Enterprise Risk Management Update

PRESENTED BY

JAY AHUJA, CHIEF RISK OFFICER

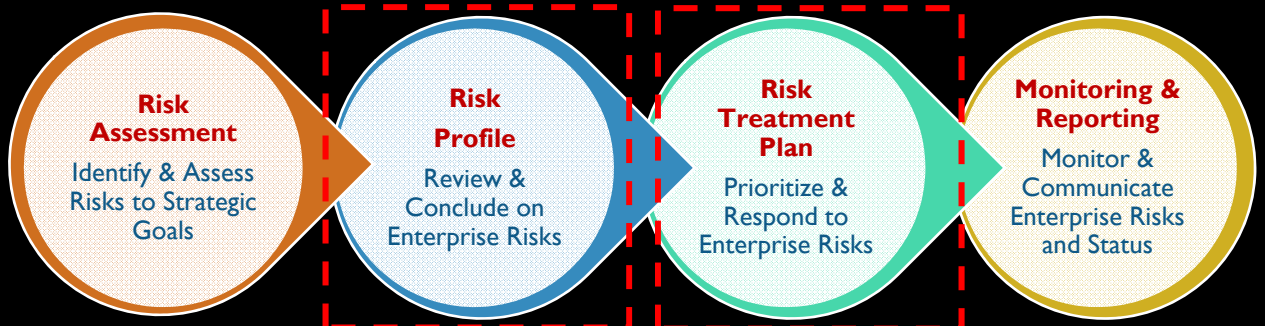
OFFICE OF ENTERPRISE RISK MANAGEMENT (OERM)

March 23, 2020

AGENDA

- Enterprise Risk Management Program Cycle
- Calendar Year (CY) 2020 Enterprise Risk Profile
- CY 2020 Enterprise Risk Treatment Plans
- Upcoming Key ERM Initiatives

FRTIB'S ANNUAL ERM PROGRAM CYCLE



- OERM
- Executive Owners
- Office SMEs

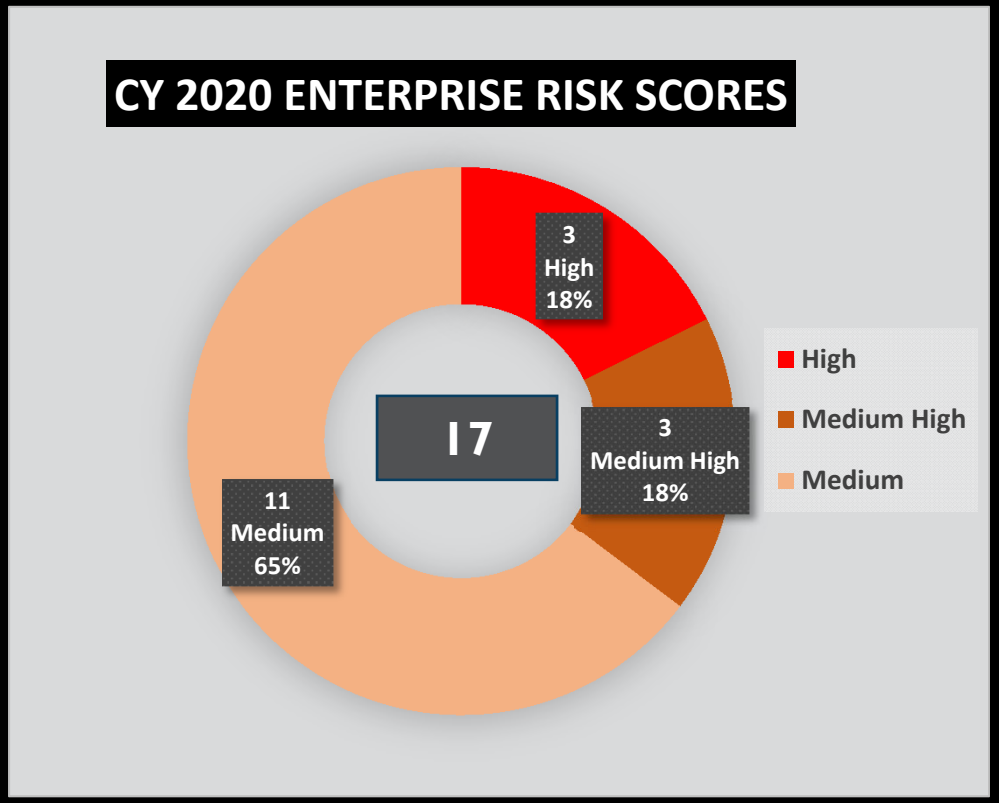
- OERM
- Executive Owners
- Enterprise Risk Steering Committed (ERSC)
- Executive Leadership Council (ELC)
- Board

