U.S. DEPARTMENT OF ENERGY

FAIRCON Event Series

Maturing A Quantitative Risk Management Program in the Federal Government

Presentation and Discussion with Ignatius Liberto, Department of Energy

DOE OCIO ECRM Team

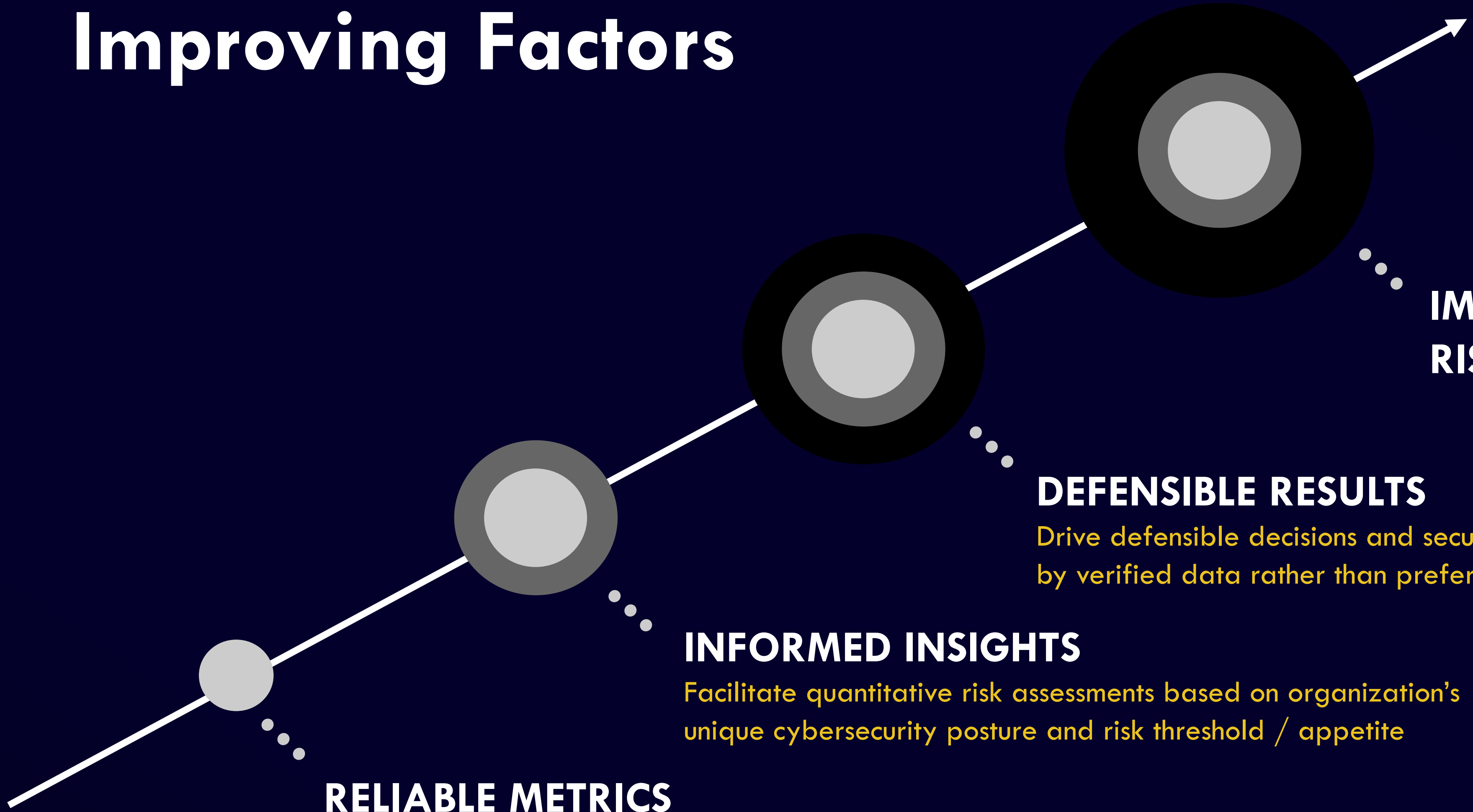
Ignatius Liberto
Director, IM-32
Department of Energy

