Correspondence Memorandum

Date: May 24, 2019

To: Audit Committee

From: Yikchau Sze, Director
Office of Internal Audit

Subject: FY2020 – FY2021 Internal Audit Plan

ETF requests the Audit Committee approve the draft internal audit plan for fiscal year 2020 through fiscal year 2021.

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 FY2020 – FY2021

Board	Mtg Date	Item #
AUD	6.20.19	5

Internal Audit Plan - Draft

FY 2020 – FY 2021

Office of Internal Audit

May 24 2019

Board	Mtg Date	Item #
AUD	6.20.19	5

EXECUTIVE SUMMARY

The Office of Internal Audit (OIA) is submitting this audit plan (Plan) for biennial period FY2020 and FY2021, 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, Part I, 19 projects that will be preformed by the OIA and, Part II, 13 information technology (IT) projects that will be performed by a consulting firm specialized in IT auditing and consulting services. 6 potential IT projects for FY 2022 and beyond are included for reference. Third party administrator (TPA) audits and vendor audits by independent auditors 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.

PART I – Non Information Technology 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 Leadership Team Meetings and other executive and management meetings
	• Updated the risk and control assessment criteria
	• Created audit universe based on ETF's Business Capability Model of Enterprise Architecture
	• Updated risk assessment template and instructions
	• Surveyed divisions/offices on their assessment of risks
		• 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
			• Discussion 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 and made necessary adjustments to the Plan
			• Finalized draft audit 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 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: 160 - 480 hours

Consulting
Responding to request for formal study or assessment of high risk areas with a quicker turn around 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: 160 - 320 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: 80 – 120 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 develop 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 Process and Change Management

Failure to effectively manage business processes and execute changes identified to improve business processes may result in inefficiency, increased cost, low employee morale and poor service delivery.

2 Customer Relations

Lack of customer engagement, communication, and education may result in operation inefficiency, low customer satisfaction and inadequate support of ETF modernization initiatives.

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 Process and Change Management

- Disability Annuity Benefits
- Locating Beneficiaries
- Establishing Banking Information for Lump Sum Payments
- Variable Transfer
- Medicare Split Contract Invoicing
- Health Insurance Billing

2 Customer Relations

- Employer Call Center Service
- Member Account Maintenance
- Annual Statement of Benefits Abnormal Balance
- Employer Onboarding
- Employer Compliance Review

