# Enterprise Risk Management (ERM) Update

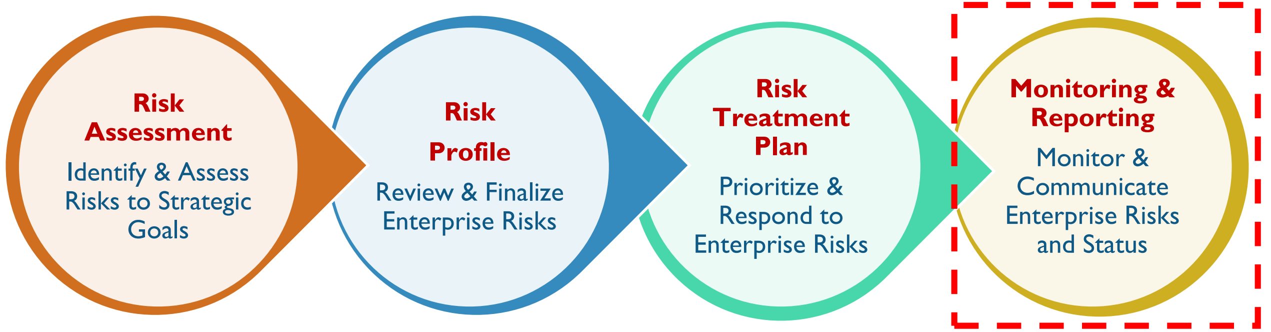
SUZANNE TOSINI, ACTING CHIEF RISK OFFICER

OFFICE OF ENTERPRISE RISK MANAGEMENT (OERM)

# AGENDA

- Enterprise Risk Management (ERM) Program Cycle
- Calendar Year (CY) 2020 Enterprise Risk Profile and Risk Treatment Plans
- Current ERM Key Initiatives
- CY 2021 ERM Program Cycle Kickoff and Status
- Upcoming Key ERM Initiatives

# FRTIB'S ANNUAL ERM PROGRAM CYCLE



**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

- Office Directors
- Office SMEs

- Executive Owners
- Enterprise Risk and Internal Control Steering Committed (ERISC)
- ELC

