CYBERSECURITY RISK MANAGEMENT METHODOLOGY

Amplification Guidance

5 August 2021

Final Version

Approval Page

I have reviewed all content contained within this Cybersecurity Risk Management Methodology Amplification Guidance. I sincerely appreciate all the innovation, hard work and team collaboration. I concur with the content and approve this Risk Management Methodology Amplification Guidance for widest dissemination across the Department of Energy and with other Risk Management Stakeholders across the Federal Government.

Signature: Ignatius P. Liberto Digitally signed by Ignatius P. Liberto Date: 2021.08.05 13:05:56 -04'00' Date: 5 August 2021

Ignatius Liberto
Director, Cybersecurity Compliance & Oversight (IM-32)
Office of the Chief Information Officer
U.S. Department of Energy
Ignatius.Liberto@hq.doe.gov

Document Revision History

Version	Date	Changed By	Notes
1.2	04/06/2020	IM-32	Initial Amplification Guidance Publish Date
1.3	06/30/2020	IM-32	Updated based on IM-32 review & CISO Roundtable Member Review

Table of Contents

Table of Figures

1.0 Methodology Background

The Department of Energy (DOE) has developed a Risk Management Methodology (Methodology) as amplification guidance for executing risk management to support risk-based decisions. The Methodology serves to describe the scope, processes, terms, and methods the Department can leverage to meet Federal requirements to manage security and privacy risks to the agency's operations and assets. The Methodology utilizes a blended framework to risk assessment and management, drawing from multiple established risk management approaches and methods. In addition, this Methodology documents the Department's approach to executing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Risk Management Framework (RMF) and NIST Framework for Improving Critical Infrastructure Cybersecurity and Cybersecurity Framework (CSF) to enhance risk management beyond traditional qualitative methods. This Methodology integrates quantitative risk evaluation methods to tie risk mitigation investments with outcomes and performance to track cybersecurity maturity and efficiency in resource utilization. The suggested risk management process set forth in this Methodology builds upon this foundation by promoting a continuous and iterative process in alignment with Federal guidance.

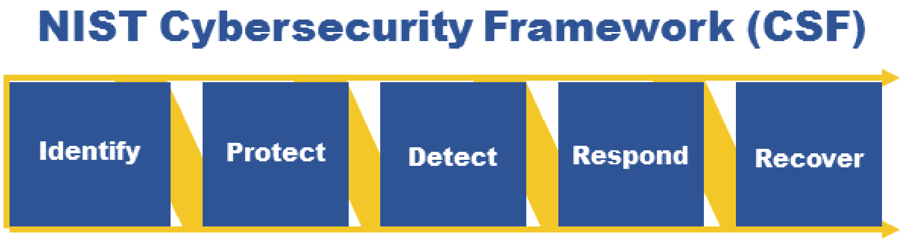


Figure 1 NIST Cybersecurity Framework

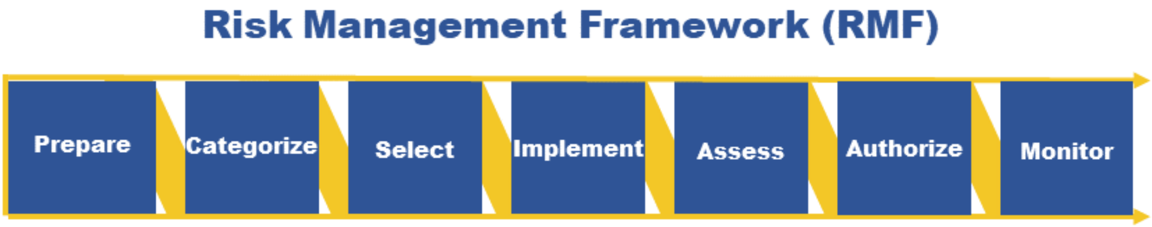


Figure 2 Risk Management Framework

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.

