Enterprise Risk Management (ERM) Update

Presented by:
Brittany Borg, Office of Planning and Risk (OPR)

April 28, 2026

Thrift Savings Plan
Federal Retirement Thrift Investment Board
tsp.gov

Agenda

Annual ERM Program Cycle

OPR uses a cyclical, five-step process to manage enterprise level risks across their full lifecycles. This process provides a comprehensive, enterprise-wide view of organizational challenges to improve insight on how to address the highest priority risks to mission delivery.

STATUS Completed | In Progress | Not yet started

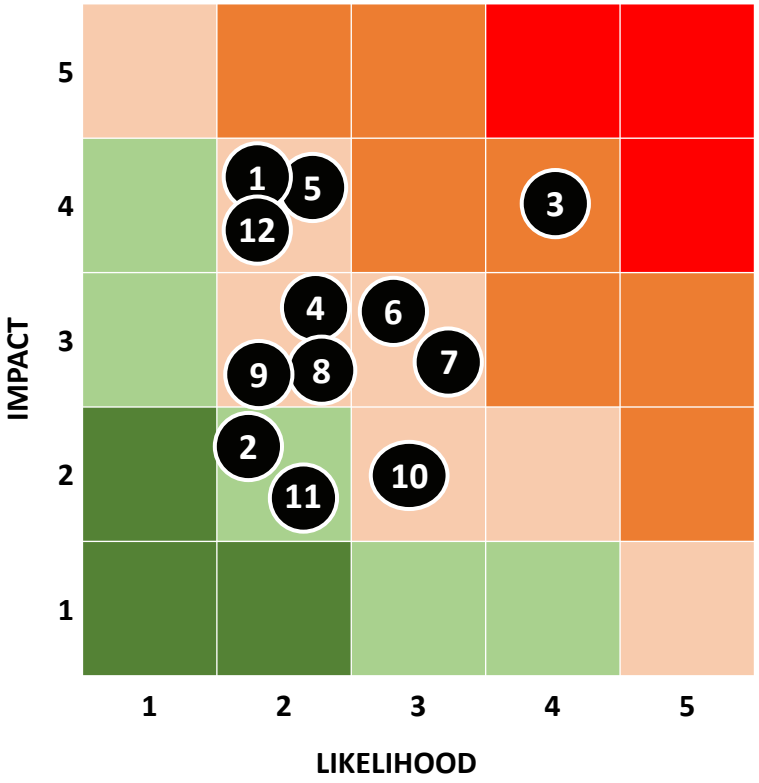
ERM CYCLE

Overview of the ERM Program cycle conducted throughout the year

1. **RISK IDENTIFICATION**
   Identify adverse conditions or events that could prevent the Agency from delivering its mission and achieving its strategic goals and objectives
2. **RISK ASSESSMENT & PRIORITIZATION**
   Apply standardized qualitative/quantitative criteria to evaluate the likelihood, impact, and velocity of identified risks to arrive at an Enterprise Risk Profile
3. **RISK TREATMENT**
   Develop Risk Treatment Plans with specific strategies and actions to manage identified risks to an acceptable level in line with expectations and risk appetite
4. **RISK MONITORING**
   Continuously monitor the progress and performance of Risk Treatment Plans to determine whether chosen strategies and actions are managing risks as intended
5. **RISK REPORTING**
   Regularly report risk information, including risk treatment progress and performance and other risk trends and insights, to inform decision-making

CY2026 Enterprise Risk Profile Dashboard

Below is a dashboard view of OPR's Enterprise Risk Profile, which contains a prioritized inventory of the most significant risks identified through the annual enterprise risk assessment process to provide a thoughtful analysis of the risks FRTIB faces toward achieving its strategic goals and objectives.



#	ENTERPRISE RISK	RISK RATING	RISK CATEGORY	RISK OWNER
1	Artificial Intelligence (AI)	Medium	Info Technology	OPR
2	Records Management	Medium Low	Operational	ORM
3	Cybersecurity	Medium High	Cyber	OTS
4	Economic Change Events	Medium	Strategic	OPE
5	Vendor Risk	Medium	Operational	OPR
6	Compliance	Medium	Legal	OGC
7	Data Privacy	Medium	Operational	OGC
8	Performance Based Contracts	Medium	Operational	OCFO
9	Contracting Officers' Representative	Medium	Operational	OCFO
10	TSP Fraud	Medium	Reputational	OPE
11	Reputational Risk of TSP Ops	Medium Low	Reputational	OPE
12	Fiduciary Risk	Medium	Legal	OGC