Lili Cameron
Program Manager, IM-32
Department of Energy

Claudine Roxas
Strategy & Advisory Lead
Department of Energy

John Lamm
ECRM Team Lead
Department of Energy

Improving Factors



IMPROVED CYBERSECURITY RISK MANAGEMENT

DEFENSIBLE RESULTS

Drive defensible decisions and secure investment decisions driven by verified data rather than preferences or red herrings

INFORMED INSIGHTS

Facilitate quantitative risk assessments based on organization’s unique cybersecurity posture and risk threshold / appetite

RELIABLE METRICS

Track measurable progress of risk mitigations and responses to minimize risk exposure and promote accountability

Keys to Maturing a Program

ANALYSIS COOPRATION

External assessments rely on participation and responsiveness of the stakeholder organizations

SCALABILITY AND ADOPTION

Translating analysis findings into applicable terms for your organization

TAILORING

Customizing FAIR language and training to the government space and missions; overcoming lack of industry standards

ADAPTABILITY

Customize industry best practices and methodologies to your organization’s interests

Challenges: External Communication

DATA GATHERTING

Getting cooperation and buy-in from subject matter experts and data owners

COMMUNICATING RESULTS

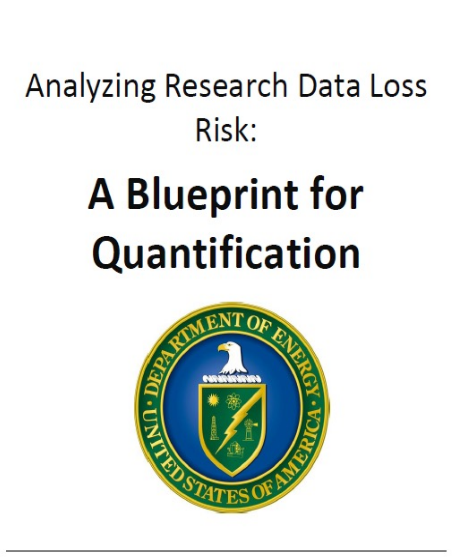
Translating analysis findings into applicable terms for your organization

RESOURCE MANAGEMENT

Clarifying expectations in resource-constrained environment with few dedicated risk analysts

External Communication Resources

Pitch risk management as an offering and fill in resource gaps by maximizing a team's efficiency with supportive materials and streamlined, replicable processes

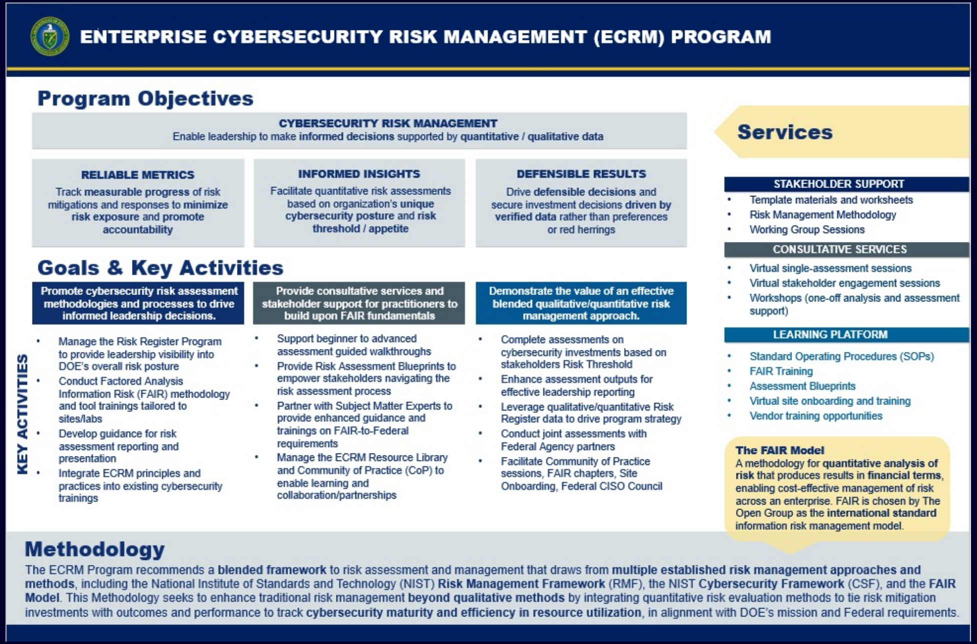


Analyzing Research Data Loss Risk:

