FRTIB FY 2019 Enterprise Risk Assessment

OFFICE OF ENTERPRISE RISK MANAGEMENT (OERM)

December 17, 2018

Thrift Savings Plan
FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE · Washington, DC · 20002
1-877-968-3778 · tsp.gov

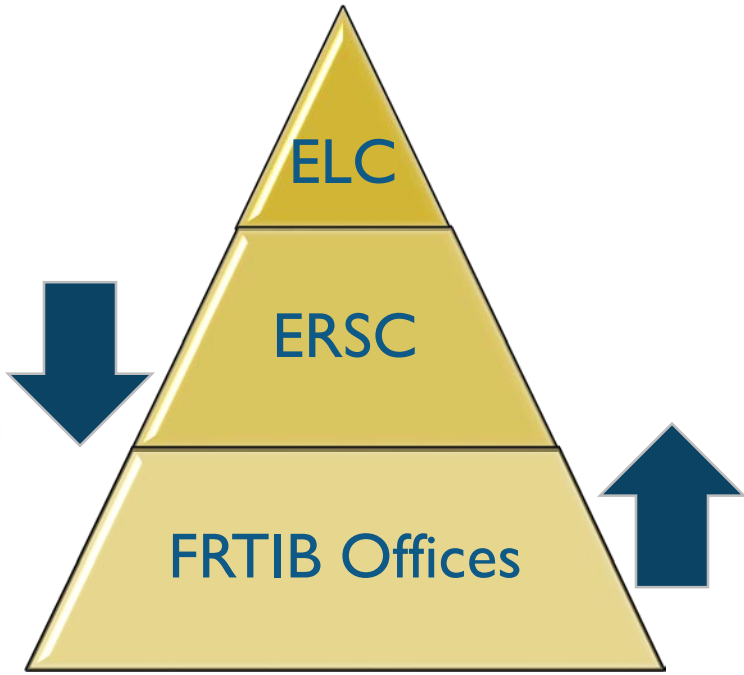
Agenda

- Enterprise Risk Assessment Process
- FRTIB 2019 Enterprise Risk Profile/Dashboard
- Enterprise Risk Management Key Initiatives