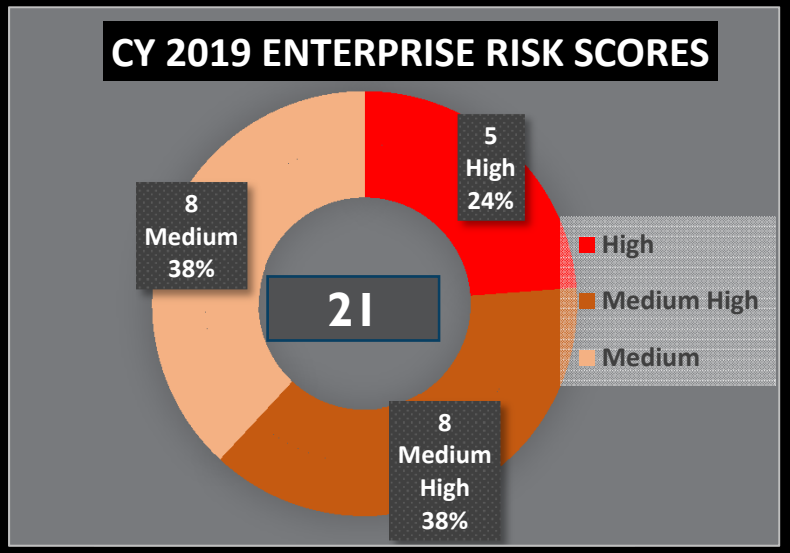
- OERM
- Risk Owners/SMEs
- ERSC
- ELC
- Board

- OERM
- ERSC
- ELC
- Board

✓ Repeatable
✓ Collaborative
✓ Accountable
✓ Transparent

ENTERPRISE RISK PROFILE (CY 2020 - 2019)





FRTIB ENTERPRISE RISK PROFILE – HIGH RISKS

Risk	Statement	Executive Owner	Prior Rating/Score (CY 2019)	Current Rating/Score (CY 2020)	Accomplishments (CY 2019)
Insider Threat Management	There is a risk that an Insider may maliciously or unintentionally engage in activities that compromise data, critical assets, business processes or computer networks.	OERM	**High (20)**	**High (20)**	• Insider Threat Program Policy developed and approved. • Conducted an Analysis of Alternatives to host Insider Threat/Hotline services. • Developed the Insider Threat Program staffing requirements. • Developed training material for all FRTIB staff. • Developed list of potential risk indicators (PRIs).
Information Security	There is a risk the Agency may fail to adequately protect and secure information resulting in unauthorized access, denial of services or compromise of sensitive information.	OTS	**High (25)**	**High (20)**	• Completed Identity, Credential, and Access Management (ICAM) Phase 3 completed. • Federal Information Security Management Act (FISMA) Maturity Process Health Metrics Framework developed. • Network Access Control (NAC) implementation completed. • Phase 1 DHS Continuous Diagnostics and Mitigation (CDM) dashboard launched. • Completed Analysis of Alternatives for Security Operations Center-as-a-Service (SOCaaS).
Disaster Recovery/Business Continuity	There is a risk the Agency may not be able to restore critical business processes within maximum tolerable downtimes resulting in significant disruption to FRTIB critical processes.	OTS	**High (25)**	**High (20)**	• Executed a successful disaster recovery tabletop exercise. • Increased the mainframe storage at PA Data Center and VA Data Center by at least 33%. • Established session initiation protocol (SIP) trunks at PA Data Center and VA Data Center. • Successful completion of Mainframe hosted applications smoke test.