A Blueprint for Quantification

Risk Assessment Blueprints

Provides sites and labs walkthroughs for scoping relevant topics as specified by DOE leadership



ENTERPRISE CYBERSECURITY RISK MANAGEMENT (ECRM) PROGRAM

Program Objectives

CYBERSECURITY RISK MANAGEMENT
Enable leadership to make **informed decisions** supported by **quantitative / qualitative data**

RELIABLE METRICS
Track **measurable progress** of risk mitigations and responses to **minimize risk exposure and promote accountability**

INFORMED INSIGHTS
Facilitate quantitative risk assessments based on organization's **unique cybersecurity posture and risk threshold / appetite**

DEFENSIBLE RESULTS
Drive **defensible decisions** and secure investment decisions **driven by verified data** rather than preferences or red herrings

Goals & Key Activities

KEY ACTIVITIES

Promote cybersecurity risk assessment methodologies and processes to drive informed leadership decisions.

- Manage the Risk Register Program to provide leadership visibility into DOE's overall risk posture
- Conduct Factored Analysis Information Risk (FAIR) methodology and tool trainings tailored to sites/labs
- Develop guidance for risk assessment reporting and presentation
- Integrate ECRM principles and practices into existing cybersecurity trainings

Provide consultative services and stakeholder support for practitioners to build upon FAIR fundamentals

- Support beginner to advanced assessment guided walkthroughs
- Provide Risk Assessment Blueprints to empower stakeholders navigating the risk assessment process
- Partner with Subject Matter Experts to provide enhanced guidance and trainings on FAIR-to-Federal requirements
- Manage the ECRM Resource Library and Community of Practice (CoP) to enable learning and collaboration/partnerships

Demonstrate the value of an effective blended qualitative/quantitative risk management approach.

- Complete assessments on cybersecurity investments based on stakeholders Risk Threshold
- Enhance assessment outputs for effective leadership reporting
- Leverage qualitative/quantitative Risk Register data to drive program strategy
- Conduct joint assessments with Federal Agency partners
- Facilitate Community of Practice sessions, FAIR chapters, Site Onboarding, Federal CISO Council

Services

STAKEHOLDER SUPPORT

- Template materials and worksheets
- Risk Management Methodology
- Working Group Sessions

CONSULTATIVE SERVICES

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

LEARNING PLATFORM

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

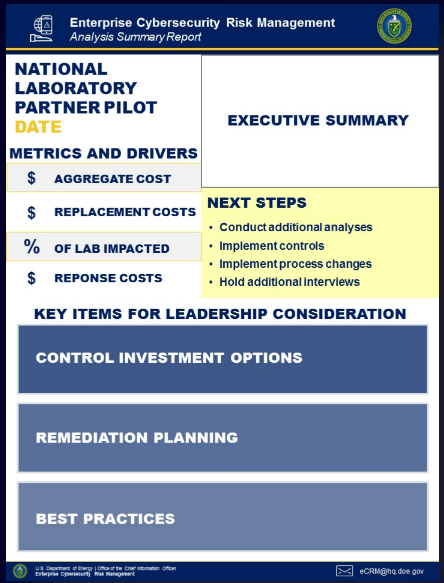
The FAIR Model
A methodology for **quantitative analysis of risk** that produces results in **financial terms**, enabling cost-effective management of risk across an enterprise. FAIR is chosen by The Open Group as the **international standard** information risk management model.

Methodology

The ECRM Program recommends a **blended framework** to risk assessment and management that draws from **multiple established risk management approaches and methods**, including the National Institute of Standards and Technology (NIST) **Risk Management Framework** (RMF), the NIST **Cybersecurity Framework** (CSF), and the **FAIR Model**. This Methodology seeks to enhance traditional risk management **beyond qualitative methods** by integrating quantitative risk evaluation methods to tie risk mitigation investments with outcomes and performance to track **cybersecurity maturity and efficiency in resource utilization**, in alignment with DOE's mission and Federal requirements.

