Enterprise Risk Management (ERM) Update

Presented By
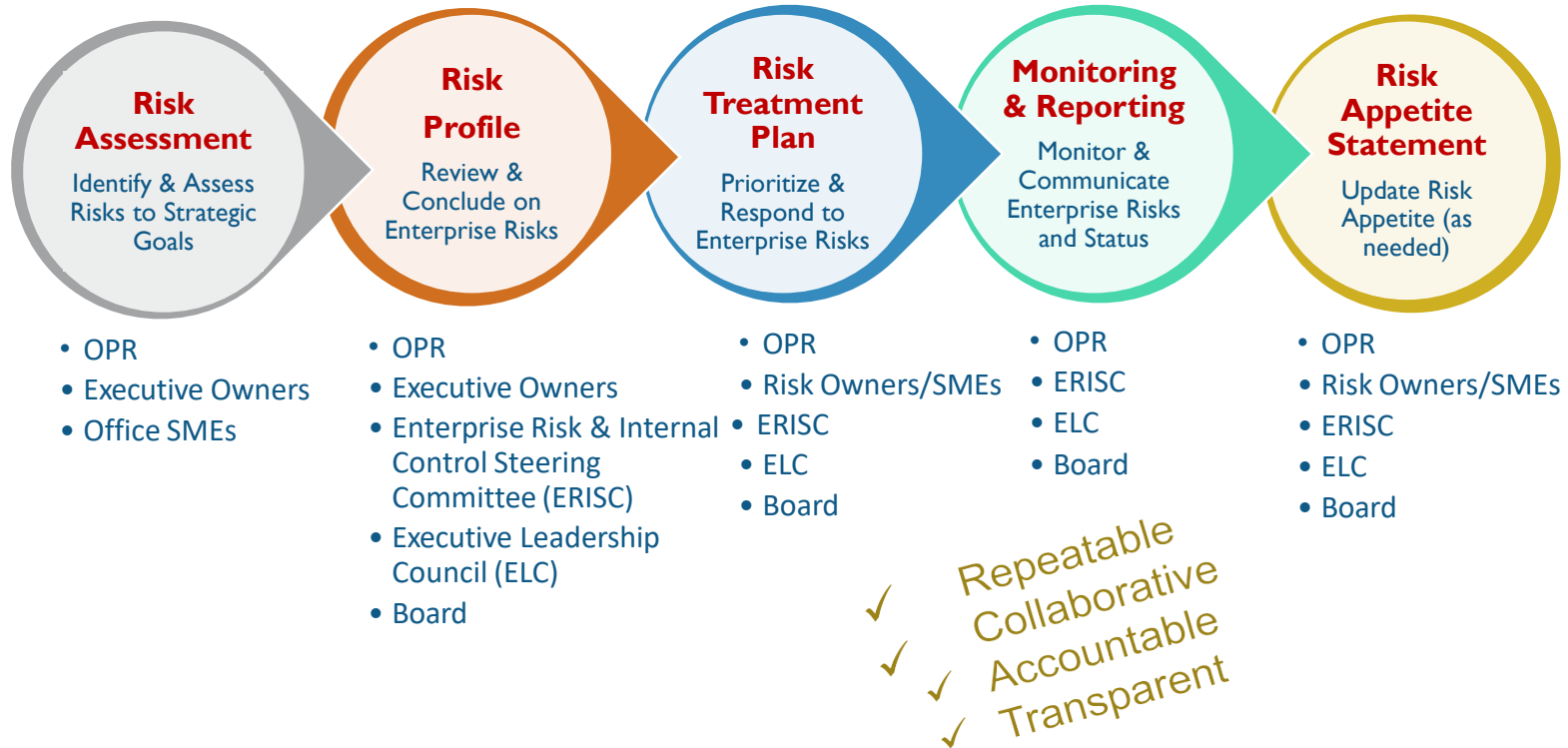Thomas Brandt, Office of Planning and Risk
October 25, 2022
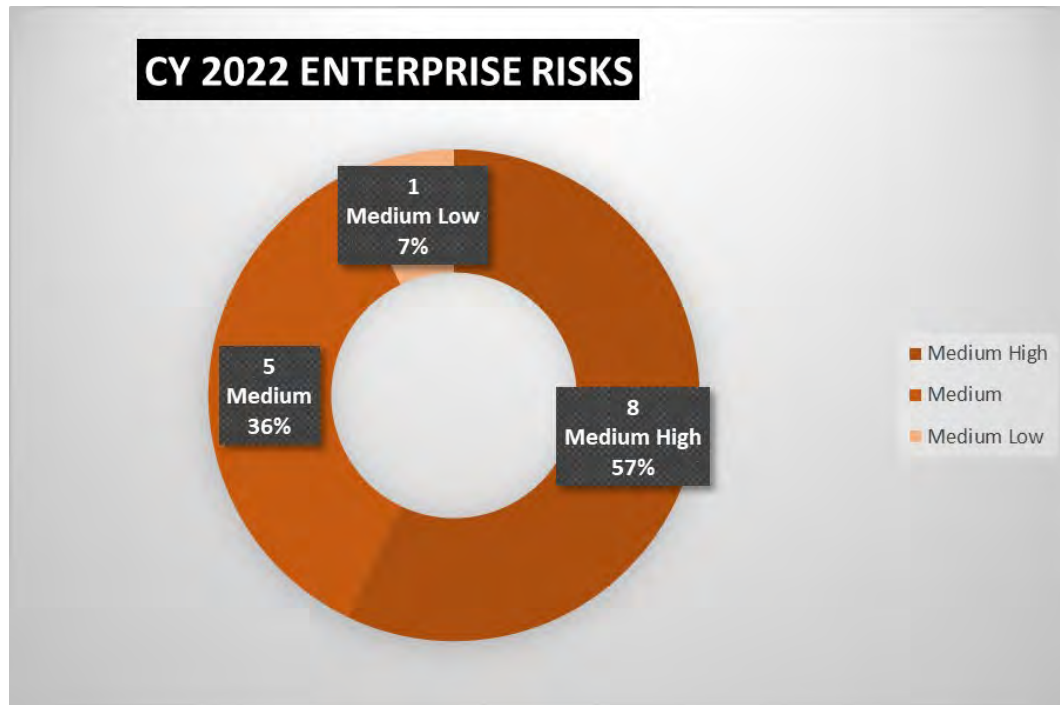
Thrift Savings Plan
Federal Retirement Thrift Investment Board
tsp.gov