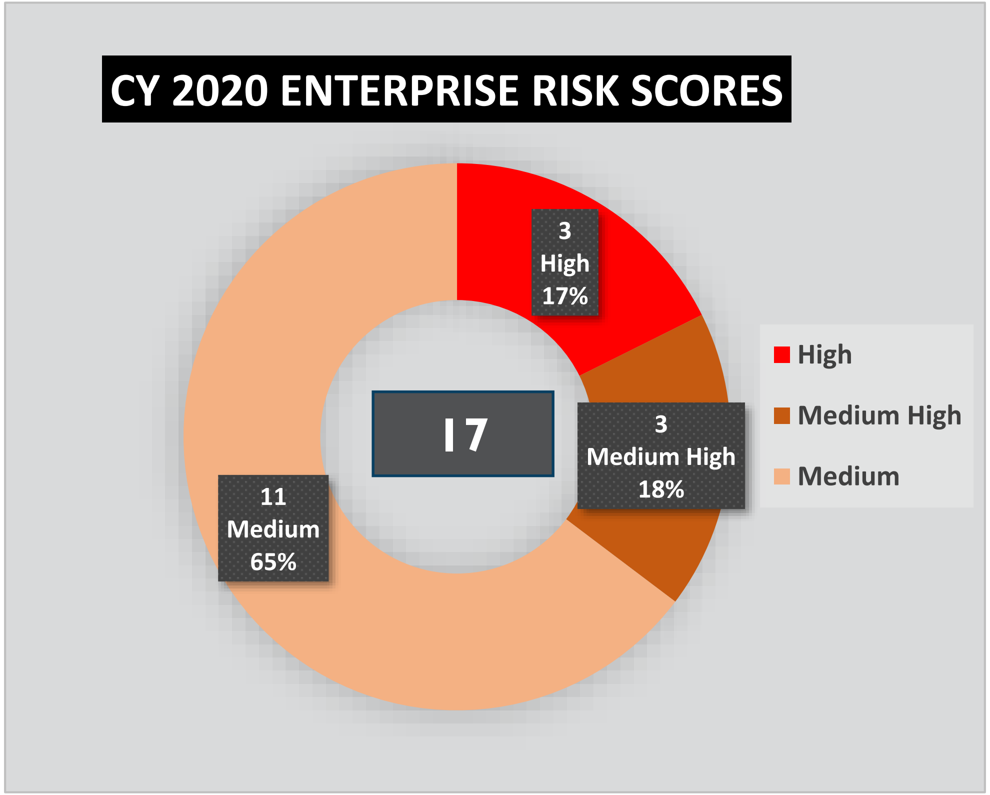
- Risk Owners/SMEs
- ERISC
- ELC

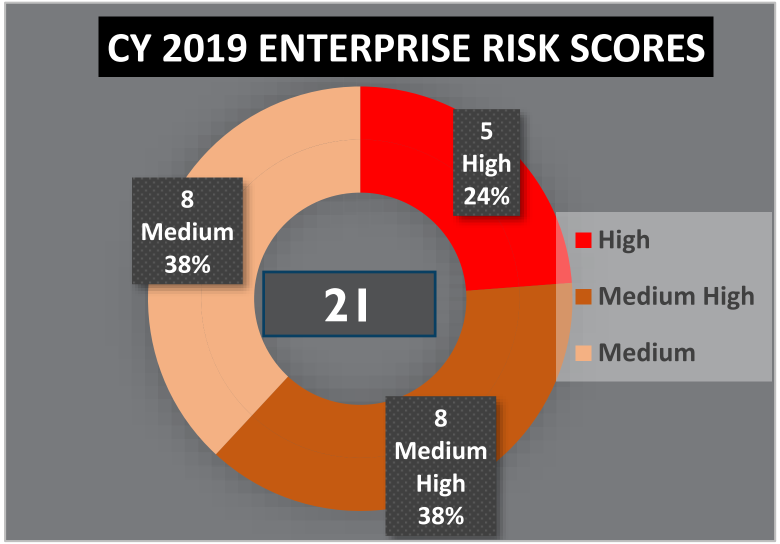
- ERISC
- ELC
- Board

✓ Repeatable
✓ Collaborative
✓ Accountable
✓ Transparent

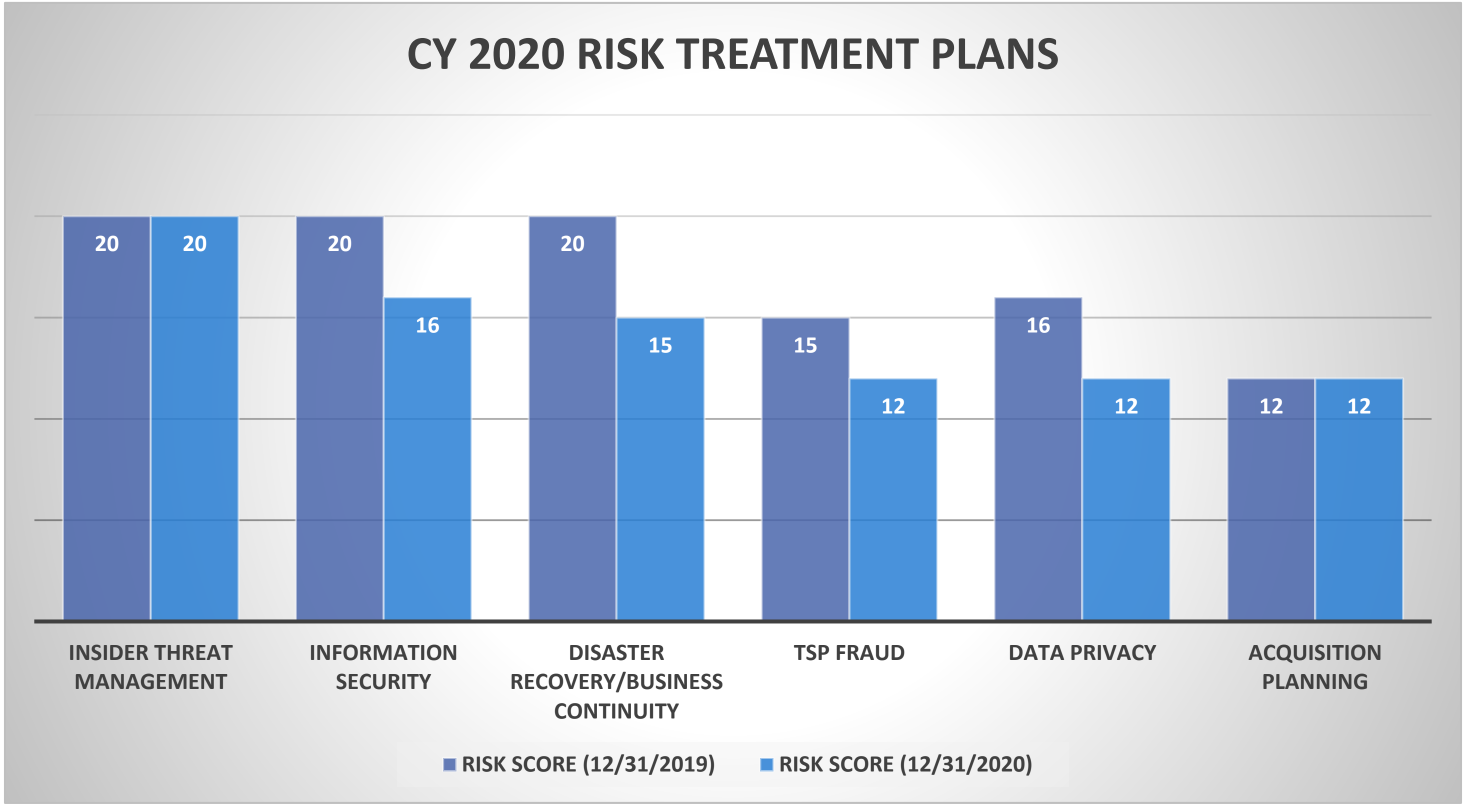
OERM Support and Coordination

# ENTERPRISE RISK PROFILE (CY2020 -2019)





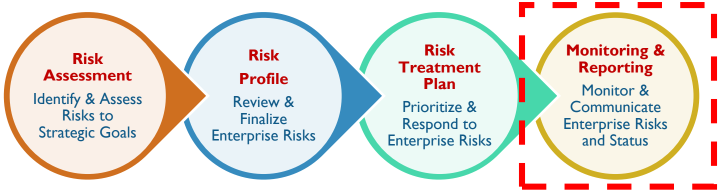
# CY 2020 RISK Treatment Plans



| Risk Rating | Score |
|---|---|
| High | 20-25 |
| Medium High | 10-19 |
| Medium | 5-9 |
| Medium Low | 3-4 |
| Low | 1-2 |

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

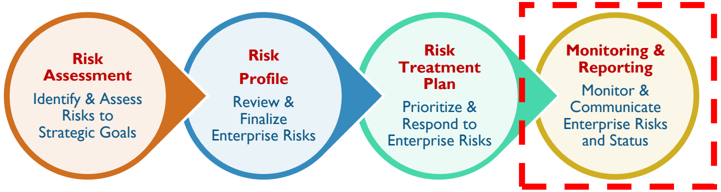
**Monitoring & Reporting**
Monitor & Communicate Enterprise Risks and Status

| Statement | Executive Owner | Current Risk Score (12/31/19) | Risk Treatment Plan Status* (09/30/20) | Future Risk Score** (12/31/20) | Key Accomplishments (March 2020 – September 2020) |
|---|---|---|---|---|---|
| There is a risk that an Insider may maliciously or unintentionally engage in activities that compromise data, critical assets, business processes or computer networks. | OERM | High | On Target | Medium High | • Completed the Critical Asset Vulnerability Analysis, in conjunction with the Department of Justice personnel which identified critical assets that will be tracked when program is in production status<br>• Started the process to develop the PTA and PIA needed for privacy compliance. Discussed the  System of Records Notice (SORN) that will need to be issued for the Insider Threat program prior to implementation.<br>• Held discussions with Department of Justice staff on the workflows and data flows needed to implement the Insider Threat and Hotline services at FRTIB. |