Program Placemat

Full overview of program goals, services, methodologies and objectives



Enterprise Cybersecurity Risk Management
Analysis Summary Report

NATIONAL LABORATORY PARTNER PILOT
DATE

EXECUTIVE SUMMARY

METRICS AND DRIVERS

$	AGGREGATE COST
$	REPLACEMENT COSTS
%	OF LAB IMPACTED
$	REPONSE COSTS

NEXT STEPS

- Conduct additional analyses
- Implement controls
- Implement process changes
- Hold additional interviews

KEY ITEMS FOR LEADERSHIP CONSIDERATION

CONTROL INVESTMENT OPTIONS

REMEDIATION PLANNING

BEST PRACTICES

U.S. Department of Energy | Office of the Chief Information Officer
Enterprise Cybersecurity Risk Management

eCRM@hq.doe.gov

Reporting Templates

To transform findings into recommendations, a visual breakdown of the analysis results is required

Challenges: Education

TIERED TRAINING

Targeting training to the right audiences

FEDERAL REQUIREMENTS/GUIDELINES

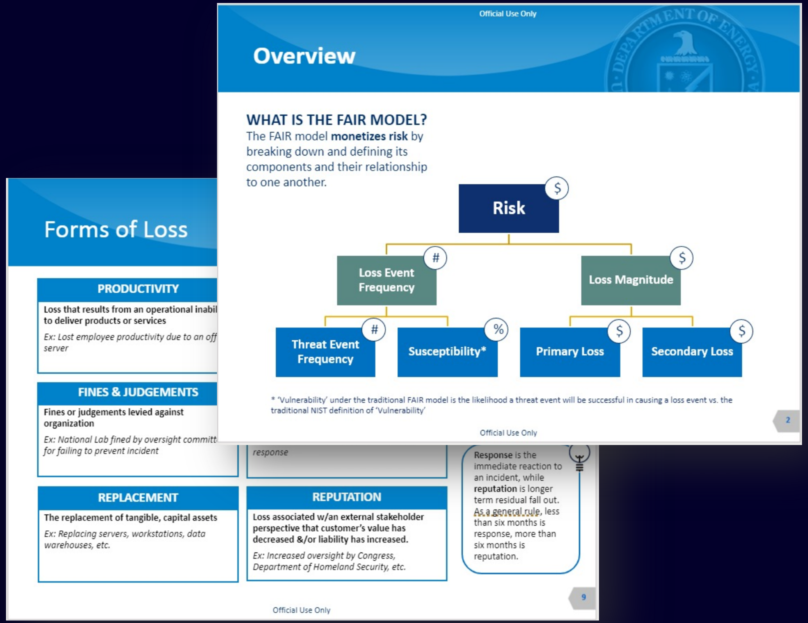
Incorporating quantitative risk management with Federal guidance

CALIBRATION TECHNIQUES

Teaching calibration in a way that is accessible and applicable

Education Resources

Recognize that risk management is not one-size-fits all for any organization or individual and offer customizable education



Official Use Only

Overview

WHAT IS THE FAIR MODEL?
The FAIR model **monetizes risk** by breaking down and defining its components and their relationship to one another.

* 'Vulnerability' under the traditional FAIR model is the likelihood a threat event will be successful in causing a loss event vs. the traditional NIST definition of 'Vulnerability'

Official Use Only

2

Forms of Loss

PRODUCTIVITY
Loss that results from an operational inabil to deliver products or services
Ex: Lost employee productivity due to an off server

FINES & JUDGEMENTS
Fines or judgements levied against organization
Ex: National Lab fined by oversight committ for failing to prevent incident

response

REPLACEMENT
The replacement of tangible, capital assets
Ex: Replacing servers, workstations, data warehouses, etc.

REPUTATION
Loss associated w/an external stakeholder perspective that customer's value has decreased &/or liability has increased.
Ex: Increased oversight by Congress, Department of Homeland Security, etc.