FRTIB ENTERPRISE RISK PROFILE – MEDIUM HIGH RISKS

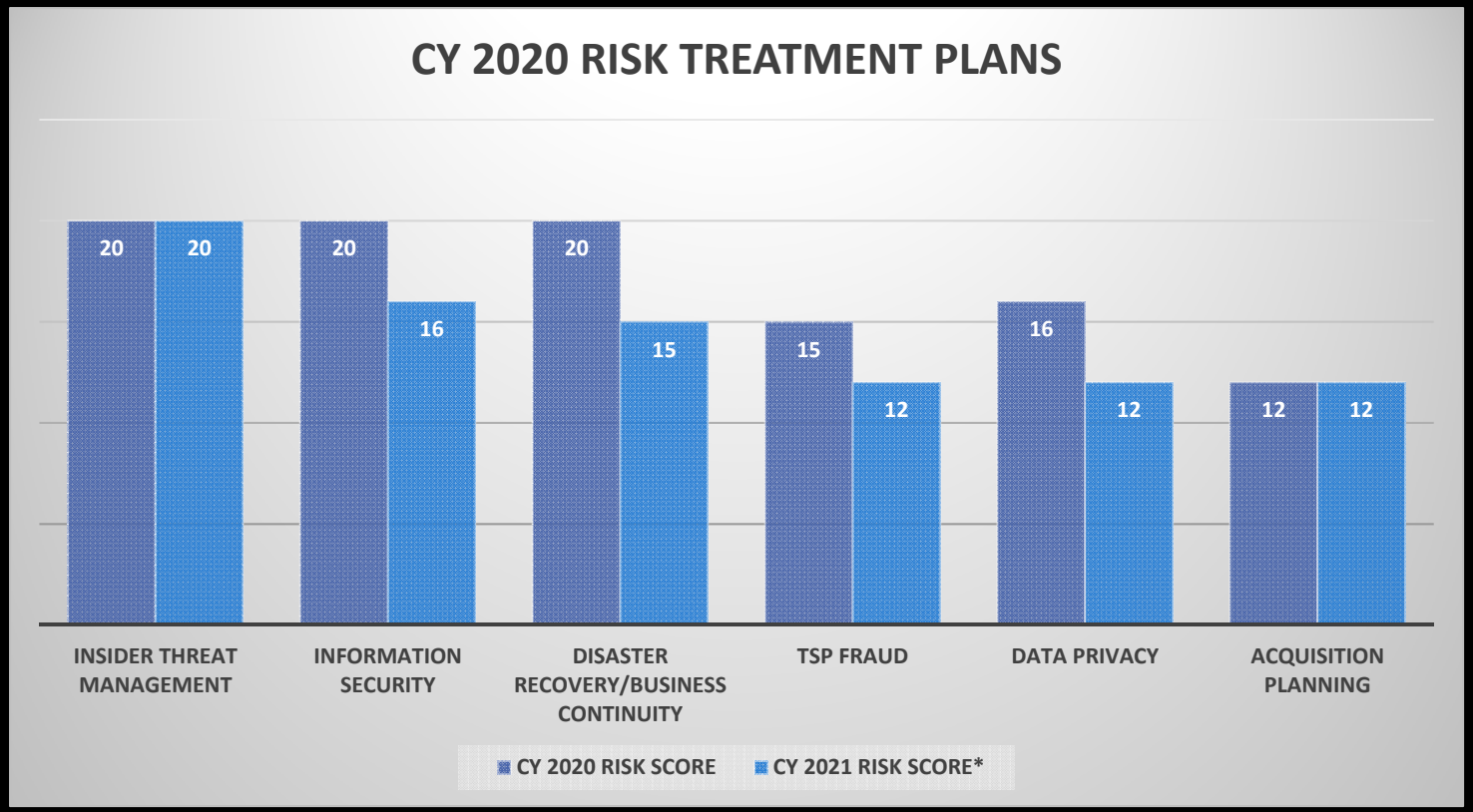
Risk	Statement	Executive Owner	Prior Rating/Score (CY 2019)	Current Rating/Score (CY 2020)	Accomplishments (CY 2019)
TSP Fraud	There is a risk fraudulent actors may obtain unauthorized access to TSP participant accounts resulting in financial loss to the participants or reputational damage to the FRTIB status as a trusted provider of retirement services.	OPS	**High (20)**	**Medium High (15)**	• Implemented mandatory two factor authentication. • Established new holds for participant elected hold, spousal misconduct hold, and manual mail hold on returned mail. • Automated watchlist to monitor suspicious withdrawal activity. • Deployed OMNI software change for faster withdrawal notification to participant. • Removed withdrawal forms from public website and began requiring online initiation/submission of withdrawal requests.
Data Privacy	There is a risk the Agency has not integrated appropriate privacy controls in FRTIB business programs and strategic initiatives resulting in the improper collection, use, or disclosure of personally identifiable information, which could create legal risk, action by oversight entities, or the loss of FRTIB status as a trusted financial provider.	OGC	**Medium High (16)**	**Medium High (16)**	• Began to integrate NIST privacy controls into the Assessment & Authorization process • Finalized Privacy Risk Management Policy, PII Handling Policy, and Privacy Training Procedures • Revised Breach Response policy and procedures • Conducted a Breach Response Tabletop exercise • Made significant improvement completing PTAs and PIAs in a timely manner
Acquisition Planning	There is a risk the Agency may not obtain products and services necessary to support the FRTIB and TSP programs resulting in significant cost overruns and inability to support strategic initiatives.	OEP	**Medium High (12)**	**Medium High (12)**	• Master Schedule updated to reflect re-baselined (shortened) procurement schedules • Created internal websites, guides, templates and forms • Launched monthly newsletter • Published dates for training sessions