The Methodology acts as amplification guidance by providing contextual background about the importance of cybersecurity risk management, a comprehensive framework, and implementation recommendations to support adoption of recommended risk management methods. DOE Program Offices may adopt other acceptable risk management methodologies, methods, or procedures as determined appropriate by their leadership, per DOE Order (O) 205.1C, or incorporate aspects of this Methodology as needed. The approach may be tailored according to business needs and program goals and can be combined with an existing risk management program.

The Methodology outlines the process and capabilities that can be used in conjunction with—and to leverage—on-going risk management activities at each level to make informed risk management decisions at an organizational level. Risk management activities can be used to identify and prioritize items for risk analysis, inform quantitative estimates, and provide data points for risk factors such as probability and impact, and document the value of risk remediation strategies pursued as a result of the analysis.

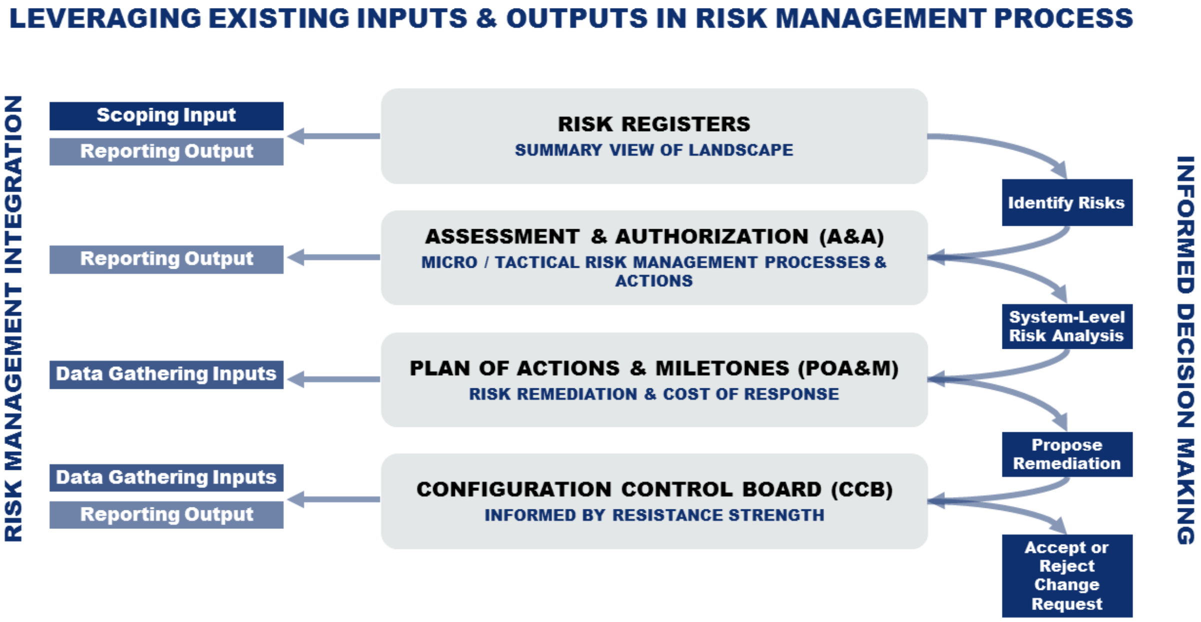

LEVERAGING EXISTING INPUTS & OUTPUTS IN RISK MANAGEMENT PROCESS
RISK MANAGEMENT INTEGRATION
Scoping Input
Reporting Output
RISK REGISTERS
SUMMARY VIEW OF LANDSCAPE
Identify Risks
Reporting Output
ASSESSMENT & AUTHORIZATION (A&A)
MICRO / TACTICAL RISK MANAGEMENT PROCESSES & ACTIONS
System-Level Risk Analysis
Data Gathering Inputs
PLAN OF ACTIONS & MILETONES (POA&M)
RISK REMEDIATION & COST OF RESPONSE
Propose Remediation
Data Gathering Inputs
Reporting Output
CONFIGURATION CONTROL BOARD (CCB)
INFORMED BY RESISTANCE STRENGTH
Accept or Reject Change Request
INFORMED DECISION MAKING

