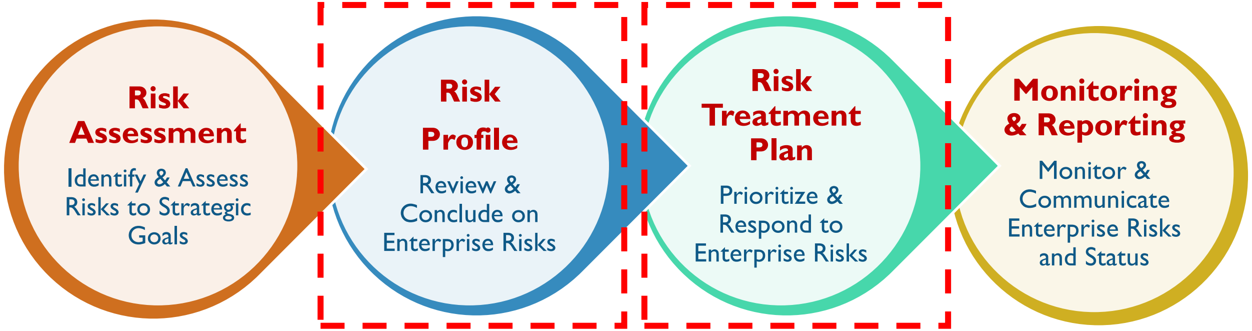
Enterprise Risk Management Update

Presented By
Suzanne Tosini, Acting Chief Risk Officer
March 23, 2021

Agenda

- Enterprise Risk Management (ERM) Program Cycle
- Calendar Year (CY) 2021 Enterprise Risk Profile
- CY 2021 Enterprise Risk Treatment Plans
- Looking Ahead

Annual ERM Cycle



Risk Assessment

Identify & Assess Risks to Strategic Goals

Risk Profile

Review & Conclude on Enterprise Risks

Risk Treatment Plan

Prioritize & Respond to Enterprise Risks

Monitoring & Reporting

Monitor & Communicate Enterprise Risks and Status

- OERM
- Executive Owners
- Office SMEs

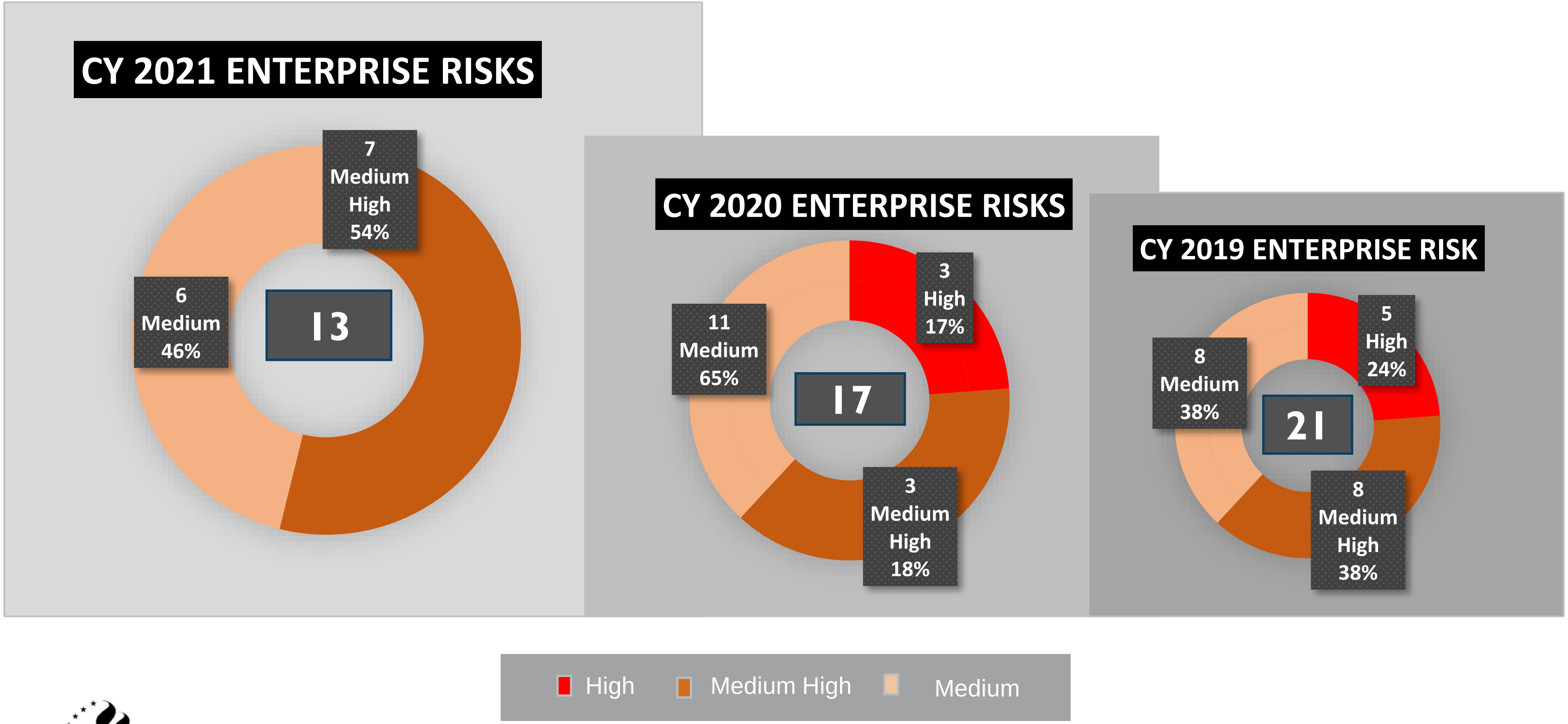
- OERM
- Executive Owners
- Enterprise Risk & Internal Control Steering Committed (ERISC)
- Executive Leadership Council (ELC)
- Board