Thrift Savings Plan

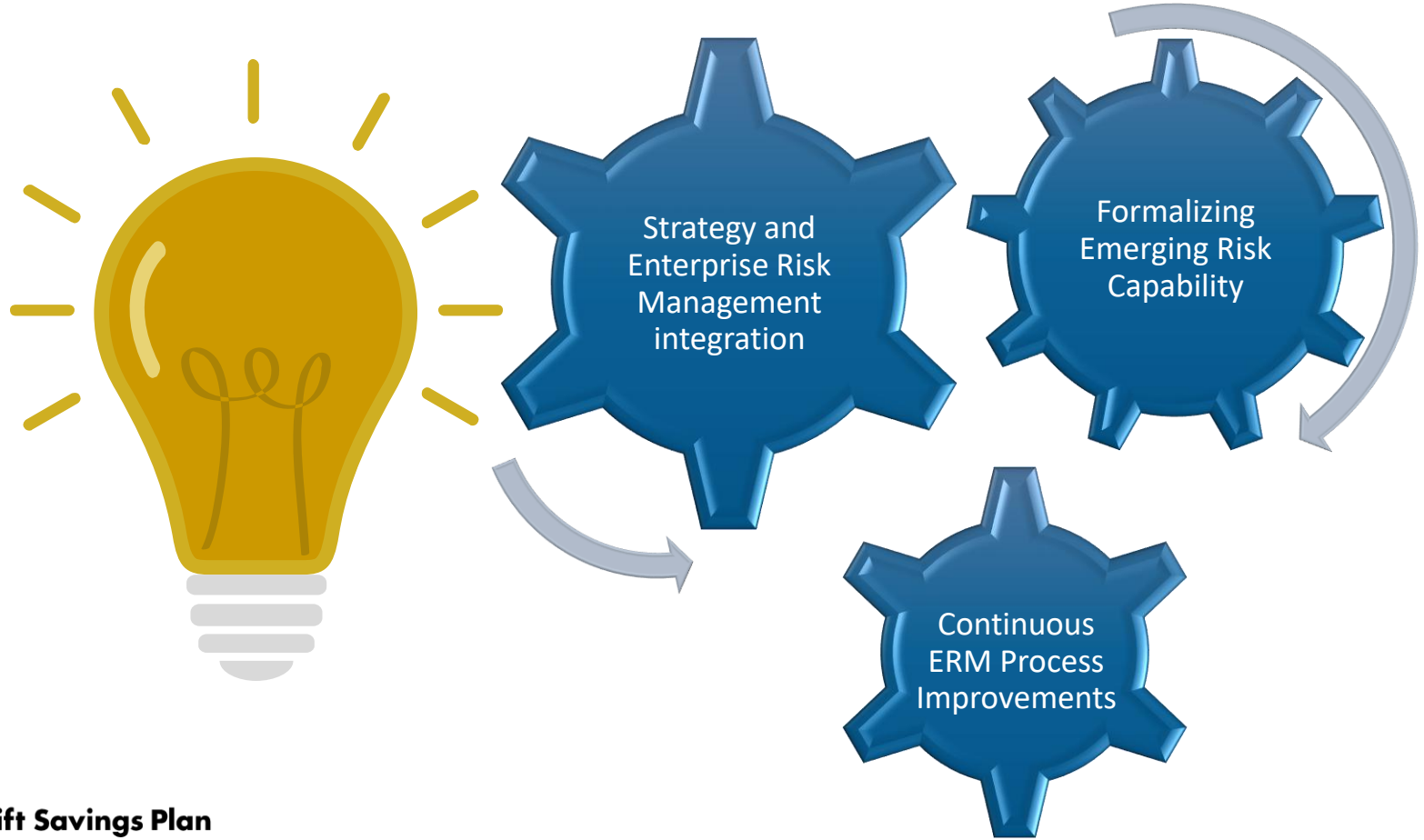
***Note:** Risk treatment plan reporting is only required for risks rated "Medium-High" or above.*

CY2026 Risk Treatment Plan Updates | Cybersecurity Risk

Below are updates from Risk Owners on the progress and performance of Risk Treatment Plans.

RISK STATEMENT	EXECUTIVE OWNER	CURRENT RISK SCORE	STATUS	FUTURE RISK SCORE	PLANNED ACCOMPLISHMENTS (CY2026)
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	• Implement phishing resistant Multi-Factor Authentication for required contractors and provide TSP participants the option of using phishing resistant authentication. • Strengthen oversight of service provider cybersecurity through clearer metrics and timely reporting. • Establish clear processes to identify and address unapproved technology use. • Continue review of historical risk acceptances. • Continue oversight of policies and procedures, utilization of Continuous Diagnostics and Mitigation, and vulnerability scanning tools.

Ongoing ERM Initiatives



Questions