*** 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



**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 (12/31/19) | Risk Treatment Plan Status* (09/30/20) | Future Risk Score** (12/31/20) | Key Accomplishments (March 2020 – September 2020) |
|---|---|---|---|---|---|
| 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 | High | On Target | Medium High | • New NIST Risk Management Framework policies are implemented and have been vetted through multiple audits<br>• Process Health Metrics Dashboard is having a positive impact on FISMA maturity<br>• SOC-as-a-Service implementation with Department of Justice has begun, with 8 of 10 work streams started<br>• New security technologies important to the managed services transition are being evaluated through the TIC 3.0/ZeroTrust pilot project<br>• 18 of 30 system authorizations are complete |

*** 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
# - Disaster Recovery/Business Continuity

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

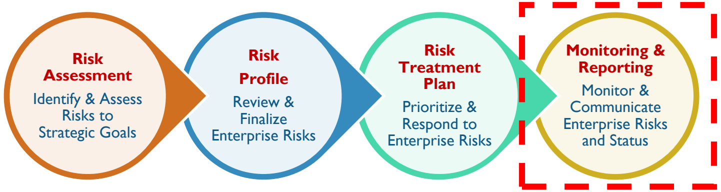
| Statement | Executive Owner | Current Risk Score (12/31/19) | Risk Treatment Plan Status* (09/30/20) | Future Risk Score** (12/31/20) | Key Accomplishments (March 2020 – September 2020) |
|---|---|---|---|---|---|
| There is a risk the Agency may not be able to restore critical business processes within maximum tolerable downtimes resulting in significant disruption to FRTIB critical processes. | OTS | High | On Target | Medium High | • Completed the ServiceNow migration to the Government Community Cloud<br>• Developed Back to 77K Plan in accordance with White House Reopening American Guidelines and District of Columbia Reopening Guidance<br>• Performed quarterly Government Emergency Telecommunications card test<br>• Deployed Microsoft O365 Teams collaboration tool on all Agency Laptops<br>• Staffed End User Support and Asset Management to support FRTIB Phase-2 of the Back to 77K Plan<br>• In coordination with Office of Enterprise Planning collected critical business processes for Agency leadership review and approval.<br>• Completed the data center transition event that involved transitioning both the production distributed applications and the new z14 mainframe to PDC achieving disaster recovery capabilities for the Agency at VDC.<br>• Performed a Disaster Recovery Exercise that tested the Agency's ability to execute a full failover to the alternate data center.<br>• Performed a Call Tree Exercise (Emergency Notification Test) that tested the ability for critical personnel to be notified in the event of a disaster or a disruption |

*** 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.**

Updated due to COVID-19

# Risk Treatment Plan
# - Data Privacy


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 (12/31/19) | Risk Treatment Plan Status* (09/30/20) | Future Risk Score** (12/31/20) | Key Accomplishments (March 2020 – September 2020) |
|---|---|---|---|---|---|
| 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** | • Coordinated with ORM to ensure 100% of new hires received privacy training.<br>• Conducted Role-Based Training for Assessors, ISSOs, Business Owners, PSRs, PSR and AG Users, Account Security, and the CUI Program.<br>• 100% of current FRTIB employees completed Annual Privacy Training.<br>• Published two System of Records Notice (SORN) in the Federal Register; two SORNs under review with OMB.<br>• Completed 18 PTAs and 7 PIA.<br>• Completed 14 assessments of the NIST SP 800-53 Rev 4 privacy controls as a part of the Assessment & Authorization (A&A) 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 - TSP Fraud