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

- OERM
- ERISC
- ELC
- Board

✓ Repeatable
✓ Collaborative
✓ Accountable
✓ Transparent

Enterprise Risk Profile



Enterprise Risks – Key Changes

Risk	Statement	Executive Owner	Prior Results (CY 2020)	Current Results (CY 2021)	Accomplishments (CY 2020)
Insider Threat Management	There is a risk that the ack of an operational Insider Threat Program that protects agency defined critical assets may result in harm to Agency critical assets, FRTIB operations, and/or FRTIB personnel as a result of malicious and/or unintentional acts conducted by an FRTIB insider.	ORM	**High**	**Medium High**	• Established an Intra-agency Agreement with a federal service provider as part of the larger managed services umbrella. • Established, recruited, and onboarded the Insider Threat Analyst. • Coordinated efforts between the FRTIB and the federal service provider, such as the Critical Asset Vulnerability Analysis to identify critical assets that will be tracked during the program execution. • Started the process to develop the PTA and PIA needed for privacy compliance and discussed the requirements for the System of Records Notice (SORN). • Discussed and worked on the workflows and data flows needed to implement the Insider Threat Program at FRTIB.
Information Security	There is a risk that the Agency may fail to adequately protect and secure information resulting in unauthorized access, denial of services or compromise of sensitive information.	OTS	**High**	**Medium High**	• Updated and implemented Agency IT related policies based on the recent NIST standards and guidelines. • Launched & matured the FISMA Process Health Metrics Dashboard. • Completed almost all the 30 system authorizations. • Decommissioned legacy systems, such as mobile device. • Launched the O365 with more advanced security capabilities. • Began implementation of SOC-as-a-Service with a federal service provider. • Evaluated the new security technologies in the managed services.

Enterprise Risks – Key Changes

Risk	Statement	Executive Owner	Prior Results (CY 2020)	Current Results (CY 2021)	Accomplishments (CY 2020)
Disaster Recovery/ Business Continuity	There is a risk that the Agency may not be able to restore critical business processes within maximum tolerable downtimes resulting in significant disruption to FRTIB critical processes.	OTS	**Medium High**	**Medium**	• Updated the RTP actions to respond to the COVID-19 pandemic. • Developed Back to 77K Plan in accordance with White House and District of Columbia Reopening guidance and guidelines. • Conducted Government Emergency Telecommunications card test. • Performed a 100% business continuity telework exercise. • Migrated the ServiceNow to the Government Community Cloud. • Migrated all mailboxes to Exchange Online and Intune for mobile device management. • Deployed MS O365 Teams to support virtual working environment. • Doubled the VPN capacity at both data centers that increased the max concurrent users from 5000 to 10000. • Enabled telework capabilities for 798 on-site workforce contractors, located at the SBUs & SPUs. • Staffed End User Support and Asset Management to support FRTIB Phase-2 of the Back to 77K Plan. • Performed application testing and validation.
Human Capital Management	Inability to effectively recruit and retain a highly-skilled workforce, failure to execute succession planning and knowledge transfer, results in a failure to achieve FRTIB business objectives.	ORM	**Medium**	**Medium High**	Newly tracked risk in CY2021 due to increased risk score.