tsp4gov @

Agenda

Topic	Slide
Enterprise Risk Management Program Cycle	**3**
Calendar Year (CY) 2022 Enterprise Risk Profile	**4**
CY 2022 Risk Response	**5**
CY 2022 Q3 Enterprise Risk Treatment Plans	**6**
Ongoing Key ERM Initiatives	**15**

Thrift Savings Plan

FRTIB's Annual ERM Program 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

Risk Appetite Statement
Update Risk Appetite (as needed)

- 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

Thrift Savings Plan

CY2022 Enterprise Risk Profile

CY 2022 ENTERPRISE RISKS

1
Medium Low
7%

5
Medium
36%

8
Medium High
57%

- Medium High
- Medium
- Medium Low

Thrift Savings Plan

CY 2022 Risk Response
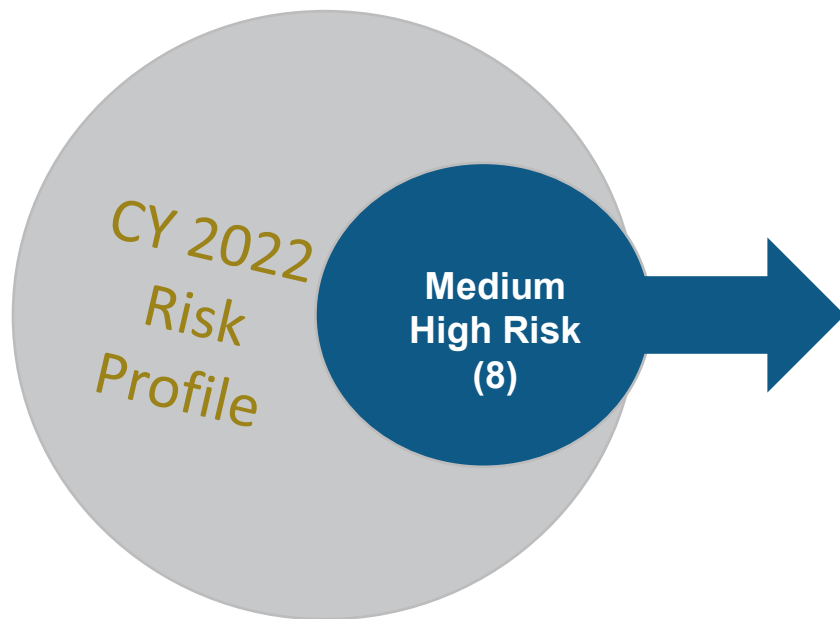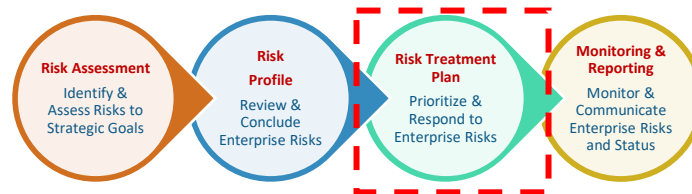
Risk Treatment Plan	Executive Owner
Procurement Contract Management	OED
Supply Chain Risk Management (SCRM)*	OPR
Converge Steady State Converge Go Live	OPS
Insider Threat Management	ORM
Human Capital Management	ORM
Information Security	OTS