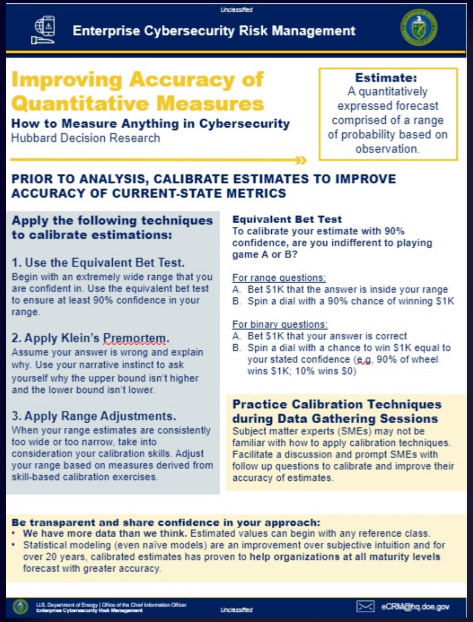
Response is the immediate reaction to an incident, while **reputation** is longer term residual fall out. As a general rule, less than six months is response, more than six months is reputation.

9

Official Use Only

Introductory Deck

Introduction to FAIR and the foundations of quantitative risk management



Unclassified

Enterprise Cybersecurity Risk Management

Improving Accuracy of Quantitative Measures

How to Measure Anything in Cybersecurity
Hubbard Decision Research

Estimate:
A quantitatively expressed forecast comprised of a range of probability based on observation.

PRIOR TO ANALYSIS, CALIBRATE ESTIMATES TO IMPROVE ACCURACY OF CURRENT-STATE METRICS

Apply the following techniques to calibrate estimations:

1. Use the Equivalent Bet Test.
Begin with an extremely wide range that you are confident in. Use the equivalent bet test to ensure at least 90% confidence in your range.

2. Apply Klein's Premortem.
Assume your answer is wrong and explain why. Use your narrative instinct to ask yourself why the upper bound isn't higher and the lower bound isn't lower.

3. Apply Range Adjustments.
When your range estimates are consistently too wide or too narrow, take into consideration your calibration skills. Adjust your range based on measures derived from skill-based calibration exercises.

Equivalent Bet Test
To calibrate your estimate with 90% confidence, are you indifferent to playing game A or B?

For range questions:
A. Bet $1K that the answer is inside your range
B. Spin a dial with a 90% chance of winning $1K

For binary questions:
A. Bet $1K that your answer is correct
B. Spin a dial with a chance to win $1K equal to your stated confidence (e.g. 90% of wheel wins $1K; 10% wins $0)

Practice Calibration Techniques during Data Gathering Sessions
Subject matter experts (SMEs) may not be familiar with how to apply calibration techniques. Facilitate a discussion and prompt SMEs with follow up questions to calibrate and improve their accuracy of estimates.

Be transparent and share confidence in your approach:
- **We have more data than we think.** Estimated values can begin with any reference class.
- Statistical modeling (even naïve models) are an improvement over subjective intuition and for over 20 years, calibrated estimates has proven to **help organizations at all maturity levels** forecast with greater accuracy.

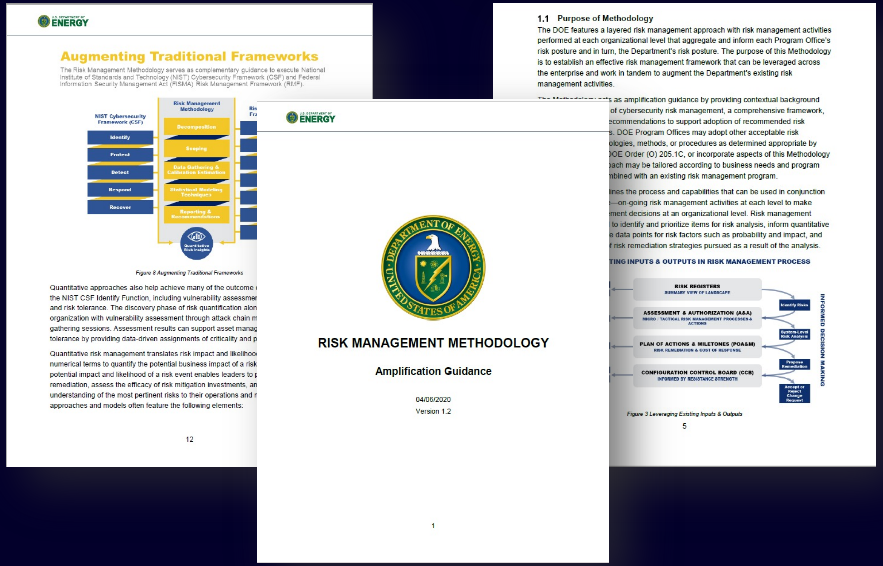
U.S. Department of Energy | Office of the Chief Information Officer
Enterprise Cybersecurity Risk Management

