Enterprise Risk Management (ERM) Update

Presented By
Thomas Brandt, Office of Planning and Risk
March 24, 2022

Agenda

FRTIB's Annual ERM Program Cycle

- OPR
- Executive Owners
- Office SMEs

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

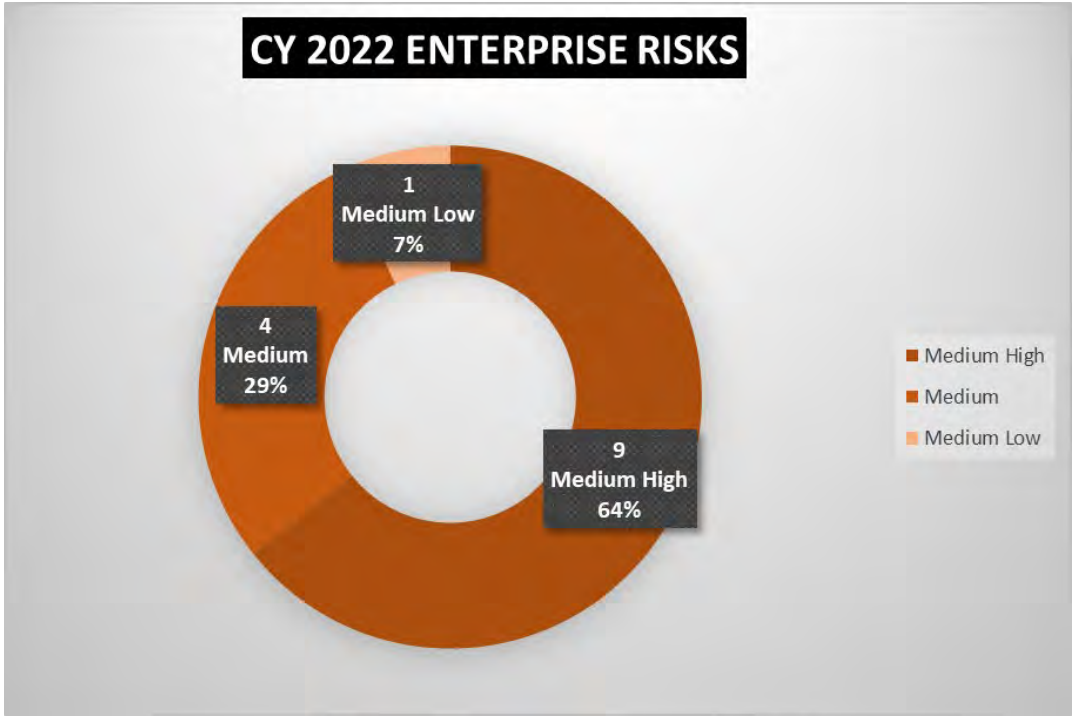
- OPR
- Risk Owners/SMEs
- ERISC
- ELC
- Board