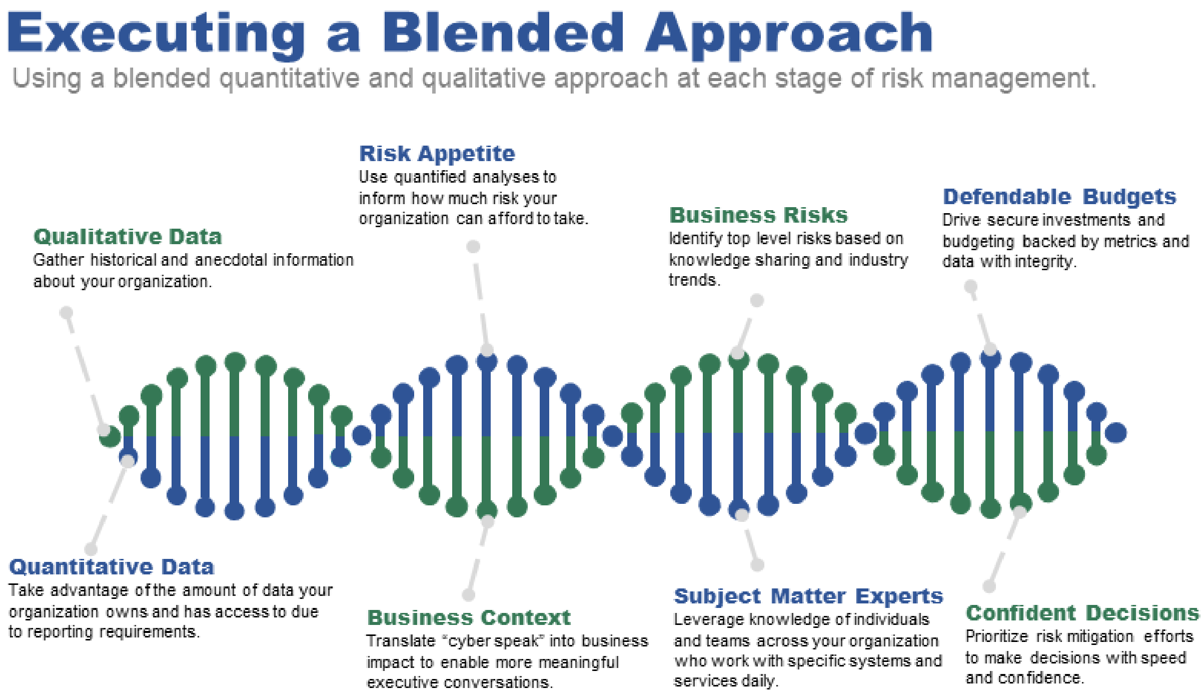
Figure 3 Leveraging Existing Inputs & Outputs

These risk management activities support and fill in data or information gaps to ensure leaders make informed risk decisions, leveraging the tools and resources available and the information derived from reporting requirements they already adhere to.

This Methodology includes a lexicon designed to codify a common vocabulary and language around which risk information can be structured, aggregated, analyzed, and communicated. A common language supports the ability to clearly communicate cyber risk information across the enterprise, enables aggregation, and can improve risk mitigation efforts. The lexicon within this Methodology lays out the terms that are essential to the practice of risk assessment and management. It intends to de-conflict and improve risk management discussions among DOE risk stakeholders. The lexicon will continuously evolve as risk management matures and expands to include other approaches and frameworks that may arise. However, it must be noted that other definitions for terms found in the lexicon may be found in guidance, regulations, or statutes that will be specifically applicable in those regulatory or legal contexts.

1.2 Approach of Methodology

The Methodology utilizes a blended approach by incorporating a standard quantitative model to strengthen, rather than replace, its existing risk analysis processes, complementing its use of the CSF and RMF methodologies for risk management. The Methodology leverages quantitative risk analysis methods to derive data-backed models and metrics to power risk management and investment decisions. Quantitative methods are used in conjunction with existing qualitative approaches to strengthen risk analysis phases, such as risk factor calibration and estimation, to reduce the overall level of uncertainty found in risk assessment and management. The blended approach outlined in Figure 4 seeks to create a consistent, repeatable, and precise practice of risk management to better support and inform risk recommendations. The Methodology intends to provide a foundation that National Laboratories, Sites, and Program Offices can incorporate into their programs and processes.