FRTIB ENTERPRISE RISK PROFILE – MEDIUM AND LOW RISKS

Risk	Executive Owner	Prior Results (CY 2019)	Current Results (CY 2020)
Human Capital Management	ORM	Medium	Medium
Procurement	OCFO	Medium High	Medium
Data Governance	OEP	Medium	Medium
Records Retention	ORM	Medium	Medium
Configuration Management	OTS	Medium High	Medium
Contract Management	OCFO	Medium High	Medium

Risk	Executive Owner	Prior Results (CY 2019)	Current Results (CY 2020)
Compliance	OGC	Medium	Medium
Project Management	OEP	Medium	Medium
Internal Control Program	OERM	Medium High	Medium
Economic Change Events	OI	Medium	Medium
Non-integrated systems and processes	OCFO	Medium	Medium
Unforeseen Senior Leadership Change	OED	Medium	Low
Stakeholder (Participant) Confidence	OED	Medium High	
Governmental and External Stakeholder Events	OED	Medium High	

IMPACT OF RISK TREATMENT PLANS



Risk Rating	Score
High	20-25
Medium High	10-19
Medium	5-9
Medium Low	3-4
Low	1-2

*** Future Risk Score: Projected CY 2021 risk score, which reflects the successful implementation of the Risk Treatment Plan.**

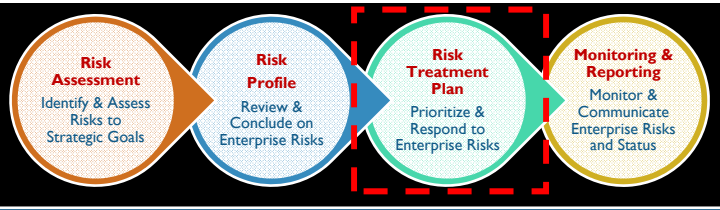
UPCOMING KEY ERM INITIATIVES

Are we taking the right amount and type of risks to achieve our goals?