Enterprise Risks – Key Changes

Risk	Statement	Executive Owner	Prior Results (CY 2020)	Current Results (CY 2021)	Accomplishments (CY 2020)
Data Privacy	There is a risk that 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**	**Medium High**	• Coordinated with ORM to ensure the100% of current FRTIB employees and new hires completed Annual Privacy Training. • Launched the Agency Annual Privacy Refresher Training. • Updated PTA/PIA procedures and conducted Role-Based Training for DLC re: role of Business Owners completing PIAs. • Conducted Role-Based Training for Assessors and ISSOs. • Completed and sent PIA Annual Review Form to Business Owners. • Completed 15 PTAs and 4 PIA. • Completed 9 assessments of the NIST SP 800-53 Rev 4 privacy controls as a part of Assessment & Authorization (A&A) process. • Published one System of Records Notice (SORN) in the Federal Register; two SORNs under review with OMB.
TSP Fraud	There is a risk that 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**	**Medium High**	• Deployed faster transaction notification when money transactions are requested via SMS and/or email communication. • Deployed an updated algorithm for the forms review process to include 100% review for financial institutions known to be used in fraudulent withdrawal attempts. • Implemented notification capability to send SMS text and email to both old and new phone numbers and email addresses when participants update their contact information.
Acquisition Planning	There is a risk that 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**	**Medium High**	• Established a partnership with OCFO and identified key dependencies to address the risks. • Identified the elements to form and communicate the draft strategy, including additional resources, approach, plan etc.

Enterprise Risks – Other

New CY 2021 Enterprise Risk

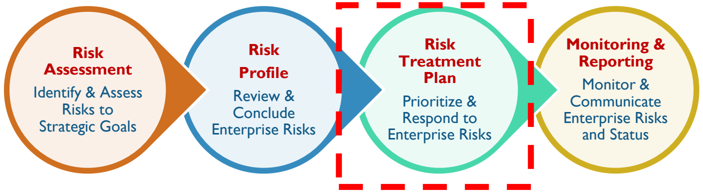
Risk	Statement	Executive Owner	Prior Results (CY 2020)	Current Results (CY 2021)
RKSA - Converge	There is a risk that steady state operations are not maintained throughout RKSA transition caused by focusing too much on RKSA transition while neglecting steady state continuity, resulting in TSP processing delays or errors.	OPS	**NA**	**Medium High**

Remaining CY 2021 Enterprise Risks

Risk	Executive Owner	Prior Results (CY 2020)	Current Results (CY 2021)
Procurement	OCFO	Medium	Medium
Records Retention	ORM	Medium	Medium
Contract Management	OCFO	Medium	Medium
Compliance	OGC	Medium	Medium
Economic Change Events	OI	Medium	Medium