Enterprise Risk Assessment Process

- Audit findings
- Internal Control Review Results
- Prior Year Risks

- Assessments
- Projects

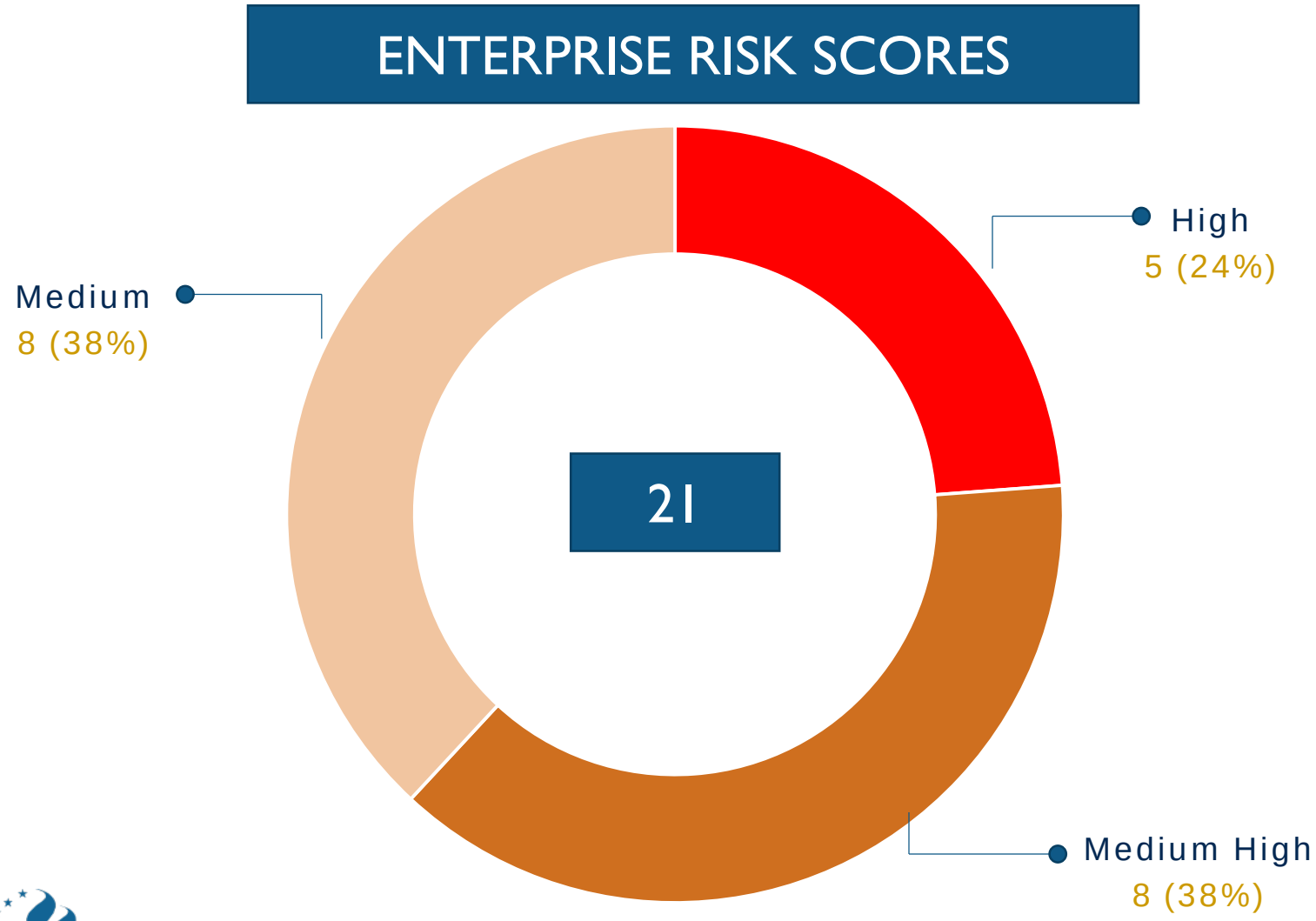


ELC: Executive Leadership Council
ERSC: Enterprise Risk Steering Committee

Enterprise Risk Assessment Process

- Developed Initial FY 2019 Enterprise Risk Profile/Dashboard.
- Enterprise Risk Steering Committee and Risk Owners reviewed the Enterprise Risk Profile/Dashboard and recommended for approval.
- Executive Leadership Council reviewed the Profile/Dashboard.
- Executive Director approved the Profile/Dashboard.
- Brief the FRTIB Board on the Agency 2019 Risk Profile/Dashboard.

FY 2019 Enterprise Risk Profile/Dashboard Summary



Thrift Savings Plan

FRTIB Enterprise Risk Profile/Dashboard (FY18 -19)

