

# Enterprise Risk Management (ERM) Update

Presented By  
Kim Weaver, Office of Planning and Risk  
November 19, 2021

# Agenda

<b>Topic</b>	<b>Slide</b>
Enterprise Risk Management Program Cycle	<b>3</b>
Update of the Risk Appetite Statement	<b>4</b>
Calendar Year (CY) 2021 Enterprise Risk Profile	<b>5</b>
CY 2021 Enterprise Risk Treatment Plans	<b>8</b>
Upcoming Key ERM Initiatives	<b>15</b>

# FRTIB's Annual ERM Program Cycle



# Updated FRTIB Risk Appetite Statement - 2021

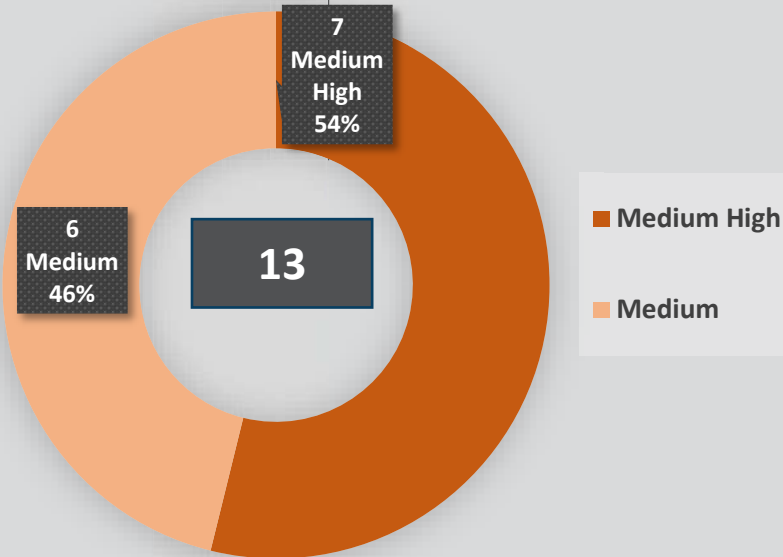
## ERM Risk Appetite by Risk Category

RISK CATEGORY	RISK APPETITE
Strategic	Moderate
Operational	Moderate*
Legal	Low
Information Technology	Low
Reputational	Low
External	Moderate
Overall	Low

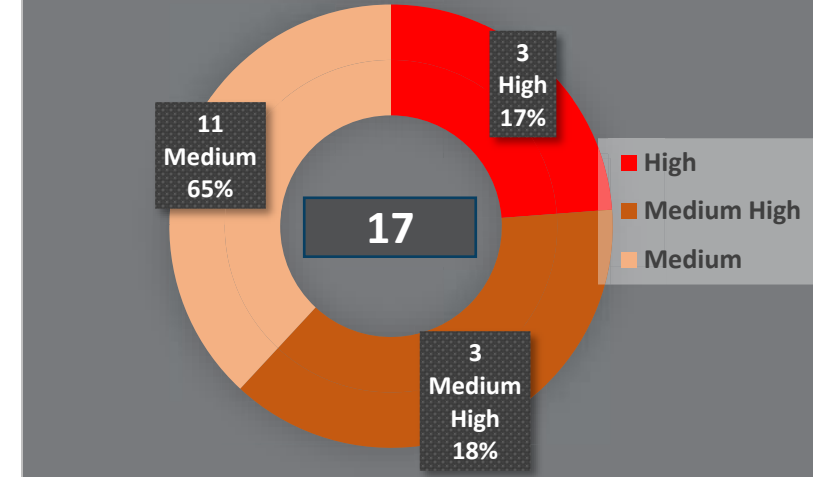
\* Risk Appetite increased from Low in the prior Risk Appetite Statement