Unclassified

eCRM@hq.doe.gov

Theme driven One Pagers

Overviews of best practices and techniques, such as calibration



U.S. DEPARTMENT OF ENERGY

Augmenting Traditional Frameworks

The Risk Management Methodology serves as complementary guidance to execute National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Federal Information Security Management Act (FISMA) Risk Management Framework (RMF).

NIST Cybersecurity Framework (CSF)
Identify
Protect
Detect
Respond
Recover
Risk Management Methodology
Decomposition
Scoping
Data Gathering & Calibration Estimation
Statistical Modeling Techniques
Reporting & Recommendations
Quantitative Risk Insights
Ris
Fr

Figure 8 Augmenting Traditional Frameworks

Quantitative approaches also help achieve many of the outcome
the NIST CSF Identify Function, including vulnerability assessmen
and risk tolerance. The discovery phase of risk quantification alon
organization with vulnerability assessment through attack chain m
gathering sessions. Assessment results can support asset manag
tolerance by providing data-driven assignments of criticality and p

Quantitative risk management translates risk impact and likelihoo
numerical terms to quantify the potential business impact of a risk
potential impact and likelihood of a risk event enables leaders to p
remediation, assess the efficacy of risk mitigation investments, an
understanding of the most pertinent risks to their operations and r
approaches and models often feature the following elements:

12

U.S. DEPARTMENT OF ENERGY

RISK MANAGEMENT METHODOLOGY

Amplification Guidance

04/06/2020
Version 1.2

1

1.1 Purpose of Methodology

The DOE features a layered risk management approach with risk management activities performed at each organizational level that aggregate and inform each Program Office's risk posture and in turn, the Department's risk posture. The purpose of this Methodology is to establish an effective risk management framework that can be leveraged across the enterprise and work in tandem to augment the Department's existing risk management activities.

s as amplification guidance by providing contextual background
of cybersecurity risk management, a comprehensive framework,
ecommendations to support adoption of recommended risk
s. DOE Program Offices may adopt other acceptable risk
ologies, methods, or procedures as determined appropriate by
DOE Order (O) 205.1C, or incorporate aspects of this Methodology
ach may be tailored according to business needs and program
mbined with an existing risk management program.

lines the process and capabilities that can be used in conjunction
—on-going risk management activities at each level to make
ment decisions at an organizational level. Risk management
to identify and prioritize items for risk analysis, inform quantitative
e data points for risk factors such as probability and impact, and
f risk remediation strategies pursued as a result of the analysis.

TING INPUTS & OUTPUTS IN RISK MANAGEMENT PROCESS

RISK REGISTERS
SUMMARY VIEW OF LANDSCAPE
ASSESSMENT & AUTHORIZATION (A&A)
MICRO / TACTICAL RISK MANAGEMENT PROCESSES & ACTIONS
PLAN OF ACTIONS & MILETONES (POA&M)
RISK REMEDIATION & COST OF RESPONSE
CONFIGURATION CONTROL BOARD (CCB)
INFORMED BY RESISTANCE STRENGTH
Identify Risks
System-Level Risk Analysis
Propose Remediation
Accept or Reject Change Request
INFORMED DECISION MAKING