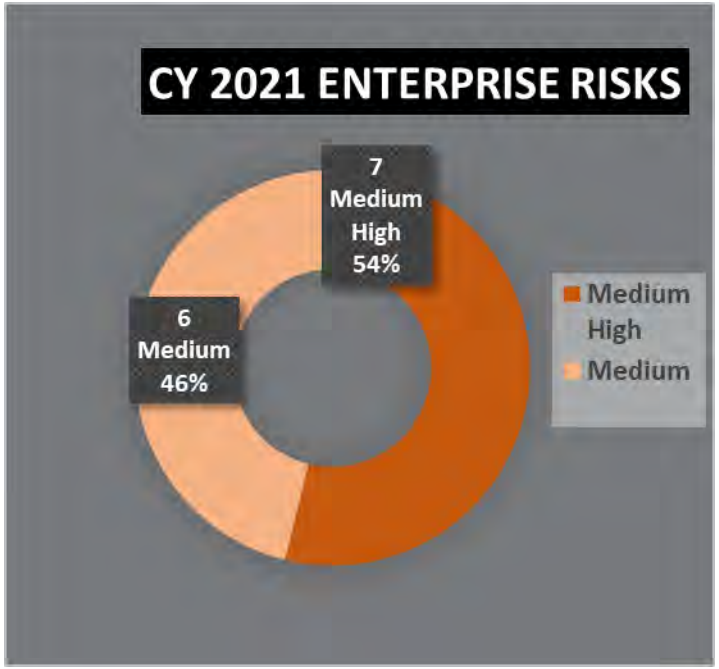
- OPR
- ERISC
- ELC
- Board

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

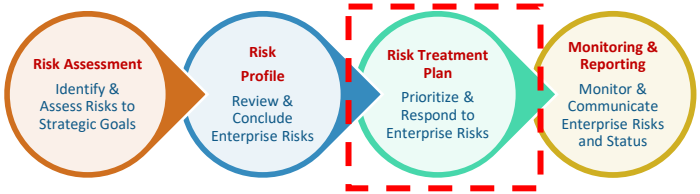
✓ Repeatable
✓ Collaborative
✓ Accountable
✓ Transparent

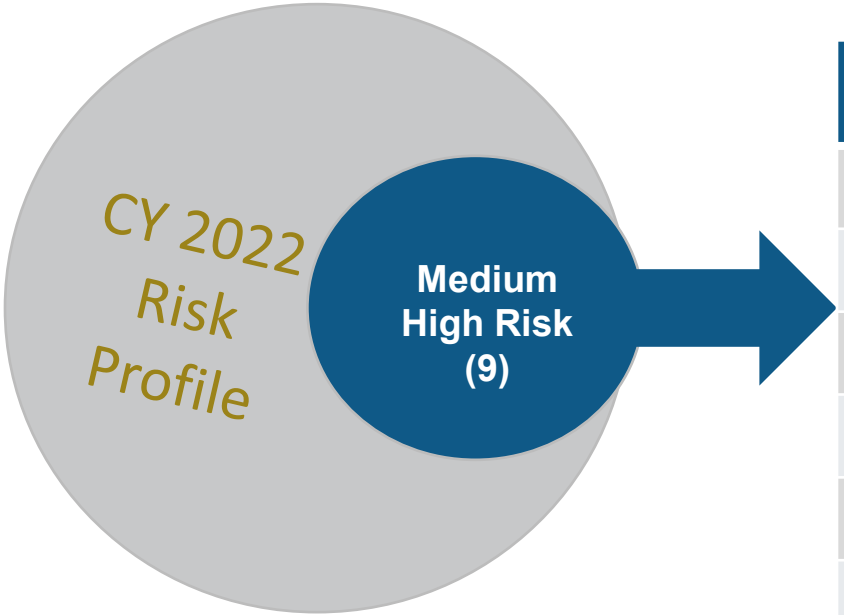
Enterprise Risk Profile (CY 2022 - 2021)





CY 2022 Risk Response





Risk Treatment Plan	Executive Owner
Insider Threat Management	ORM
Information Security	OTS
Data Privacy	OGC
TSP Fraud	OPS
Procurement / Contract Management	OED
Human Capital Management	ORM
Converge	OPS
*Supply Chain Risk Management	OPR

* New CY 2022 FRTIB Enterprise Risk

CY 2021 Q4 Risk Treatment Plan Updates

Risk Treatment Plan – Insider Threat Management

Statement	Executive Owner	Current Risk Score (12/31/20)	Risk Treatment Plan Status* (12/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (October 2021- December 2021)
Lack 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	Medium High	On Target	Medium	• Insider Threat Program Procedures Published, ORM.571 – Completed Sept 30, 2021 • Insider Threat Program Privacy Impact Assessment (Final Draft) Submitted to OGC – Completed Sept 30, 2021 • User Activity Monitoring (UAM) detection tools deployed to FRTIB's Network – Completed Sept 13, 2021

*** Categorization of Risk Treatment Plans:**
- **On Target**
- **Some Delay = 1-4 months**
- **Delayed = 4+ months**

**** Future Risk Score: reflects the successful implementation of the Risk Treatment Plan.**

Risk Treatment Plan – Information Security

Statement	Executive Owner	Current Risk Score (12/31/20)	Risk Treatment Plan Status* (12/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (October 2021- December 2021)
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	Medium High	On Target	Medium High	• Department of Justice SOC-as-a-Service implementation is complete. • Process Health Metrics Dashboard continues to develop based on auditor feedback, working sessions are ongoing. • TIC 3.0/ZeroTrust pilot project completed with good results. • 23 of 25 system authorizations are complete. • 10 Continuous Monitoring Authorizations completed, w/another 9 in progress • Completed FY21 FISMA audit, results are consistent with last year's performance. • Continue to implement FISMA and other auditor recommendations.