# Enterprise Risk Profile (CY 2021 - 2020)

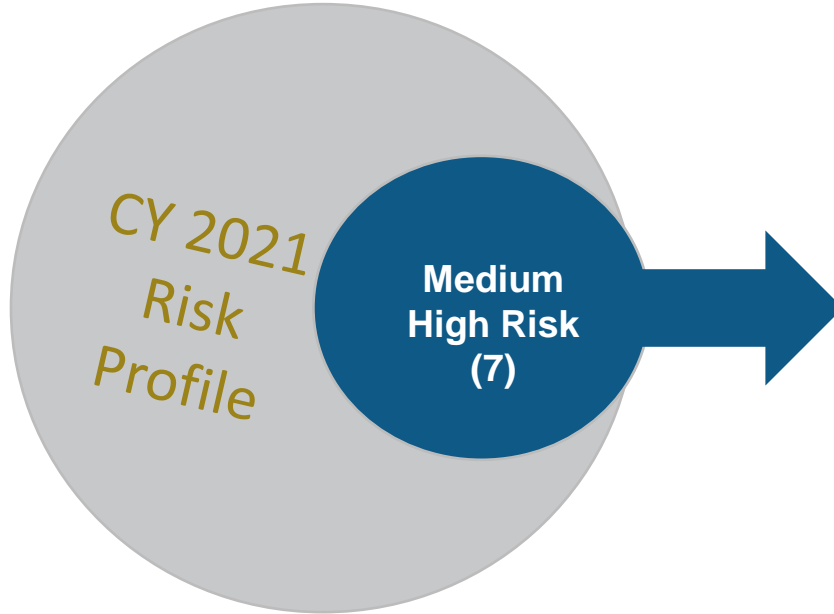
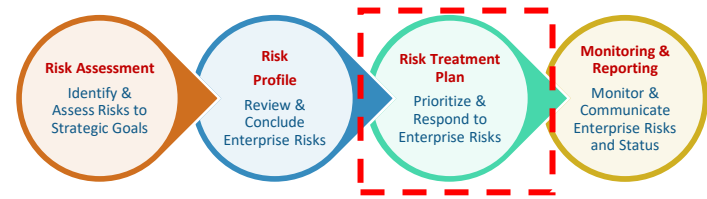
## CY 2021 ENTERPRISE RISKS



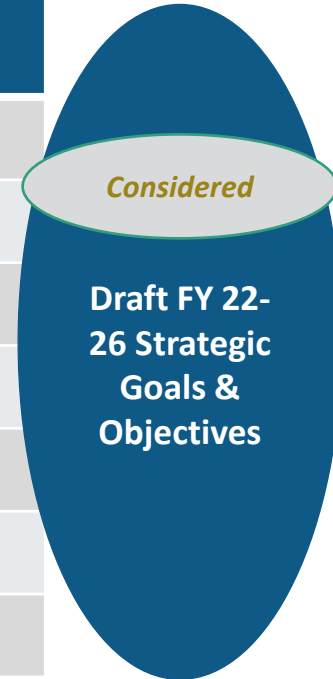
## CY 2020 ENTERPRISE RISKS



# CY 2021 Risk Response



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



# Risk Treatment Plan

## – Insider Threat Management



Statement	Executive Owner	Current Risk Score (12/31/20)	Risk Treatment Plan Status* (10/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (January 2021 – October 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	<ul style="list-style-type: none"> <li>Insider Threat Program Procedures Published, ORM.571 – Completed Sept 30, 2021</li> <li>Insider Threat Program Privacy Impact Assessment (Final Draft) Submitted to OGC – Completed Sept 30, 2021</li> <li>User Activity Monitoring (UAM) detection tools deployed to FRTIB's Network – Completed Sept 13, 2021</li> <li>DOJ's SORN Published to the National Archives Federal Register – completed July 30, 2021</li> <li>FRTIB Insider Threat Program SORN (FRTIB-23) published to the National Archives Federal Register – completed July 28, 2021</li> <li>Insider Threat Program Awareness/Overview briefing finalized – Completed July 8, 2021</li> <li>Updated Insider Threat Policy Published, ORM.570 – Completed May 31, 2021</li> </ul>

\* 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* (10/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (January 2021 – October 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	<ul style="list-style-type: none"> <li>Complied with 1 DHS/CISA Emergency Directive, and submission was on time.</li> <li>Department of Justice SOC-as-a-Service implementation is complete.</li> <li>Process Health Metrics Dashboard continues to develop based on auditor feedback, working sessions are ongoing.</li> <li>TIC 3.0/ZeroTrust pilot project completed with good results.</li> <li>23 of 25 system authorizations are complete.</li> <li>10 Continuous Monitoring Authorizations completed, w/another 9 in progress</li> <li>Completed FY21 FISMA audit, results are consistent with last year's performance.</li> <li>Continue to implement FISMA and other auditor recommendations.</li> </ul>