Figure 3 Leveraging Existing Inputs & Outputs

5

Amplification Guidance

Risk management methodology and integration of relevant guidance and policies

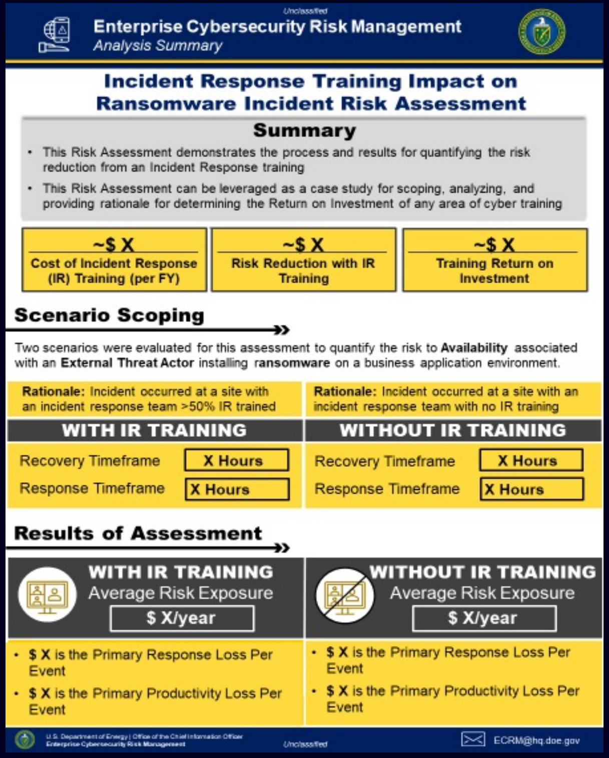
Pragmatic Use Case

Assessment Summary

The ECRM team recommends continued investment in Incident Response Training, as even a modest predicted impact on the response time and recovery timeframe results in a significant ROI for training when experiencing a Ransomware incident for a GSS asset.

Justification of Decision

- Survey results from the Training and SOC SME interviews indicated at least a 15% improvement in response ability.
- For the “With Incident Response Training” Scenario, it is assumed that the incident occurs at a laboratory with an incident response team with greater than 50% of members having attended the Incident Response Training.
- This improvement is reinforced by the participant surveys. 100% of DOE survey participants who completed the Incident Coordination Training responded positively to the survey questions.



Unclassified

Enterprise Cybersecurity Risk Management
Analysis Summary

Incident Response Training Impact on Ransomware Incident Risk Assessment

Summary

- This Risk Assessment demonstrates the process and results for quantifying the risk reduction from an Incident Response training
- This Risk Assessment can be leveraged as a case study for scoping, analyzing, and providing rationale for determining the Return on Investment of any area of cyber training

~$ X	~$ X	~$ X
Cost of Incident Response (IR) Training (per FY)	Risk Reduction with IR Training	Training Return on Investment

Scenario Scoping

Two scenarios were evaluated for this assessment to quantify the risk to **Availability** associated with an **External Threat Actor** installing **ransomware** on a business application environment.

Rationale: Incident occurred at a site with an incident response team >50% IR trained	**Rationale:** Incident occurred at a site with an incident response team with no IR training
WITH IR TRAINING	**WITHOUT IR TRAINING**
Recovery Timeframe: X Hours	Recovery Timeframe: X Hours
Response Timeframe: X Hours	Response Timeframe: X Hours

Results of Assessment

WITH IR TRAINING Average Risk Exposure $ X/year	**WITHOUT IR TRAINING** Average Risk Exposure $ X/year
• $ X is the Primary Response Loss Per Event • $ X is the Primary Productivity Loss Per Event	• $ X is the Primary Response Loss Per Event • $ X is the Primary Productivity Loss Per Event

U.S. Department of Energy | Office of the Chief Information Officer
Enterprise Cybersecurity Risk Management

Unclassified

ECRM@hq.doe.gov

Key Takeaways

USE CASES

Let your tactical success drive your program.

Don't get hung up on an enterprise-wide silver bullet strategy. Find tactical applications for the work and employ quantitative risk management for specific use cases to meet demands of your stakeholders.

TEMPLATES

Build a library of tailorable templates to help lighten the load for your resources.

Use these templates to guide analyses and streamline reporting and training.

EXECUTIVE MESSAGING

Develop talking points and field-tested / effective language that can be tailored for different types of leadership.

Customize based on the priorities of the organization and include tactical success stories.

For additional information:
Email the DOE ECRM Team (ecrm@hq.doe.gov)