3 Third-Party

- SOC Report Review
- TPA Contract Compliance
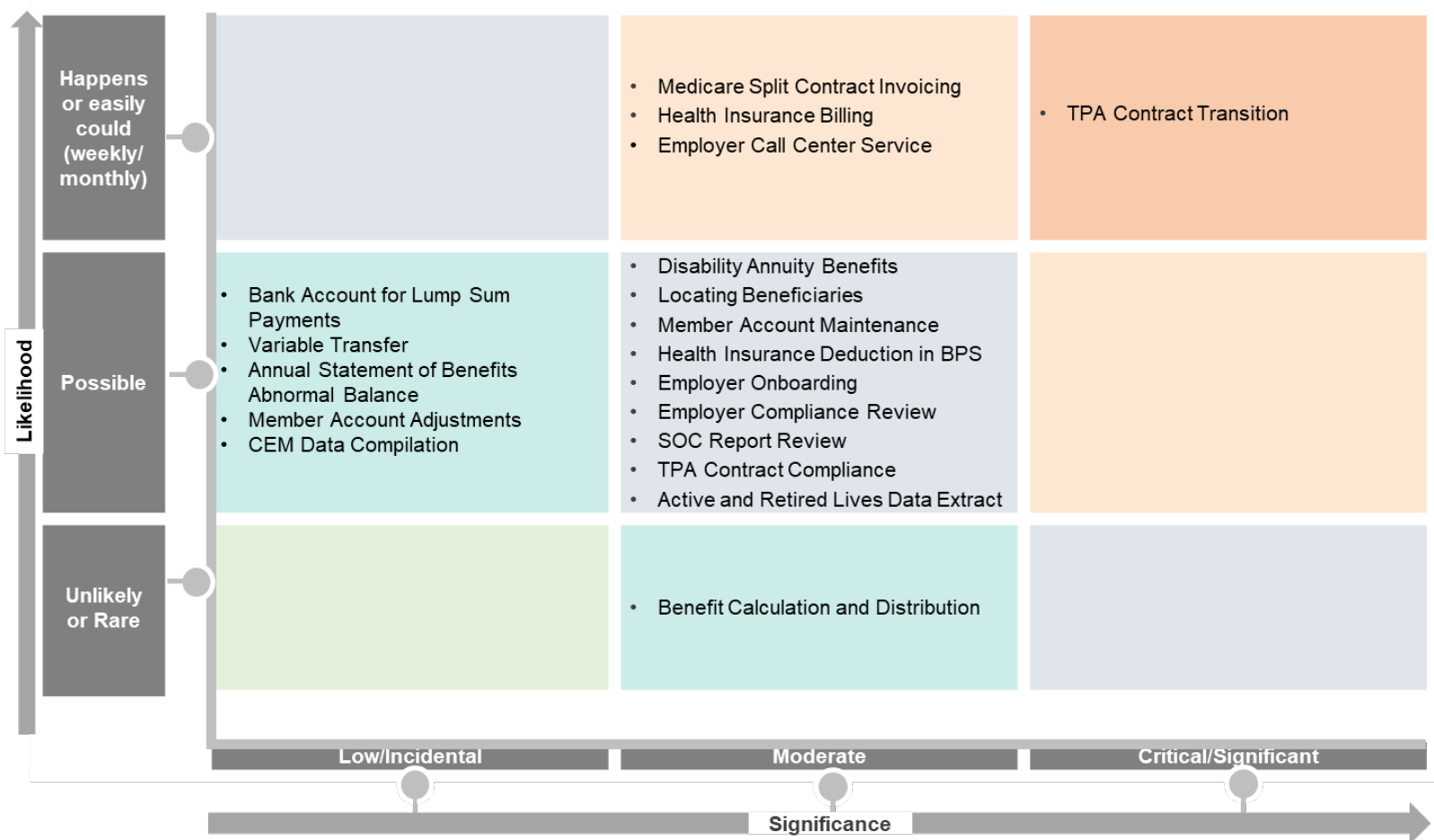- TPA Contract Transition

4 Transaction Processing

- Active and Retired Lives Data Extract for Actuarial Valuations
- Health Insurance Deduction in BPS
- Benefit Calculation and Distribution
- Member Account Adjustments
- CEM Data Compilation

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.

Likelihood	Low/Incidental	Moderate	Critical/Significant
Happens or easily could (weekly/ monthly)		• Medicare Split Contract Invoicing • Health Insurance Billing • Employer Call Center Service	• TPA Contract Transition
Possible	• Bank Account for Lump Sum Payments • Variable Transfer • Annual Statement of Benefits Abnormal Balance • Member Account Adjustments • CEM Data Compilation	• Disability Annuity Benefits • Locating Beneficiaries • Member Account Maintenance • Health Insurance Deduction in BPS • Employer Onboarding • Employer Compliance Review • SOC Report Review • TPA Contract Compliance • Active and Retired Lives Data Extract	
Unlikely or Rare		• Benefit Calculation and Distribution	

Significance →

8

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.