Thrift Savings Plan

CY 2021 Risk Response

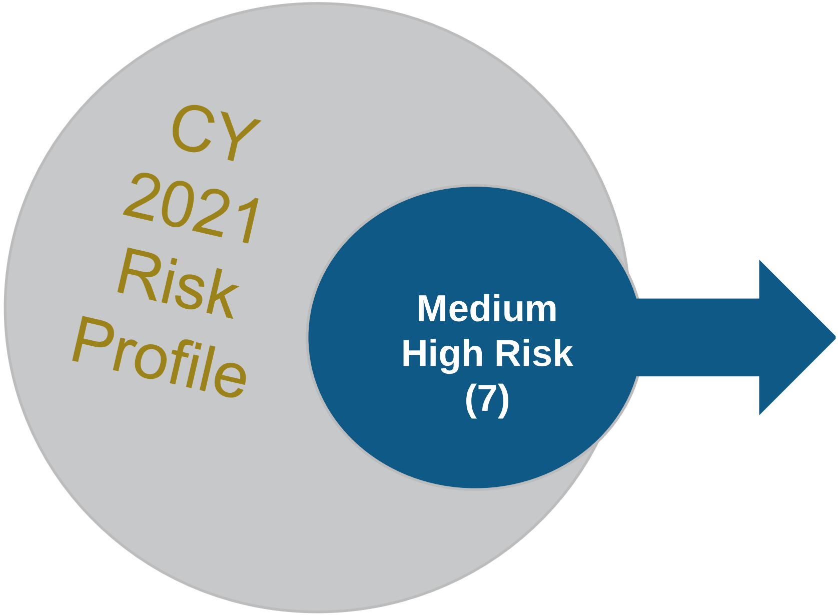


Risk Assessment
Identify & Assess Risks to Strategic Goals

Risk Profile
Review & Conclude Enterprise Risks

Risk Treatment Plan
Prioritize & Respond to Enterprise Risks

Monitoring & Reporting
Monitor & Communicate Enterprise Risks and Status



CY 2021 Risk Profile

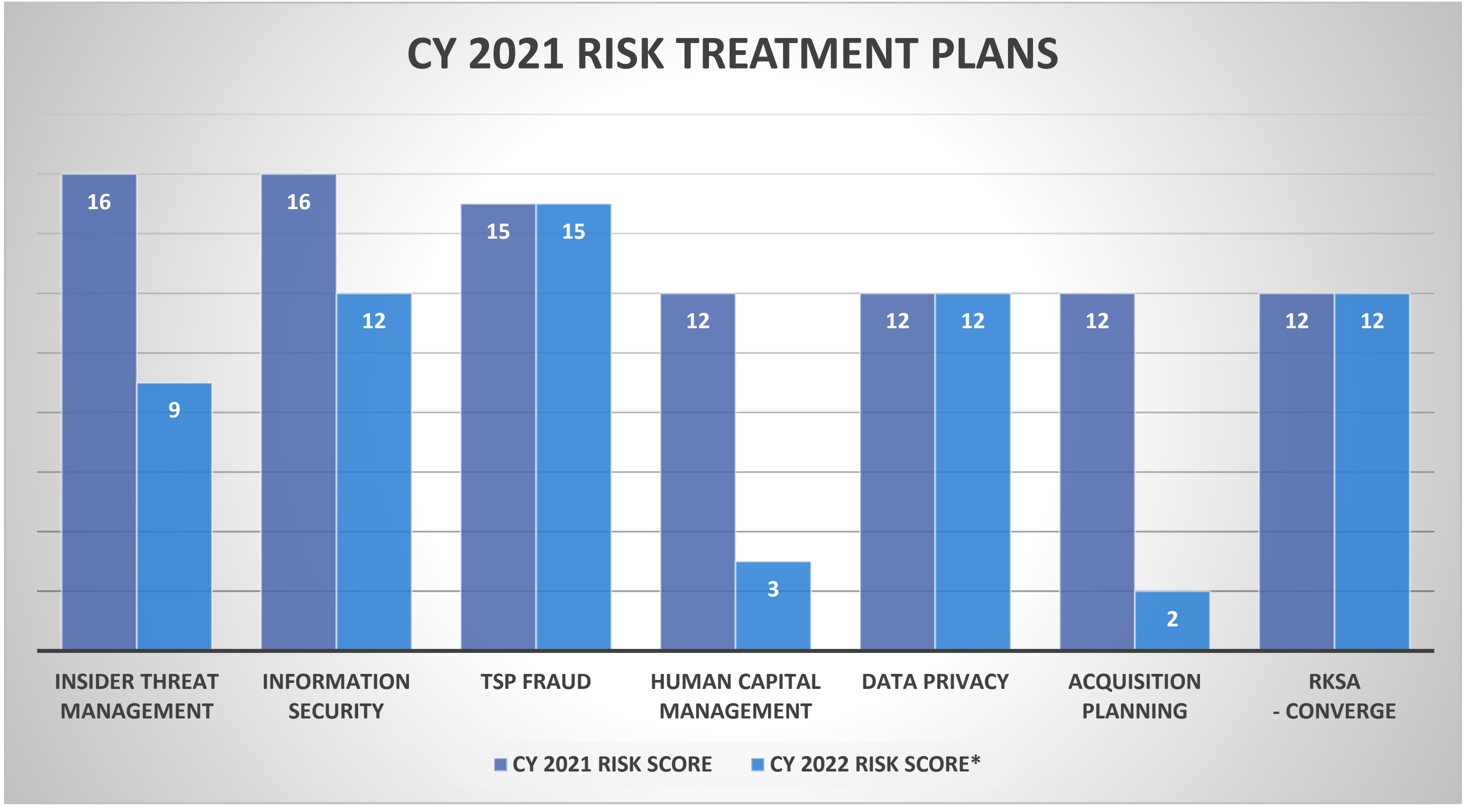
Medium High Risk (7)

Risk Treatment Plan	Executive Owner
Insider Threat Management	ORM
Information Security	OTS
Data Privacy	OGC
TSP Fraud	OPS
Acquisition Planning	OEP
Human Capital Management	ORM
RKSA - Converge	OPS

Considered

Draft FY 22-26 Strategic Goals & Objectives

Effect 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 2022 risk score, reflects the successful implementation of the Risk Treatment Plan.

Thrift Savings Plan

Questions?