

Enterprise Risk Management (ERM) Update

Presented by

Thomas Brandt, Office of Planning and Risk
September 26, 2023

FRTIB's Annual ERM Program Cycle



CY 2023 Enterprise Risks

| Risk Category | Risk |
|------------------------|--|
| Strategic | Human Capital Management |
| Operational | Insider Threat Management |
| Operational | Records Management |
| Information Technology | Cybersecurity |
| Strategic | Economic Change Events |
| Operational | Supply Chain Risk Management |
| Legal | Compliance |
| Operational | Data Privacy |
| Operational | Procurement |
| Operational | Contract Management |
| Operational | TSP Fraud |
| Operational | Reputational Risk of TSP Operations to Customer Experience |

CY 2023 Enterprise Risk Profile



CY 2023 Risk Response



| Risk Treatment Plan | Executive Owner |
|--|-----------------|
| Cybersecurity | OTS |
| Procurement | OED |
| Contract Management | OED |
| Supply Chain Risk Management | OPR |
| Reputational Risk of TSP Operations to Customer Experience | OPE |

CY 2023 Risk Treatment Plan Updates

Risk Treatment Plan – Cyber Security



| Statement | Executive Owner | Current Risk Score (12/31/22) | Risk Treatment Plan Status* (08/31/23) | Future Risk Score** (12/31/23) | Key Accomplishments (May 2023 - September 2023) |
|---|-----------------|----------------------------------|---|-----------------------------------|--|
| 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"> Achieved Level 5 “Optimized” in 3 of 9 FISMA audit domains, and Level 4 “Managed and Measurable” in the remainder Finalized content and procedures for a new Cybersecurity Risk Register to better integrate cyber risk into the enterprise risk program Completed development of a completely new Cybersecurity Risk Treatment Plan leveraging the new Cybersecurity Risk Register Completed transition to a new continuous penetration testing model working with DOJ and Synack Continued to implement ongoing requirements of the 2021 Cybersecurity Executive Order |

* 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

– Procurement



| Statement | Executive Owner | Current Risk Score (12/31/22) | Risk Treatment Plan Status* (08/31/23) | Future Risk Score** (12/31/23) | Key Accomplishments (May 2023 - September 2023) |
|---|-----------------|----------------------------------|---|-----------------------------------|---|
| There is a risk that the agency may be over-directive in contractor performance for current and future Performance Based Contracts, most importantly Converge and AITS. These contracts were designed to minimize risk to the Agency and to allow the vendor to solution and achieve objectives with minimal constraints from the Agency. However, there is a natural tendency to maintain the status quo, which may prevent the vendors from owning the risk and performance, the results of which could be missed strategic objectives, cost growth, schedule implications and the Agency re-assuming risk unintentionally. | OED | Medium High | On Target | Medium | <ul style="list-style-type: none"> The Acquisition Liaison Team will continue to conduct trainings on the roles and responsibilities of the CORs in managing, tracking milestones and understanding performance-based contracts - training is scheduled for FY 2024 AMD provided internal training for CO/SC on Individual Government Cost Estimate (IGCE) and cost/price tool process; these tools are standardized and available on SharePoint as of FY 2023 Extended an OTS Cybersecurity contract to ensure continuity of services for a period of 60 days Continue to support the transition to FFP contracts with managed services which inherently minimizes procurement risk to FRTIB |
| <p>* Categorization of Risk Treatment Plans:</p> <ul style="list-style-type: none"> On Target Some Delay = 1-4 months Delayed = 4+ months <p>** Future Risk Score: reflects the successful implementation of the Risk Treatment Plan.</p> | | | | | |

Risk Treatment Plan

– Contract Management



| Statement | Executive Owner | Current Risk Score (12/31/22) | Risk Treatment Plan Status* (08/31/23) | Future Risk Score** (12/31/23) | Key Accomplishments (May 2023 - September 2023) |
|--|-----------------|-------------------------------|--|--------------------------------|---|
| There is a risk that our quality assurance and surveillance personnel (e.g. CORs) may not have sufficient experience and expertise to adopt or adapt to the Agency's change in acquisition strategy for operations. In addition, the Agency may not have enough of these personnel to provide the level of oversight and quality assurance efforts necessary for new and emerging contracts, which could result in diminished quality of services provided to the participant and beneficiaries and/or linked KPIs. Other implications could be cost, schedule, and scope creep beyond the Agency's original intent due to unauthorized commitments. | OED | Medium High | On Target | Medium | <ul style="list-style-type: none"> Conduct live 1 hour training on MS-Teams to all FRTIB CORs monthly The Acquisition Liaison Team reviews purchase request and addresses other procurement planning issues to identify any items requiring correction which prevents delays in processing Provide monthly Federal Acquisition Institute (FAI) report on the status of certified CORs to every Office Director 95% of FRTIB CORs are certified and have met the required continuing education requirements mandated by the Office of Federal Procurement Policy (OFPP) Continue to provide mentorship opportunities for CORs depending on the availability of participants; this is still ongoing and will likely be implemented at a future date Developed a 12-month training schedule which details various aspects of contract management; last quarter we demonstrated how and where to store contract management files. We had a 90% participation rate Implemented an automated COR nomination tool which streamlined the 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 (12/31/22) | Risk Treatment Plan Status* (08/31/23) | Future Risk Score** (12/31/23) | Key Accomplishments (May 2023 - September 2023) |
|--|-----------------|----------------------------------|---|-----------------------------------|--|
| 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 | <ul style="list-style-type: none"> Created a new Third Party Risk Analyst position description, which was announced on USA Jobs (09/08/2023) Created proposed Vendor Risk Management (VRM)/SCRM Risk Taxonomy (08/2023) Developing requirements for a SCRM dashboard (August/September 2023) Prepared targeted stakeholder training and communication plan (August 2023) The IRM/Service Project Manager has scheduled stakeholder ServiceNow stakeholder training for September/October 2023 |

*** 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

– Reputational Risk of TSP Operations



| Statement | Executive Owner | Current Risk Score (12/31/22) | Risk Treatment Plan Status* (08/31/23) | Future Risk Score** (12/31/23) | Key Accomplishments (May 2023 - September 2023) |
|--|-----------------|-------------------------------|--|--------------------------------|---|
| If FRTIB is not able to meet customer expectations due to challenges during steady-state Converge TSP operations, then there is a risk of negative impact to FRTIB's reputation with external partners and TSP participants and beneficiaries. | OPE | Medium High | On Target | Medium | <ul style="list-style-type: none">• Conducting proper contract oversight to ensure SLRs and KPIs are met, and financial penalties are assessed as needed.• Leveraging key accomplishments in procurement and contract management risk treatment plans to improve vendor oversight.• Analyzing web comments and participant feedback to improve participant experience (e.g. redesign of MyAccount; ability to change monthly installments online).• Participant satisfaction scores for interactions with the TSP steadily increased month over month to achieve target levels for the first time in the month of August.• Participating in a robust cycle of external and internal audits. |

* 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.

Ongoing ERM Initiatives