What are the acceptable level of variance in performance to achieve business objectives?

APPENDIX

Risk: Insider Threat Management



Statement	Executive Owner	CY 2020 Risk Score	CY 2021 Risk Score*	Summary of Actions Required to Treat Risks
There is a risk that an Insider may maliciously or unintentionally engage in activities that compromise data, critical assets, business processes or computer networks.	OERM	High (20)	High (20)	• Enter into agreement with federal shared service provider to host Insider Threat and Hotline services • On-board Insider Threat Analyst • Implement interfaces to ingest automated and manual inputs to the Insider Threat Tool used by provider • Train FRTIB staff on their role in sustaining the Insider Threat and Hotline services • Monitor Insider Threat activities reported by the provider and refine/streamline processes, as needed

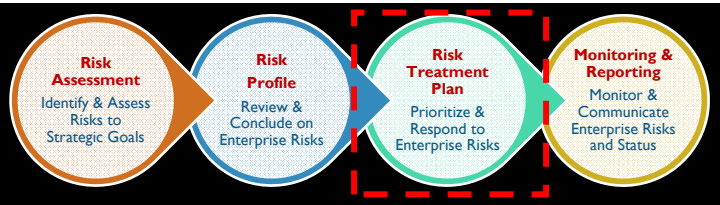
* Future Risk Score: Projected CY 2021 risk score, which reflects the successful implementation of the Risk Treatment Plan.

Risk: Information Security

Statement	Executive Owner	CY 2020 Risk Score	CY 2021 Risk Score*	Summary of Actions Required to Treat Risks
There is a risk the Agency may fail to adequately protect and secure information resulting in unauthorized access, denial of services or compromise of sensitive information.	OTS	High (20)	Medium High (16)	• Engage in periodic external assessments of Agency infrastructure to discover vulnerabilities • Increase the Agency's Federal Information Security Modernization Act of 2014 (FISMA) maturity Process Health Measurement (PHM) • Update System Assessment and Authorization (SA&A) packages for all Agency systems • Implement the Information Security Continuous Monitoring (ISCM) and DHS' Continuous Diagnostic & Mitigation Program • Implement a High Value Asset (HVA) Program • Implement OTS Operational Metrics Framework • Enhance Agency Supply Chain Risk to include vendors' cybersecurity risk posture • Enhance the Contingency Planning FISMA domain • Transition to Security Operations (SOC) as a Service Migration

*** Future Risk Score: Projected CY 2021 risk score, which reflects the successful implementation of the Risk Treatment Plan.**

Risk: Disaster Recovery/Business Continuity



Statement	Executive Owner	CY 2020 Risk Score	CY 2021 Risk Score*	Summary of Actions Required to Treat Risks
There is a risk the Agency may not be able to restore critical business processes within maximum tolerable downtimes resulting in significant disruption to FRTIB critical processes.	OTS	High (20)	Medium High (15)	• Migrate email and office automation applications to Office 365. • Upgrade and migrate mainframes at VA data center and PD data center. • Perform annual real-time live DR test by executing a failover/failback exercise of both datacenters (VDC/PDC).