Executing a Blended Approach

Using a blended quantitative and qualitative approach at each stage of risk management.

Qualitative Data
Gather historical and anecdotal information about your organization.

Risk Appetite
Use quantified analyses to inform how much risk your organization can afford to take.

Business Risks
Identify top level risks based on knowledge sharing and industry trends.

Defendable Budgets
Drive secure investments and budgeting backed by metrics and data with integrity.

Quantitative Data
Take advantage of the amount of data your organization owns and has access to due to reporting requirements.

Business Context
Translate "cyber speak" into business impact to enable more meaningful executive conversations.

Subject Matter Experts
Leverage knowledge of individuals and teams across your organization who work with specific systems and services daily.

Confident Decisions
Prioritize risk mitigation efforts to make decisions with speed and confidence.

Figure 4 Executing a Blended Approach

1.2.1 DOE Federated Model

The DOE has a unique set of missions that spans national security, science, operations, and partnership functions. This uniquely broad mission set has required a federated model for oversight and management of all functions, including cybersecurity and risk management. The federated model enables National Laboratories, Sites, and Program Offices to operate with significant independence to execute their missions while adhering to Department standards. At the same time, establishing an enterprise-wide cybersecurity risk management program requires aggregation across all departments, functions, and missions.

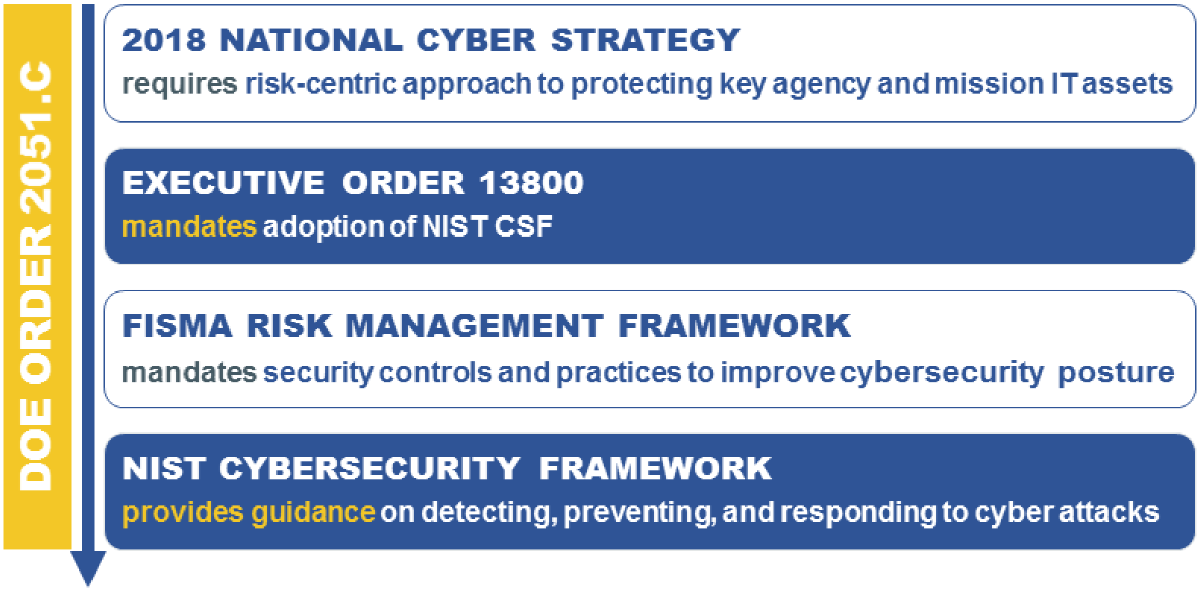
However, this autonomy presents a unique challenge to enterprise cybersecurity engagement. Under the existing "Centers of Excellence" cyber capability model, National Laboratories, Sites, and Program Offices build, own, and operate their cybersecurity programs with autonomy and self-sufficiency, often with their own self-developed and defined methods and frameworks. The disparate methods used substantially impact the DOE's ability to efficiently prioritize and allocate resources to safeguard essential information technology (IT) assets, information, and the operations dependent upon them. To effectively aggregate risk management information from its

Program Offices, DOE requires the ability to maintain operational visibility over cyber performance at the enterprise level.