Risk	Statement	Executive Owner	Prior Results (FY 2018)	Current Results (FY 2019)	Accomplishments
Information Security	Failure to protect and secure information that results from weaknesses or gaps in a security program allowing unauthorized access, denial of services or compromise of sensitive information.	**OTS**	**High**	**High**	• Implemented the Trusted Internet Connection (TIC), a DHS requirement; allows Agency and DHS to better monitor internet connections for suspicious activity. • Moved from "Ad Hoc" to "Defined" in 3 FISMA domains (as assessed by independent auditors). • 100% BOD 18-01 compliant, 3 months ahead of schedule. • 0 vulnerabilities (all categories) for >6 months in NCATS scans. • Network access control "agents" installed on all end points (laptops, servers, etc.).
Disaster Recovery	Lack of adequate processes to ensure service continuity across the entire range of potential disruptions covering the primary and alternate processing facilities, results in a loss of FRTIB status as a trusted provider of retirement services.	**OTS**	**High**	**High**	• Successfully restored operations after two outages with minimal participant impact. • Moved to automatic failover state for internet services between VA and PA data centers. • Preparations underway to perform comprehensive "failover" test in summer 2019—incremental tests of subcomponents commenced.
Business Continuity	Lack of an implemented formal process and technology to enable quick resumption of critical business processes impacted by natural or human events, results in a loss of FRTIB status as a trusted provider of retirement services.	**ORM**	**High**	**High**	• Maximum Tolerable Disruption Times (MTDs) for Critical Business Processes updated and approved by COO April 2018. Supporting OTS in work with TESS to prioritize and implement Disaster Recovery that meets agency-approved MTDs. • Tabletop Business Continuity exercises at FRTIB and critical contractors conducted from May-July 2018. • Business Continuity/Disaster Recovery exercises conducted April and June 2018.
Insider Threat Management	Failure to independently monitor, protect and secure information assets from insiders who have access to FRTIB's network, system, or data, and/or if employees intentionally exceed or intentionally use that access, results in a significant impact to the confidentiality, integrity, or availability of FRTIB's information and/or information systems.	**OERM**	**High**	**High**	• Completed Current State Assessment and Gap Analysis resulting in an initial implementation roadmap. • Established a dedicated team and commenced the implementation of a formal Insider Threat program.
TSP Fraud	Fraudulent/unauthorized access to TSP participant funds could result in financial damage plus a loss of FRTIB status as a trusted provider of retirement services.	**OPS**	**High**	**High**	• Changed authentication process when participant uses SSN for verification. • Redesigned entire contact center Quality Assurance (QA) program to place a greater emphasis on account security. • Removed select money out forms from public website to drive participants to wizards on authenticated website.
Configuration Management	Lack of a formal process to ensure system changes in the production environment that processes critical business applications are authorized and cannot be modified, results in the risk of outages and security breaches through the lack of visibility and tracking of changes to FRTIB systems.	**OTS**	**High**	**Medium High**	• Completed the validation of Configuration Management policies, procedures and Standard Operating Procedures. Created an Application Change Control Board (CCB) Charter. • Developed an Application CCB that provides governance and approvals for application changes prior to production release. • Created a Configuration Management Plan for Infrastructure/Applications.

Enterprise Risk Profile/Dashboard Detail (FY18 -19)

Risk	Executive Owner	Prior Results (FY 2018)	Current Results (FY 2019)
Stakeholder (Participant) Confidence	OED	Medium High	Medium High
Data Privacy	OGC	Medium High	Medium High
Internal Control Program*	OERM		Medium High
Contract Management	OCFO	Medium High	Medium High
Acquisition Planning	OEP	Medium High	Medium High
Governmental and External Stakeholder Events	OED	Medium High	Medium High
Statutory Compliance**	OPS	Medium High	
Contract Administration	OCFO	Medium High	Medium High

Risk	Executive Owner	Prior Results (FY 2018)	Current Results (FY 2019)
Human Capital Management	ORM	Medium	Medium
Non-integrated systems and processes	OCFO	Medium	Medium
Data Governance	OEP	Medium	Medium
Compliance	OGC	Medium	Medium
Economic Change Events	OI	Medium	Medium
Project Management	OEP	Medium	Medium
Records Retention	ORM	Medium	Medium
Unforeseen Senior Leadership Change	OED	Medium	Medium

*Enterprise Risk added to FY 2019 Profile/Dashboard.
**Enterprise Risk Mitigated in FY 2018 and removed from FY 2019 Profile/Dashboard.

Upcoming Key Initiatives

- Promote a more risk aware culture.
- Support risk owners to develop and implement Risk Treatment Plans.
- Refine methodology and collaborate with Agency offices to mature Enterprise Risk Management program.
- Introduce and promote Agency Risk Appetite Statement.