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 (12/31/19) | Risk Treatment Plan Status* (09/30/20) | Future Risk Score** (12/31/20) | Key Accomplishments (March 2020 – September 2020) |
|---|---|---|---|---|---|
| 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 | • Deployed faster transaction notification when money transactions are requested via Short Message Service (SMS) and/or email address.<br>• Deployed an updated algorithm for the forms review process to include 100% review for financial institutions known to be used in fraudulent withdrawal attempts.<br>• Provide Short Message Service (SMS) text and email to old and new phone numbers and email addresses when participants update their contact information. |

*** 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

**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 (12/31/19) | Risk Treatment Plan Status* (09/30/20) | Future Risk Score** (12/31/20) | Key Accomplishments (March 2020 – September 2020) |
|---|---|---|---|---|---|
| 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** | **2-3 Month Delay** | **Medium High** | • Established a partnership and identified key dependencies to address the risks.<br>• Shift from Enterprise Acquisition Planning to address future needs related to improve overall Agency planning.<br>• Present the draft strategy to the OCFO and OEP Director by November 2020. |

*** 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.**

# Current ERM Program Key Initiatives

Supply Chain Risk Management

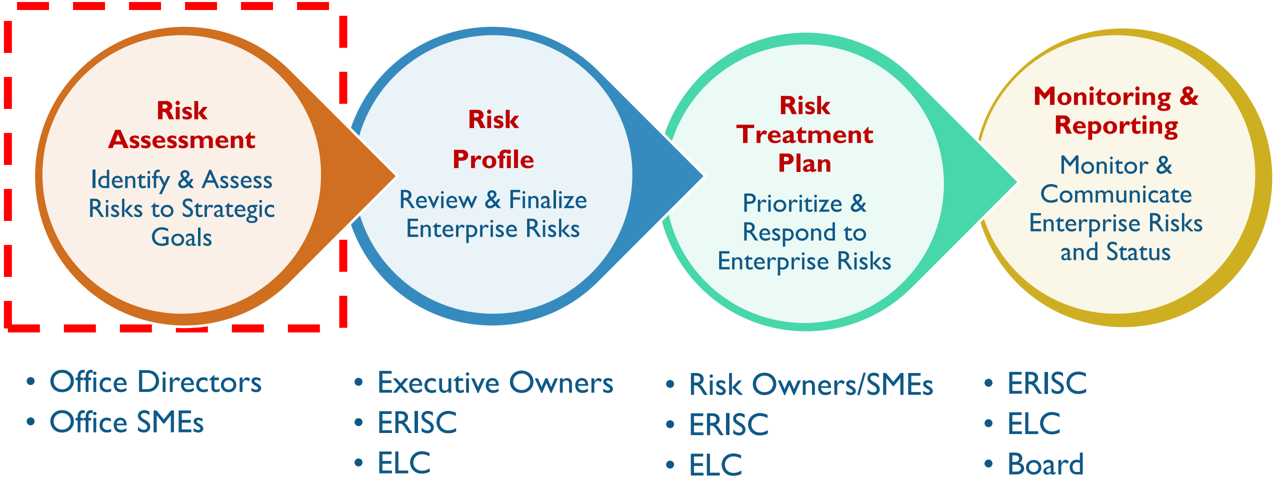
Cyber-ERM Integration

Cyber-Stat

Risk Acceptance Practices

OMB ERM Maturity Pilot @ FRTIB

# CY2021 ERM Program Cycle and Status – Kickoff Started in September 2020



**Risk Assessment**

Identify & Assess Risks to Strategic Goals

- Office Directors
- Office SMEs

**Risk Profile**

Review & Finalize Enterprise Risks

- Executive Owners
- ERISC
- ELC

**Risk Treatment Plan**

Prioritize & Respond to Enterprise Risks

- Risk Owners/SMEs
- ERISC
- ELC

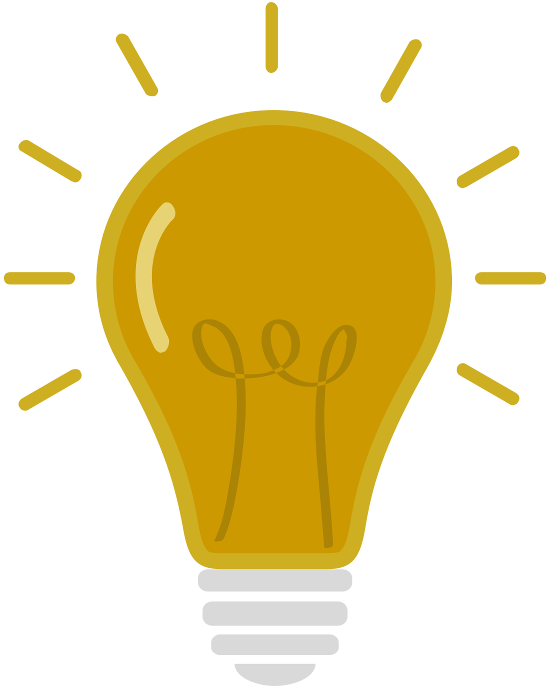
**Monitoring & Reporting**

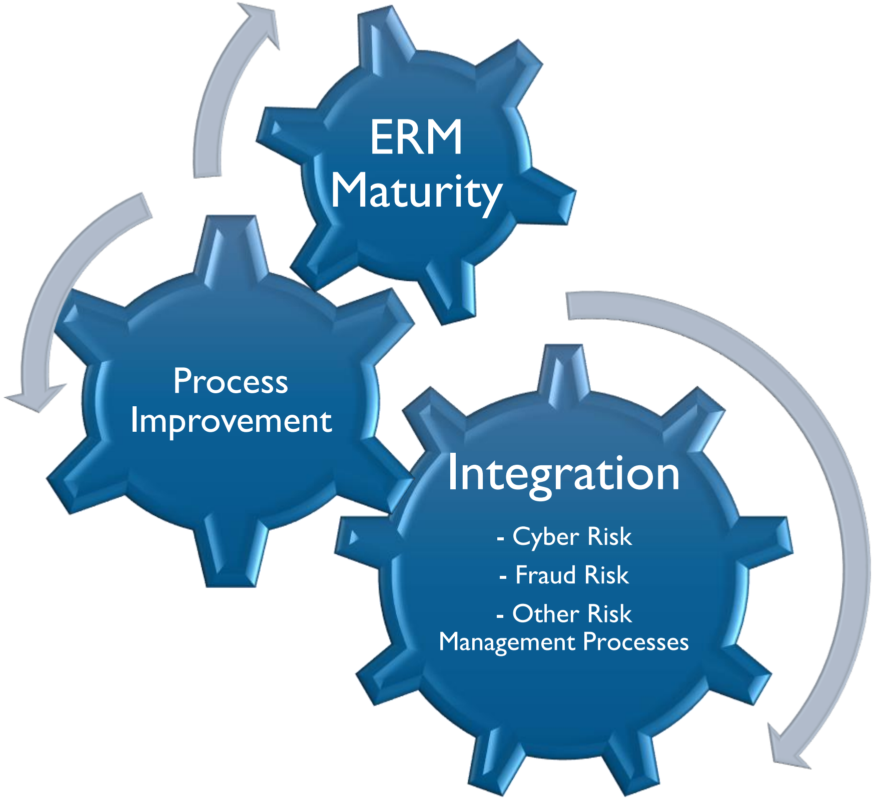
Monitor & Communicate Enterprise Risks and Status

- ERISC
- ELC
- Board

OERM Support and Coordination

# Upcoming Key ERM Initiatives




ERM Maturity
Process Improvement
Integration
- Cyber Risk
- Fraud Risk
- Other Risk Management Processes