July to Dec 2019

Audit

Active Lives Data Extract

TPA Contract Transition

Health Insurance Billing

Consulting

Annual Statement of Benefits Abnormal Balance

TPA Oversight of SOC reporting and Contract Compliance Audits

Employer Compliance Review

AUP

Benefit Calculation and Distribution

CY 2020

Audit

Retired Lives Data Extract

TPA Contract Transition

Disability Annuity Benefits

Health Insurance Deduction in BPS

Establishing Banking Information for Lump Sum Payments

Member Account Adjustments

AUP

Benefit Calculation and Distribution

Consulting

Employer Call Center Services

Member Account Maintenance

CEM Data Compilation

Employer Onboarding

Employer Compliance Review

TPA Oversight of SOC reporting and Contract Compliance Audits

Locating Beneficiaries

Jan to June 2021

Audit

Variable Transfer

Medicare Split Contract Invoicing

Consulting

Employer Compliance Review

TPA Oversight of SOC reporting and Contract Compliance Audits

AUP

Benefit Calculation and Distribution

ENGAGEMENT DESCRIPTIONS

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

Business Capability - Manage Member and Employer Relations		
Proposed Engagement	**Business Process**	**Engagement Description**
Employer Call Center Service	Manage Employer Call Center	Assess quality of call center service for accuracy and timeliness, and identify areas for improvement
Member Account Maintenance	Provide Member Statement of Account	Evaluate whether member contact information is properly maintained, including review of abandoned account process managed by Member Service Bureau for improvement opportunities
Annual Statements of Benefits Abnormal Balance	Generate Annual Statement of Benefits	Review member accounts with extreme low or negative balances to identify root causes and opportunities for process improvement

ENGAGEMENT DESCRIPTIONS

Business Capability - Manage Benefit Programs		
Proposed Engagement	**Business Process**	**Engagement Description**
Active Lives Data Extract	Active Lives Valuation	Determine accuracy of data extract provided to actuary for the valuation
Retired Lives Data Extract	Retired Lives Valuation	Determine accuracy of data extract provided to actuary for the valuation
TPA Oversight	Manage Health Insurance, Disability, Life Insurance and Deferred Compensation Programs	Facilitate the review of service organization control reports, the assessment of user entity controls and oversee TPA contract compliance audits
TPA Contract Transition	Manage Flexible Spending Account Plan	Ensure accuracy and integrity of data transferred from the existing TPA to the new TPA

ENGAGEMENT DESCRIPTIONS

Business Capability - Manage Benefits Distribution		
Proposed Engagement	**Business Process**	**Engagement Description**
Disability Annuity Benefits	Receive, Verify and Process Disability	Ensure internal controls are adequately designed and operating as intended for the disability annuity claims process
Locating Beneficiaries	Benefits Distribution	Review the process of locating beneficiaries after the death of the annuitant for improvement opportunities and compliance with Statute
Health Insurance Deductions in BPS	Set up Health Insurance Deduction	Ensure the set-up of health insurance deductions in the Benefit Payment System (BPS) for retirees is coordinated with information in the myETF Benefits system that contains health insurance information
Establish Banking Information for Lump Sum Payments	Process Lump Sum Payroll	Ensure the banking information is updated correctly in the Lump Sum Payment System and BPS for correct processing
Benefit Calculations and Distributions	Benefits Distribution	Semi-annual sample testing of data and transactions to gain additional assurance on WRS benefits calculation and distribution

ENGAGEMENT DESCRIPTIONS

Business Capability - Manage Member Account

Proposed Engagement	Business Process	Engagement Description
Member Account Adjustments	Process Account Adjustments	Review member account adjustment entries in the ONE system, in particular the manual adjustments entered before the Adjustment Processor was in place, to ensure the adjustments are processed and calculated correctly
Variable Transfer	Variable Transfer	Ensure adequate controls are in place for the entering and processing of manual variable transfers between the Core Fund and the Variable Fund

Business Capability - Manage Agency Finance

Proposed Engagement	Functional Area	Description
CEM Data Compilation	Manage Contracts and Vendor	Review data compiled for CEM for accuracy and relevance

ENGAGEMENT DESCRIPTIONS

Business Capability - Support Employers		
Proposed Engagement	**Business Process**	**Engagement Description**
Employer Onboarding	Onboard, Enroll and Maintain Employers	Assess employer onboarding process to identify opportunities for better communication and administration of health benefit information by employer agents for their members
Employer Compliance Review	Employer Reporting	Assist the employer compliance review program of the Division of Retirement Services to ensure appropriate employer reporting
Medicare Split Contract Invoicing	Provide Billing Statement	Ensure the Medicare Split Contract invoicing is working as intended
Health Insurance Billing	Process Invoice	Evaluate the health insurance billing process for adequate controls and improvement opportunities