*** Future Risk Score: Projected CY 2021 risk score, which reflects the successful implementation of the Risk Treatment Plan.**

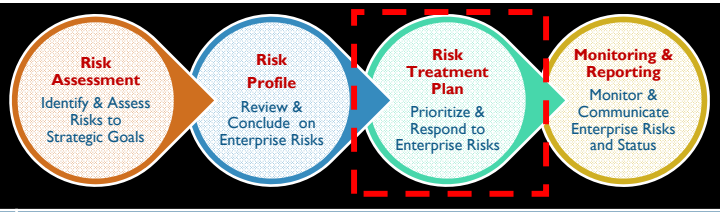
Risk: TSP Fraud

Statement	Executive Owner	CY 2020 Risk Score	CY 2021 Risk Score*	Summary of Actions Required to Treat Risks
There is a risk fraudulent actors may obtain unauthorized access to TSP participant accounts resulting in financial loss to the participants or reputational damage to the FRTIB status as a trusted provider of retirement services.	OPS	Medium High (15)	Medium High (12)	• Deploy Faster Transaction Notifications - Notifications will be sent to participants when money out transactions are submitted and processed or rejected. • Implement a locator service to provide more current address information about participants • Account Security Analysis - complete a risk analysis/vulnerability assessment of the TSP account security procedures and processes as it pertains to outgoing money transactions, identify potential opportunities for strengthening the TSP account security procedures for outgoing money transactions, and identify associated industry best practices with regard to outgoing money transactions (e.g. loans, withdrawals, death and legal disbursements). • ACH Payment Processing Hold Period - Consider a 3-5 day hold period when processing ACH payment requests to allow additional time for the participant to confirm or deny the transaction.

Thrift Savings Plan

*** Future Risk Score: Projected CY 2021 risk score, which reflects the successful implementation of the Risk Treatment Plan.**

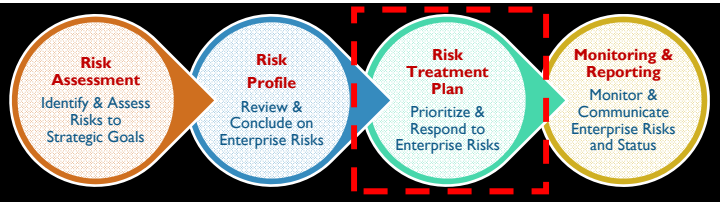
Risk: Data Privacy



Statement	Executive Owner	CY 2020 Risk Score	CY 2021 Risk Score*	Summary of Actions Required to Treat Risks
There is a risk the Agency has not integrated appropriate privacy controls in FRTIB business programs and strategic initiatives resulting in the improper collection, use, or disclosure of personally identifiable information, which could create legal risk, action by oversight entities, or the loss of FRTIB status as a trusted financial provider.	OGC	Medium High (16)	Medium High (12)	• Ensure that FRTIB employees understand how to appropriately manage personally identifiable information, and seek advice from the Privacy Division when necessary • Ensure that the Privacy Division is aware of new applications and systems and evaluates all associated privacy risks • Ensure that the Privacy Division has up-to-date information about privacy risks for FRTIB systems by reviewing, and, if necessary, updating PIAs on an annual basis • Ensure that privacy risks are considered throughout the information system lifecycle by integrating privacy and NIST SP 800-53 privacy controls into the Assessment & Authorization process • Ensure that the Agency's Breach Response process remains up-to-date and effective

* Future Risk Score: Projected CY 2021 risk score, which reflects the successful implementation of the Risk Treatment Plan.

Risk: Acquisition Planning



Statement	Executive Owner	CY 2020 Risk Score	CY 2021 Risk Score*	Summary of Actions Required to Treat Risks
There is a risk the Agency may not obtain products and services necessary to support the FRTIB and TSP programs resulting in significant cost overruns and inability to support strategic initiatives.	OEP	Medium High (12)	Medium High (12)	• Create shared definition/shared understanding of enterprise level acquisition, to include, acquisition characteristics, categories, level of review and decision authority. • Establish an Acquisition Framework • Define acquisition total lifecycle cost • Update Existing Acquisition Policy • Establish Enterprise Acquisition Procedures

*** Future Risk Score: Projected CY 2021 risk score, which reflects the successful implementation of the Risk Treatment Plan.**