*** Categorization of Risk Treatment Plans:**
- **On Target**
- **Some Delay = 1-4 months**
- **Delayed = 4+ months**

**** Future Risk Score: reflects the successful implementation of the Risk Treatment Plan.**

Risk Treatment Plan – Human Capital Management

Statement	Executive Owner	Current Risk Score (12/31/20)	Risk Treatment Plan Status* (12/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (October 2021- December 2021)
There is a risk the Agency may not be able 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 High	On Target	Medium Low	• Workforce Planning • POMP Competency Inventory Refresh. (Completion Date: August 30) • Training and Development • POMP Supervisory Training Sessions (Details and Reassignments—Completion Date: July 13th; The Reorganization Process—Completion Date: September 14th) • POMP Training Plan (Completion Date: September 30) • Strategic Hiring and Recruitment • Held ELC Hiring Subcommittee meetings on a bi-monthly basis to review backfill requests from offices (Completion Date: Ongoing). • Retention Incentives • Conducted supervisory training on retention incentives and strategies (Completion Date: September 27th)

*** Categorization of Risk Treatment Plans:**

- **On Target**
- **Some Delay = 1-4 months**
- **Delayed = 4+ months**

**** Future Risk Score: reflects the successful implementation of the Risk Treatment Plan.**

Risk Treatment Plan – TSP Fraud

Statement	Executive Owner	Current Risk Score (12/31/20)	Risk Treatment Plan Status* (12/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (October 2021- December 2021)
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	On Target	Medium High	• Account Security Analysis conducted/concluded by Deloitte, no major findings. (Completed: January 31, 2021)

*** Categorization of Risk Treatment Plans:**
- **On Target**
- **Some Delay = 1-4 months**
- **Delayed = 4+ months**

**** Future Risk Score: reflects the successful implementation of the Risk Treatment Plan.**

Risk Treatment Plan – Data Privacy

Statement	Executive Owner	Current Risk Score (12/31/19)	Risk Treatment Plan Status* (12/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (October 2021- December 2021)
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	On Target	Medium High	• Coordinated with ORM and 100% of new hires received privacy training • Conducted Annual Privacy Refresher Training for All Employees • Reviewed 2 System of Records Notices (SORNs) and submitted 1 SORN to OMB • Completed PIA Annual Review for 14 systems • Completed 10 Privacy Threshold Analysis (PTA) • Completed 13 Privacy Impact Assessment (PIA) • Completed 7 assessments of the NIST SP 800-53 Rev 4 privacy controls as part of the Assessment & Authorization (A&A) process

*** Categorization of Risk Treatment Plans:**
- **On Target**
- **Some Delay = 1-4 months**
- **Delayed = 4+ months**

**** Future Risk Score: reflects the successful implementation of the Risk Treatment Plan.**

Risk Treatment Plan – Acquisition Planning

Statement	Executive Owner	Current Risk Score (12/31/19)	Risk Treatment Plan Status* (12/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (October 2021- December 2021)
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	On Target	Low	• Revised framework and draft presentation completed (Completion Date: September 3, 2021) • During the CY 2022 Risk Profile/dashboard updating, the risk owner decided to retire the risk as the agency has completed a bulk of the large acquisitions for the foreseeable future.