APPENDIX A - Budget

ESTIMATED OIA HOURS

	Audit Director	Internal Auditors	Summary	
Total Hours - Biennial	4,160	12,480	16,640	100%
			-	
Less			-	
Meetings	640	480	1,120	7%
General Administration	300	320	620	4%
Training	80	240	320	2%
Holidays and Personal	216	648	864	5%
Vacation and Sick Leave	400	1,600	2,000	12%
	1,636	3,288	4,924	30%
Internal Audit Activities				
Audit Recommendation Follow-up	32	144	176	
Audit Manual and Charter Update	40	-	40	
Biennial Audit Planning	280	40	320	
Data Analysis Buildout	40	360	400	
Internal Quality Assurance Review	400	280	680	
Fraud Hotline Monitoring	40	80	120	
	832	904	1,736	
Total Available Audit Hours	**1,692**	**8,288**	**9,980**	**60%**
Planned Project Hours				
Consulting and Advisory	643	429	1,072	
Assurance	1,072	7,660	8,732	
Total Planned Hours	**1,715**	**8,089**	**9,804**	**98%**

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								
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				
PROBABILITY	**Description**	**Example of Operational Risk**	**CONSIDERATIONS**	
	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

Figure 2. Audit Coverage

		Risk Assessment			Audit Coverage (Calendar Year)						
		Overall Score	Inherent Risk	Residual Risk	2015	2016	2017	2018	2019	New Audit Plan	
Auditable Areas – by Business Capability Model											
10.4	Manage Change	4.62	High	High						×	*
2.8	Manage Sick Leave Conversion Program	3.65	Medium	Low							
1.6	Provide Employer Communications	3.48	Medium	Low							
4.3	Process Member Requests	3.45	Medium	Low							
1.4	Provide Member Communications	3.42	Medium	Low							
1.1	Provide Member Customer Assistance	3.38	Medium	Low							
5.4	Employer outreach and training	3.37	Medium	Low							
8.2	Manage Legal and Ethical Issues	3.37	Medium	Low							
2.5	Manage Life Insurance Program	3.33	Medium	Low							
11.4	Manage Employee Relations	3.32	Medium	Low							
11.5	Manage Employee Rewards and Retainment	3.30	Medium	Low							
11.3	Manage Employee on Boarding, Development, and Training	3.22	Medium	Low							
8.1	Manage Government and Industry Relationships	3.19	Medium	Low							
8.3	Manage Public Relations Program	3.19	Medium	Low							
2.7	Manage Supplemental Plans	3.19	Medium	Low							
11.8	Manage Employee Communication	3.17	Medium	Low							
11.7	Manage Employee Information and Analytics	3.17	Medium	Low							
11.9	Manage Facilities	3.17	Medium	Low							
7.3	Manage Accounts Receivable	3.13	Medium	Low							
11.2	Recruit, Source, and Select Employees	2.63	Medium	Low							
2.4	Manage Deferred Compensation Program	2.58	Medium	Low							
13.3	Manage Accounts Payable and Expense Reimbursements	2.20	Medium	Low			×				
10.1	Manage business processes	4.25	High	Medium						×	*
10.2	Manage Portfolio, Programs and Projects	3.96	High	Medium						×	*
10.6	Manage Organizational Performance	3.92	High	Medium						×	*
5.2	Employer Reporting	3.85	High	Medium		×		×		×	
4.1	Maintain Member Data	3.80	High	Medium						×	
1.5	Educate and Engage Employer About Available Benefits	3.70	High	Medium							
1.2	Provide Employer Customer Assistance	3.65	High	Medium						×	
4.2	Validate Member Data	3.62	High	Medium						×	
1.3	Educate and Engage Member About Available Benefits	3.61	High	Medium						×	
11.1	Develop and Manage HR Planning, Policies, Strategies	3.56	High	Medium							
2.2	Manage Health Insurance Programs	3.56	High	Medium	×	×				×	
5.1	Onboard, Enroll and Maintain Employers	3.51	High	Medium						×	
5.3	Provide Billing Statements	3.50	High	Medium						×	
2.1	Manage Wisconsin Retirement System Program	3.46	High	Medium						×	
13.4	Manage Contracts and Vendors	3.45	High	Medium				×		×	
7.2	Manage Financial Reporting	3.30	High	Medium							
14.3	Manage Policy and Compliance	3.27	High	Medium				×		×	
6.1	Determine Retirement Eligibility	3.21	High	Medium							
7.1	Account for Benefit Activity	3.13	High	Medium				×			
3.1	Receive Benefit Application	3.04	High	Medium						×	
3.4	Calculate Payment	3.02	High	Medium		×				×	
2.3	Manage Disability Programs	3.02	High	Medium	×				×		
7.4	Manage Tax Compliance and Reporting	2.98	High	Medium		×	×				
13.1	Manage Procurement	2.97	High	Medium					×		
6.2	Prepare Benefit Estimates:	2.83	High	Medium				×			
3.2	Verify Eligibility	2.81	High	Medium	×		×	×		×	
13.2	Manage Agency Operating Budget	2.75	High	Medium							
3.5	Issue Payment	2.72	High	Medium		×				×	
2.6	Manage Flex Spending Account Plan	2.68	High	Medium				×		×	
3.3	Process Benefit Applications/Payment Requests	2.62	High	Medium			×			×	
10.5	Develop and Manage Enterprise Knowledge	4.29	Medium	Medium							
6.3	Provide Member Planning Sessions (counseling)	3.89	Medium	Medium							
11.6	Manage Employee Redeployment & Retirement	2.85	Low	Low							
12.1	Develop and Maintain Business Partnerships									outsourced	
12.2	Develop and Execute Business –to-Technology Strategy									outsourced	
12.3	Optimize IT Quality & Velocity									outsourced	
12.4	Manage Enterprise Information									outsourced	
12.5	Exploit Technology & Innovation									outsourced	
12.6	Manage Technology Services/Solutions									outsourced	
12.7	Architect & Integrate Solutions									outsourced	
14.2	Manage Enterprise Risk									outsourced	

