

# Enterprise Risk Management (ERM) Update

Presented by:  
Thomas Brandt, Office of Planning and Risk (OPR)

December 18, 2025

# 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.



## ERM CYCLE

*Overview of the ERM Program cycle conducted throughout the year*

### RISK IDENTIFICATION

Identify adverse conditions or events that could prevent the Agency from delivering its mission and achieving its strategic goals and objectives

### 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

### 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

### RISK MONITORING

Continuously monitor the progress and performance of Risk Treatment Plans to determine whether chosen strategies and actions are managing risks as intended

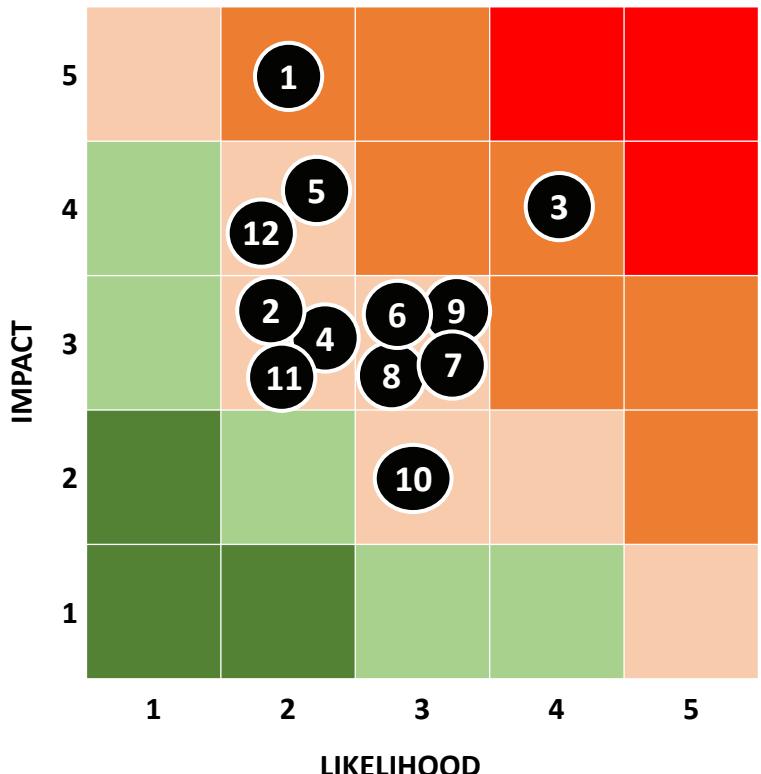
### RISK REPORTING

Regularly report risk information, including risk treatment progress and performance and other risk trends and insights, to inform decision-making



# CY2025 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 High	Info Technology	OPR
2	Records Management	Medium	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 Office Representatives	Medium	Operational	OCFO
10	TSP Fraud	Medium	Reputational	OPE
11	Reputational Risk of TSP Ops	Medium	Reputational	OPE
12	Fiduciary Risk	Medium	Reputational	OGC

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

# CY2025 Risk Treatment Plan Updates | Artificial Intelligence (AI) 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	KEY ACCOMPLISHMENTS (CY2025)
<ul style="list-style-type: none"><li>The adoption of enterprise Artificial Intelligence (AI) brings transformative potential for business efficiency and innovation; however, it also introduces privacy concerns, potential biases in decision-making processes, and additional information security risks. Furthermore, the rapid evolution of AI technologies can outpace an organization's ability to govern and control its use effectively, leading to potential regulatory compliance issues that must be carefully managed.</li></ul>	OPR	Medium High	On Target	Medium	<p>The FRTIB AI program has made significant strides in governance, workforce enablement, and innovation. It has:</p> <ul style="list-style-type: none"><li>Adopted the NIST AI Risk Management Framework.</li><li>Chartered the Information Security Governance Committee as the AI Governance Board.</li><li>Published a formal AI Policy and Strategy.</li><li>Created an AI Program Manager role to ensure strategic agency alignment.</li><li>Implemented workforce innovation initiatives including launching Microsoft CoPilot across the agency, piloting additional MS365 AI capabilities, and providing AI training sessions.</li><li>FRTIB is also complying with and reporting on the OMB-25-21 directive.</li></ul>



# CY2025 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	KEY ACCOMPLISHMENTS (CY2025)
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>Finalized a contract modification in October 2025 to implement phishing resistant Multi-Factor Authorization for all internal users of Converge.</li><li>Managing the cybersecurity posture of Managed Service Providers (MSPs) through additional SLR and KPI metrics and an increased frequency of reporting.</li><li>Completed a technical proposal, currently being reviewed by OTS senior leadership, regarding the adoption of Shadow IT procedures and processes for mitigation.</li><li>Review of historical risk acceptances was performed in February &amp; July 2025. Next review is planned for January 2026.</li></ul>