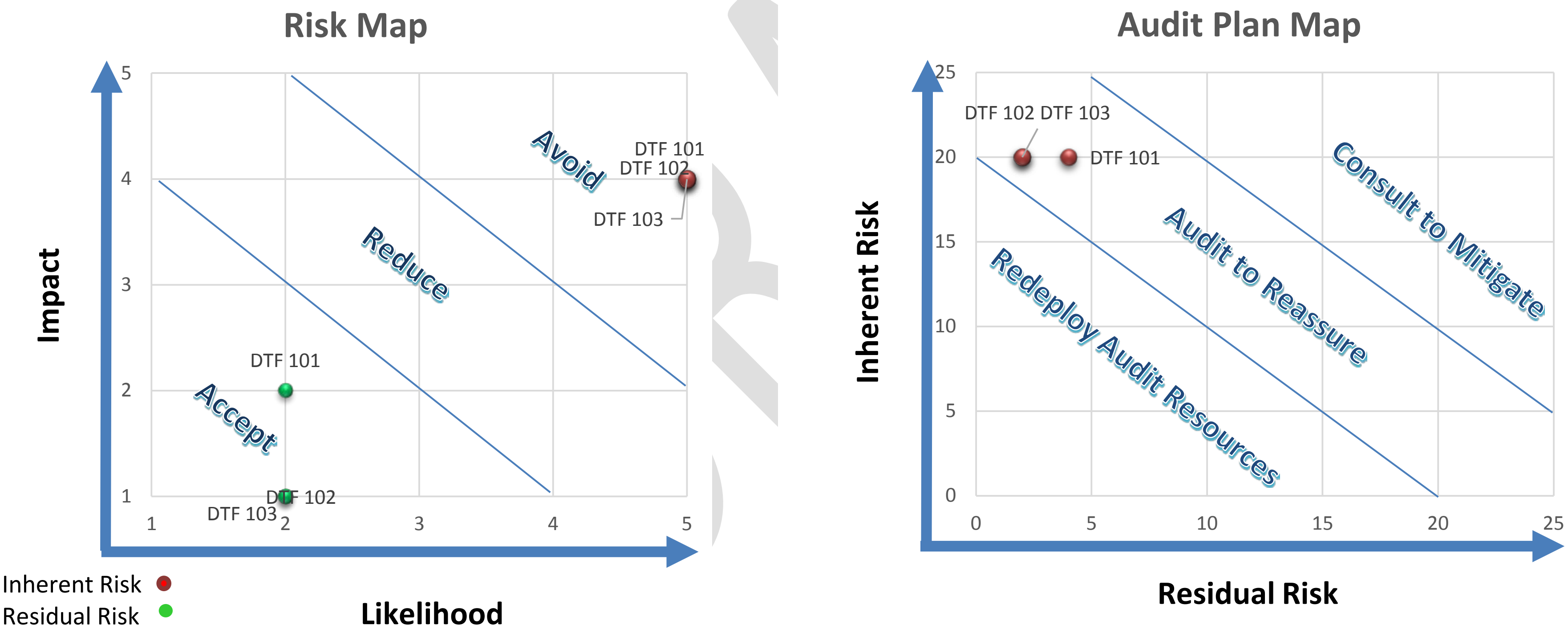


Figure 1. Risk Assessment Guidance – Assessment Criteria and Examples

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

*__Financial Risk__ - Risk that could result in a negative financial impact to the organization in terms 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

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		

Appendix C

Third Party Administrator/Vendor Audits

Third Party Administrator/Vendor Audit

Description	Administrator / Vendor	Type	Audit Firm
Deferred Compensation Program	Empower Retirement	Contract Compliance Audit Financial Audit	Wipfli Coleman & Williams
Income Continuation Insurance & Long Term Disability Insurance	Aetna	Contract Compliance Audit	Wipfli
Standard Health Plan	WPS	Contract Compliance Audit	CTI
Pharmacy Benefit Manager	Navitus	Contract Compliance Audit	TriCast
Employee Reimbursement Accounts / LPFSA / HSA	TASC	Contract Compliance Audit	Wipfli
Life Insurance	Securian	Contract Compliance Audit	Wipfli
Uniform Dental	Delta Dental	Contract Compliance Audit	TBD
Wellness	Staywell	Contract Compliance Audit	TBD
Benefits Administration System	ViTech	Secure Code Review Penetration Testing	TBD