*Consulting hours reserved

PART II – Information Technology Audit Plan

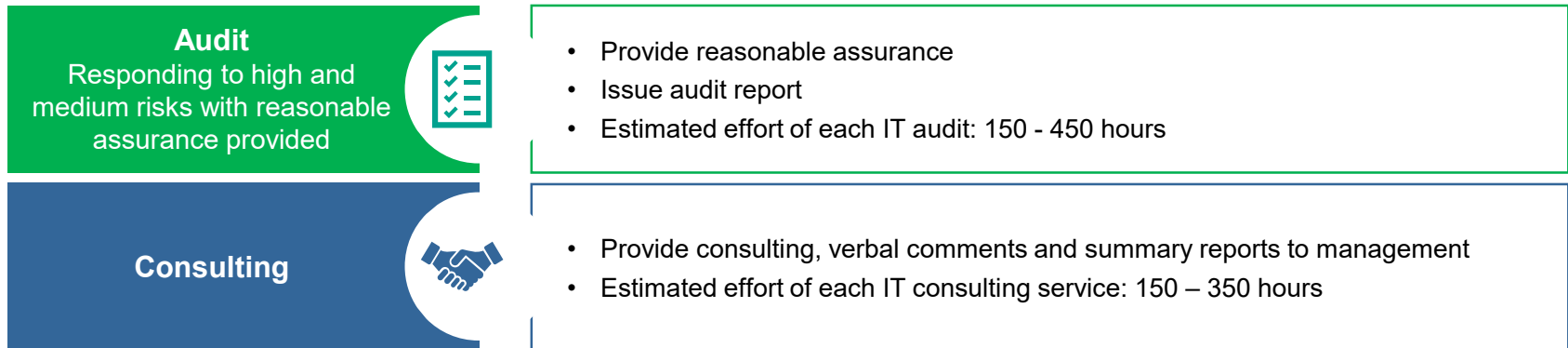# *A RISK-BASED AUDIT PLANNING APPROACH*

Using a systematic approach to conduct an IT audit risk assessment is a foundational step to form the basis for future IT audit activities. 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. The following was the approach taken in developing the IT audit plan:

Scope Understanding	Information Gathering	Information Analysis	Audit Plan Development	Audit Plan Approval

• Gained understanding of ETF's IT environment by reviewing IT strategic objectives, key initiatives, policies and procedures, and prior audit results	• Interviewed members of IT management team, and subject matter experts from representative business areas and assessed their input
	• Created IT risk register
		• Created heat map using the defined impact and likelihood criteria
		• Developed a preliminary IT audit plan based on risk assessment results
			• Discussion with ETF management on
			  • Risk assessment results
			  • Concerns and priorities
			  • Timelines of proposed engagements
			• Finalized draft IT audit plan for approval
				• Review and discuss the proposed IT audit plan with the Audit Committee in the June Audit Committee Meeting
				• Obtain Audit Committee approval

TYPES OF PROJECTS TO COVER IT 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, independent audits will be performed to provide reasonable assurance that management identified internal controls are adequate and operating effectively; while, consulting services will be provided to reduce high residual risk.

There are two levels of review will be used to cover IT risk areas:

Audit Responding to high and medium risks with reasonable assurance provided	• Provide reasonable assurance • Issue audit report • Estimated effort of each IT audit: 150 - 450 hours
Consulting	• Provide consulting, verbal comments and summary reports to management • Estimated effort of each IT consulting service: 150 – 350 hours

RISK THEMES

Risks were compiled from all the interview sessions and aggregated to remove redundancies. This process, by its nature, is *subjective* and based on the team's collective experience performing these types of assessments. The risks were then categorized into the following four "Risk Themes".

1 **Information Security**

Failure to properly protect sensitive information for employees may result in unauthorized use and/or disclosure.

2 **IT Organizational Effectiveness**

IT processes may not be consistently designed and executed to provide reasonable protection against general IT risks. Unauthorized or unintended changes to critical systems and sub-systems may negatively impact the integrity of applications.

3 **Legacy Application Support**

Changes to code and the inability to provide technical support in a timely manner may result in downstream issues and inefficiencies and may potentially impact users when performing their day to day tasks.

.

4 **Business Continuity Management**

Critical business processes and supporting technology systems may not be available or recoverable to an acceptable level in the event of a significant disruption.

AUDIT FOCUS AREAS

There are a number of 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 Information Security

- Data Protection
- Data Classification
- End Point Configuration
- Identity Access Management (IAM)
- Network Monitoring
- Records Retention
- Segregation of Duties (SoD)

2 IT Organizational Effectiveness

- DET Roles & Responsibilities
- E-Discovery
- IT Process Documentation
- IT Portfolio Management
- IT Project Management
- IT Resource Management (People)
- IT Training / Skillsets
- Third Party Vendors

3 Legacy Application Support

- IT Architecture
- Legacy Application Support
- System Implementation
- Data Quality

4 Business Continuity Management

- Business Continuity
- Disaster Recovery

APPENDIX C – Third-Party Administrator and Vendor Audits

TPA AND VENDOR AUDITS

Program	TPA / Vendor	Service Type	Audit Firm
Deferred Compensation Program	Empower Retirement	- Contract Compliance Audit - Financial Statement Audit	- Wipfli - TBD
Income Continuation Insurance (ICI)	The Hartford	Contract Compliance Audit	Wipfli
Pharmacy Benefit Manager	Navitus	Contract Compliance Audit	PillarRx
Employee Reimbursement Account/HSA/Commuter Benefits	- TASC (CY 2019) - CYC (CY 2020)	Contract Compliance Audit	Wipfli
Life Insurance	Securian	Contract Compliance Audit	Wipfli
Uniform Dental	Delta Dental	Contract Compliance Audit	CTI
ICI and Duty Disability	Milliman	Actuarial Valuation Audit	The Segal Company
Accumulated Sick Leave Conversion	Gabriel Roeder Smith & Company	Actuarial Valuation Audit	Milliman