ENTERPRISE CYBERSECURITY RISK MANAGEMENT (ECRM) PROGRAM

ECRM PROGRAM OBJECTIVES

CYBERSECURITY RISK MANAGEMENT

Enables leadership to make informed decisions supported by quantitative data

RELIABLE METRICS

Tracks measurable progress of risk mitigations and responses to minimize risk exposure and enforce accountability

INFORMED INSIGHTS

Provides quantitative risk assessments to drive leadership decision making based on organization's vulnerabilities and risk threshold.

DEFENSIBLE RESULTS

Provide defensible quantitative driven decisions based on updated and verified data inputs.

GOALS & KEY ACTIVITIES

Improve cybersecurity risk assessment methodologies and processes to support informed leadership decisions.

- Government-tailored FAIR Training
- Topical Risk Themes and Assessment blueprints to enable stakeholders to conduct Risk analyses
- Integrate ECRM principles and practices into existing Cybersecurity Trainings
- Provide stakeholders a Resource Library and Community of Practice to enable stakeholders to learn and collaborate

Build upon fundamentals by providing training and analysis opportunities for practitioners.

- Support beginner to advanced risk analyses w alkthroughs
- Collaborate w ith SMEs to tailor analyses based on stakeholders' priorities
- Provide enhanced guidance on FAIR-to-Federal requirements support
- Develop guidance for assessment reporting and presentation

Demonstrate the value of effective "blended" risk management

- Complete analyses on cybersecurity investments based on stakeholders Risk Threshold
- Enhance Risk Analysis Dashboard for effective leadership reporting
- Analyze Risk Register submissions to drive program strategy
- Conduct joint analyses w ith interested Federal Agency partners
- Conduct Community of Practice sessions, FAIR chapters, Site Onboarding, Federal CISO Council, etc.

SERVICES

STAKEHOLDER SUPPORT

- Template materials and w orksheets
- Risk Management Methodology
- Working Group Sessions

CONSULTATIVE SERVICES

- Virtual single-assessment sessions
- Virtual stakeholder engagement sessions
- Workshops (one-off analysis and assessment support)

TRAINING OFFERINGS

- Standard Operating Procedures (SOPs)
- FAIR Training
- Assessment Blueprints
- Virtual site onboarding and training
- Vendor training opportunities

METHODOLOGY

The enterprise risk management program recommends a blended qualitative/quantitative method, incorporating DOE Cybersecurity Risk Management Methodology Amplification Guidance, Factor Analysis of Information Risk (FAIR), Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST), Executive Order (EO), Cybersecurity and Infrastructure Security Agency (CISA).