*** Categorization of Risk Treatment Plans:**
- **On Target**
- **Some Delay = 1-4 months**
- **Delayed = 4+ months**

**** Future Risk Score: reflects the successful implementation of the Risk Treatment Plan.**

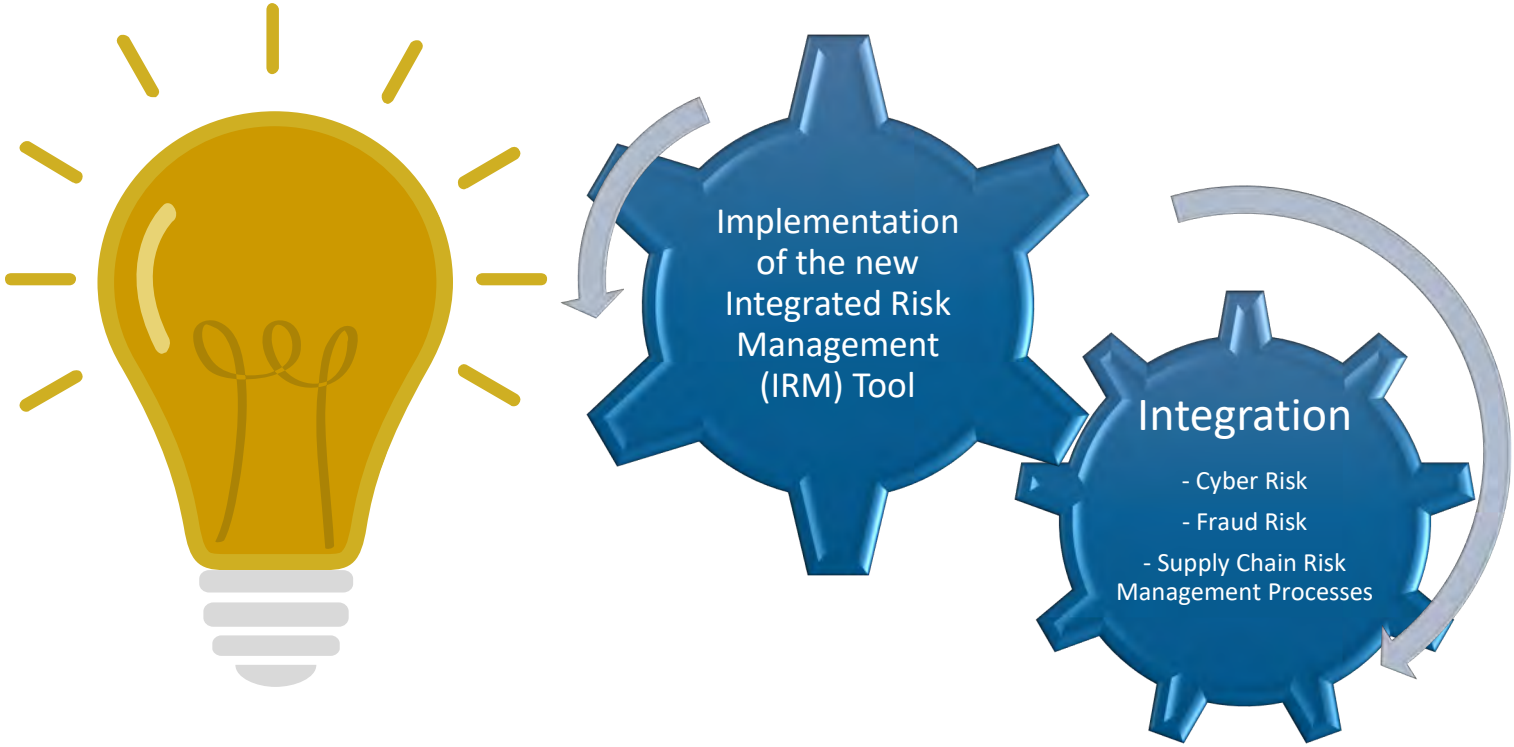
Risk Treatment Plan – Converge

Statement	Executive Owner	Current Risk Score (12/31/20)	Risk Treatment Plan Status* (12/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (October 2021- December 2021)
There is a risk that steady state operations are not maintained throughout Converge (formerly RKSA) transition caused by focusing too much on Converge transition while neglecting steady state continuity, resulting in TSP processing delays or errors.	OPS	Medium High	On Target	Medium High	• Successfully onboarded, trained, and deployed 10 contractors to augment the duties of federal staff dedicated to the Converge transition • Assure that steady state operations have run smoothly with no significant service interruptions • Maintained, exceeded, and/or improved all 54 operations service levels for CY21 • Supported and/or completed 4 KPMG audits, 2 CLA audits, and 1 internal audit

*** Categorization of Risk Treatment Plans:**
- **On Target**
- **Some Delay = 1-4 months**
- **Delayed = 4+ months**

**** Future Risk Score: reflects the successful implementation of the Risk Treatment Plan.**

Upcoming ERM Initiatives



Questions?