CY 2022 Risk Profile

Medium High Risk (8)

Thrift Savings Plan

* New CY 2022 FRTIB Enterprise Risks

CY 2022 Q3 Risk Treatment Plan updates

Risk Treatment Plan – Procurement

Statement	Executive Owner	Current Risk Score (12/31/21)	Risk Treatment Plan Status* (09/30/22)	Future Risk Score** (12/31/22)	Key Accomplishments (April 2022- October 2022)
There is a risk that the agency may be directive in contractor performance for current and future Performance Based Contracts, most importantly Converge and AITS.	OED	Medium High	On Target	Medium	**Understanding the Contract** • Developing memo for all parties to sign stating they understand the contract by the end of FY 2023 Q1 **Designation of Performance-Based contract** • Training is scheduled for FY 2023 Q2 **Correct IGCE, market research, pricing, and adherence to contract terms** • AMD provided training to CORs on the IGCE and cost/price tool and process (09/07/2022) • AMD provided subsequent reminders on tools availability to Acquisition Community via AMD Contracting Update (September 2022) and AMD Acquisition Advisor newsletter (October 2022) • Cost Support Tool and Team is fully operational and has been accepting work to assist the Agency **Creation and adherence to realistic milestones and schedules** • Training scheduled for February 2023 on proper contract surveillance techniques on tracking milestones and report deficiencies to the CO if needed **Shift the risk to vendor(s)/ contractor(s)** • Still under development

* 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.

Thrift Savings Plan

Risk Treatment Plan – Contract Management

Risk Assessment
Identify & Assess Risks to Strategic Goals

Risk Profile
Review & Finalize Enterprise Risks

Risk Treatment Plan
Prioritize & Respond to Enterprise Risks

Monitoring & Reporting
Monitor & Communicate Enterprise Risks and Status

Statement	Executive Owner	Current Risk Score (12/31/21)	Risk Treatment Plan Status* (09/30/22)	Future Risk Score** (12/31/22)	Key Accomplishments (April 2022- October 2022)

There is a risk that our quality assurance and surveillance personnel are not sufficient in experience, expertise, and quantity to adopt to the Agency's change in acquisition strategy for operations. This may result in insufficient oversight and quality assurance efforts for new or emerging contracts.	OED	Medium High	On Target	Low	Training CORs on roles and provide a POC for questions
					 • Developed twelve-month training schedule to outline various aspects of contract management for CORs)
					   • Posted training on SP for the COR community and sent invites to all CORs.
					   • October training is role of the CORs and their duties and responsibilities.
					 • Reviewed and validate COR contract assignment to make sure contracts that warrant COR assignment have coverage.
					 • Training was conducted with demonstration of the proper documentation and format to use in order to have CORs assigned to their respective contracts. This process is still ongoing and on target
					 Provide feedback to Office Directors on completing training
					 • In developmental stage will provide by the end of the first quarter fiscal year 2023
					 • Note per external guidance all CORs with existing certifications received a new two-year window to complete training beginning May 2022
					 Provide mentorship opportunities for CORs
					 • Working on providing mentorship opportunities for CORs dependent on availability of participants
					 • A full liaison team has been stood up to assist / mentor CORs through the requirements 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 – Supply Chain Risk Management

Statement	Executive Owner	Current Risk Score (12/31/21)	Risk Treatment Plan Status* (09/30/22)	Future Risk Score** (12/31/22)	Key Accomplishments (April 2022- October 2022)
There is a risk that compromises to FRTIB suppliers, their supply chains, and their products and services for IT and communication products and services will severely limit the delivery of the core recordkeeping, investment management, and other people, processes, and systems required to deliver TSP services.	OPR	Medium High	On Target	Medium High	• The Office of Planning and Risk (OPR) led the Supply Chain Risk Management (SCRM) Interagency Agreement (IAA) activities and service with the Department of Energy (DOE) – February – July 2022. • Through the DOE IAA, OPR completed a pilot test of the DOE's process and tools for monitoring various supply chain risk vectors that included Cyber Security, Foreign Interest, Geopolitical, and Compliance. Lessons learned from the pilot with DOE are being considered as part of the assessment and enhancement of FRTIB's SCRM program. • In May, OPR engaged consulting services to conduct a Current State Assessment (CSA) of the agency's SCRM and Vendor Risk Management capabilities. The CSA resulted in several process improvement recommendations that are being prioritized and incorporated into an implementation plan. • The FY 2022 FISMA audit reported that the SCRM domain scored a Level 4 (managed and measurable) out a possible 5. • One of the immediate To Dos from the CSA is to refresh the SCRM policy/procedures to reflect the current/newly proposed agency SCRM practices.