\* 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* (10/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (January 2021 – October 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	<ul style="list-style-type: none"> <li>Workforce Planning               <ul style="list-style-type: none"> <li>POMP Competency Inventory Refresh. (Completion Date: August 30)</li> </ul> </li> <li>Training and Development               <ul style="list-style-type: none"> <li>General Skills Training Classes (Conflict management--Completion Date: Date: June 30th)</li> <li>POMP HCTS Employee Brown Bag Sessions (Details and Reassignments—Completion Date: August 18th)</li> <li>POMP Supervisory Training Sessions (Details and Reassignments—Completion Date: July 13th; The Reorganization Process—Completion Date: September 14th)</li> <li>POMP Training Plan (Completion Date: September 30)</li> </ul> </li> <li>Strategic Hiring and Recruitment               <ul style="list-style-type: none"> <li>Held ELC Hiring Subcommittee meetings on a bi-monthly basis to review backfill requests from offices (Completion Date: Ongoing).</li> </ul> </li> <li>Retention Incentives               <ul style="list-style-type: none"> <li>Conducted supervisory training on retention incentives and strategies (Completion Date: September 27th)</li> </ul> </li> </ul>

\* 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* (10/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (January 2021 – October 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	<ul style="list-style-type: none"> <li>Account Security Analysis conducted/concluded by Deloitte, no major findings (Completion Date: January 31, 2021)</li> </ul>

\* 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* (10/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (January 2021 – October 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	<ul style="list-style-type: none"> <li>Coordinated with ORM and 100% of new hires received privacy training</li> <li>Reviewed 2 System of Records Notices (SORNs) and submitted 1 SORM to OMB</li> <li>Completed 10 Privacy Threshold Analysis (PTA)</li> <li>Completed 13 Privacy Impact Assessment (PIA)</li> <li>Completed PIA Annual Review for 14 systems</li> <li>Completed 7 assessments of the NIST SP 800-53 Rev 4 privacy controls as part of the Assessment &amp; Authorization (A&amp;A) process</li> </ul>

\* 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* (10/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (January 2021 – October 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	<ul style="list-style-type: none"> <li>The draft framework submitted to OPR (then-OEP) Director</li> <li>Revised framework completed September 3, 2021</li> <li>Multi-asset manager, FSM, and Converge have been awarded; MAM is implemented; FSM will go live January 2022; Converge will go live summer of 2022</li> <li>AITs draft RFQ has been issued</li> </ul>

\* 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* (10/31/21)	Future Risk Score** (12/31/21)	Key Accomplishments (January 2021 – October 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	<ul style="list-style-type: none"> <li>Successfully onboarded, trained, and deployed 10 contractors to augment the duties of federal staff dedicated to the Converge transition</li> <li>Assure that steady state operations have run smoothly with no significant service interruptions</li> <li>Maintained, exceeded, and/or improved all 54 operations service levels for CY21</li> <li>Supported and/or completed 4 KPMG audits, 2 CLA audits, and 1 internal audit</li> </ul>

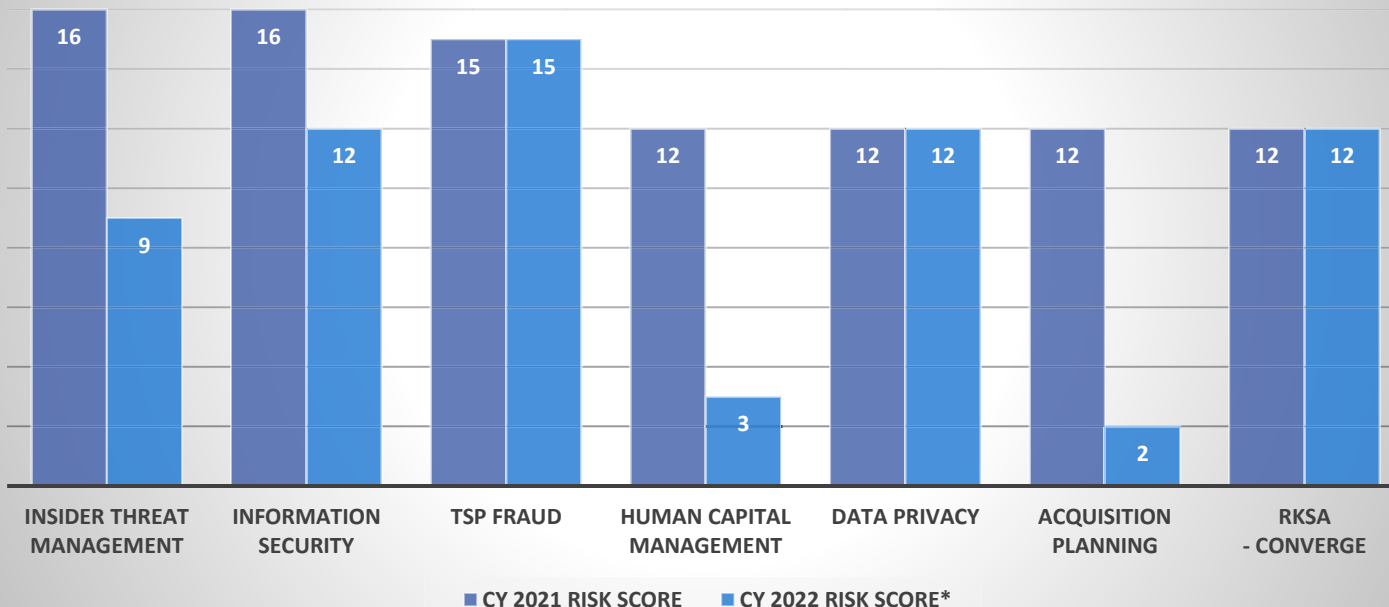
\* Categorization of Risk Treatment Plans:

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

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

# Impact of Risk Treatment Plans (RTPS)

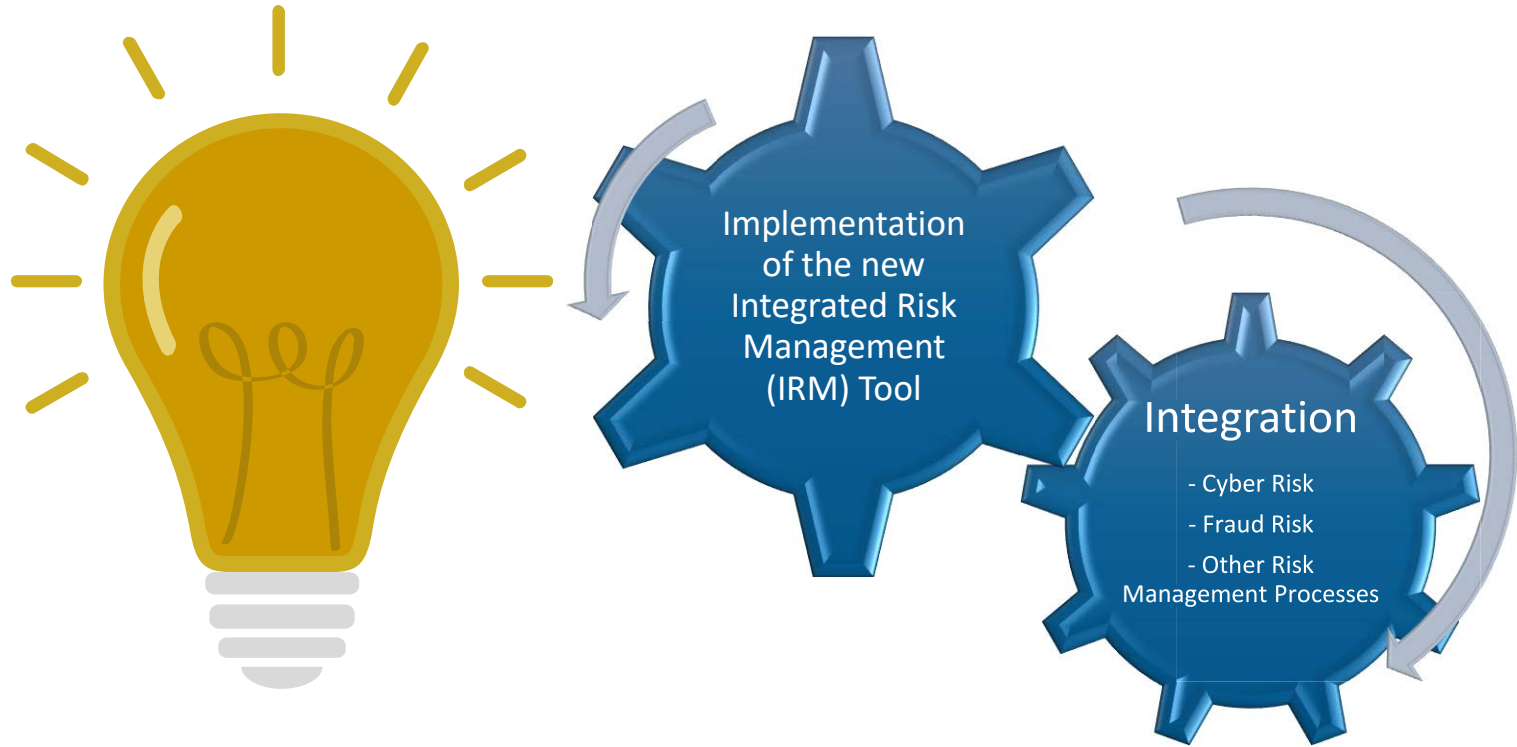
## CY 2021 RISK TREATMENT PLANS



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, which reflects the successful implementation of the Risk Treatment Plan.

# Upcoming ERM Initiatives



# Questions?