* 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 (Steady State)

Risk Assessment — Identify & Assess Risks to Strategic Goals → Risk Profile — Review & Finalize Enterprise Risks → Risk Treatment Plan — Prioritize & Respond to Enterprise Risks → Monitoring & Reporting — Monitor & Communicate Enterprise Risks and Status

Statement	Executive Owner	Current Risk Score (12/31/21)	Risk Treatment Plan Status* (09/30/22)	Future Risk Score** (12/31/22)	Key Accomplishments (April 2022- October 2022)
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	• Assured that steady state operations have run smoothly with no significant service interruptions • *OPR/OPS agreed to retire this risk from the profile/dashboard since Converge Go Live has been delivered.*

* 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.

Thrift Savings Plan

Risk Treatment Plan – Converge Go Live

Statement	Executive Owner	Current Risk Score (12/31/21)	Risk Treatment Plan Status* (09/30/22)	Future Risk Score** (12/31/22)	Key Accomplishments (April 2022- October 2022)
If Converge Go Live does not occur as planned, May 2022, then FRTIB will continue to operate in the existing operating model and continue to deliver the TSP services in its current manner and its reputation as a top-tier recordkeeper could suffer.	OPS	Medium High	On Target	Medium High	• The FRTIB Converge project team utilized the Converge Risk Management Group and its risk management capabilities at the micro level. • *OPR/OPS agreed to retire this risk from the profile/dashboard since Converge Go Live was delivered.*

* 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.

Thrift Savings Plan

Risk Treatment Plan – Insider Threat Management

Risk Assessment — Identify & Assess Risks to Strategic Goals → Risk Profile — Review & Finalize Enterprise Risks → Risk Treatment Plan — Prioritize & Respond to Enterprise Risks → Monitoring & Reporting — Monitor & Communicate Enterprise Risks and Status

Statement	Executive Owner	Current Risk Score (12/31/21)	Risk Treatment Plan Status* (09/30/22)	Future Risk Score** (12/31/22)	Key Accomplishments (April 2022- October 2022)
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	Some Delay	Medium	• Provided Insider Threat Awareness training to 117 New Hire contact center employees (Spring 2022) • Provided Insider Threat Awareness training to 9 New Hire contact center employees (Spring 2022) • Provided Insider Threat Program capability briefings to OED, OGC, OTS, OEA, and the ERIC Division (Spring 2022) • Supported a Fraud Investigation (March 2022) • Supporting a research project for OPS • The Insider Threat Program has also produced/prepared numerous User Activity Monitoring reports

* 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.

Thrift Savings Plan

Risk Treatment Plan – Human Capital Management

Statement	Executive Owner	Current Risk Score (12/31/21)	Risk Treatment Plan Status* (09/30/22)	Future Risk Score** (12/31/22)	Key Accomplishments (April 2022- October 2022)
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	Some Delay	Medium Low	**Workforce Planning** • Procured an integrated workforce planning and learning management system (OASIS) that was launched in September. OASIS will be used to conduct the bi-annual agency-wide workforce competency assessment beginning in late 2022. **Training and Development** • Delivered a POMP Employee Briefing Session on The Reorganization Process (Completion Date: February 16, 2022) • Promoted and kicked off the 2022 Mentor Program (Completion Date: January-March) • Planned and Delivered POMP aligned general competency training courses, e.g., organizational skills, decision-making, critical thinking. (January-March) **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 stay and exit interviews (Completion Date: Ongoing) • Worked with management to make enhancements to work-life policies such as telework, hours of work, and fitness subsidy (Completion Date: February-August 2022) • Provided information to management and processed retention incentives for nominated employees (Completion Date: Ongoing)

* 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.

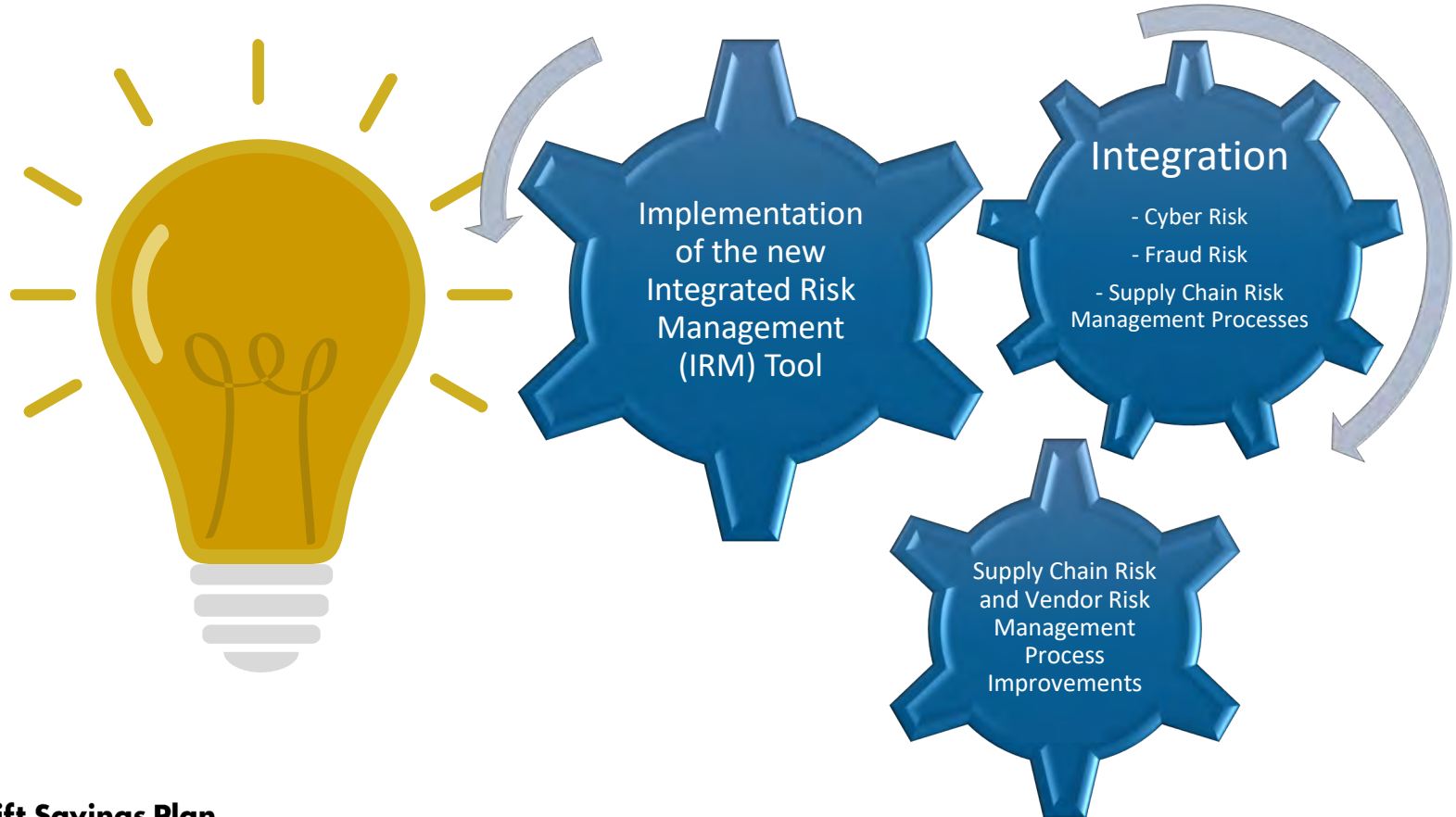# Risk Treatment Plan – Information Security

Statement	Executive Owner	Current Risk Score (12/31/21)	Risk Treatment Plan Status* (09/30/22)	Future Risk Score** (12/31/22)	Key Accomplishments (April 2022- October 2022)
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	• Decommissioned legacy TSP systems according to Federal guidance and best practices to ensure the safety of agency data • Completed an Authorization to Operate (ATO) for the Converge solution • Continue to implement requirements of the 2021 Cybersecurity Executive Order • Implement Cybersecurity Framework maturity monitoring for the Converge program • Implement CISA's Continuous Diagnostics and Mitigation CDM)

* 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.

Thrift Savings Plan

Ongoing ERM Initiatives

Implementation of the new Integrated Risk Management (IRM) Tool

Integration

- Cyber Risk
- Fraud Risk
- Supply Chain Risk Management Processes

Supply Chain Risk and Vendor Risk Management Process Improvements

Thrift Savings Plan

Questions?

Thrift Savings Plan