The Department has initiated the Enterprise Cybersecurity Risk Management (ECRM) program to begin building a common foundation for cyber risk assessment and management. Through successful partnership with National Laboratories, Sites, and Program Offices, and continued efforts to refine the Department's ECRM program and Methodology, supporters can realize gains in the following areas:

- Enable leadership at all levels to make better decisions today than yesterday, with a stronger business case;
- Track measurable progress of risk mitigations and responses to minimize risk exposure and enforce accountability;
- Provide measurable risk value to decisions with improved knowledge of your organization's susceptibility and risk response options; and
- Promote secure, defendable investment decisions driven by data, not preferences or red herrings.

1.3 Cybersecurity Risk Management Federal Requirements



DOE ORDER 2051.C

2018 NATIONAL CYBER STRATEGY
requires risk-centric approach to protecting key agency and mission IT assets

EXECUTIVE ORDER 13800
mandates adoption of NIST CSF

FISMA RISK MANAGEMENT FRAMEWORK
mandates security controls and practices to improve cybersecurity posture

NIST CYBERSECURITY FRAMEWORK
provides guidance on detecting, preventing, and responding to cyber attacks

Figure 5 Relationship of Federal Guidance and Policies

Risk assessment and management are key activities necessary for complex organizations to use finite resources to defend against cyber-attacks, which are growing in both sophistication and consequence. To address these challenges, the 2018 National Cyber Strategy (the Strategy) introduces requirements for a risk-centric approach to efficiently allocate resources to protect key agency and mission IT assets.

By aligning risk management with IT and business activities, the Strategy seeks to improve Federal network security. In addition, Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, mandates the adoption of the NIST CSF as a broad framework that agencies, regardless of their mission, can implement to accomplish the requirements outlined in the Strategy to augment existing statutes under FISMA and guidance within the RMF.

To execute requirements under the RMF and implement the NIST CSF, the DOE released DOE Order (O) 205.1C, *Department of Energy Cyber Security Program*. DOE O 205.1C is designed to enable leadership with the programmatic and operational flexibility necessary to make consistent, risk-informed investment decisions. DOE O 205.1C calls for a risk management approach that includes both quantitative and qualitative methods to mature risk management across the enterprise with the latest industry risk approaches that support informed cybersecurity risk decision-making. Figure 5 shows the relationship between each of these Federal policies and guidance.

The infusion of quantitative methods enables risk scenario comparisons and prioritization, performance and metrics tracking and benchmarking, and concrete indicators on cybersecurity maturity by removing the sole reliance on subjective and general assessments. This allows for a more robust discussion of enterprise risks to critical assets, missions, and business functions. Through its lexicon, the Methodology's ontology is focused on combining the taxonomies of multiple frameworks, particularly the NIST CSF, to minimize confusion or disruption and contradiction with current risk management programs across the Department.

This Methodology is in alignment with and executes requirements under DOE O 205.1C, section 4.f.1.d, by documenting processes and procedures for cyber risk assessment and management that can be leveraged across the Department by National Laboratories, Sites, and Program Offices. Consistency in decision-making will enhance communication between the Department's business and cyber professionals and partners to support effective implementation and delegation of risk management.

The blended approach within this Methodology incorporates the NIST CSF, RMF, and Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (Green Book). The GAO Green Book outlines risk management through a series of steps: aligning the Methodology process to agency goals, identification of risks, assessing risk, selecting risk responses, monitoring risks, and communicating and reporting risks. The steps outlined in this Methodology—decomposition, scoping, data gathering and calibration, statistical modeling techniques, and reporting and recommendations—align to the GAO's recommended steps.

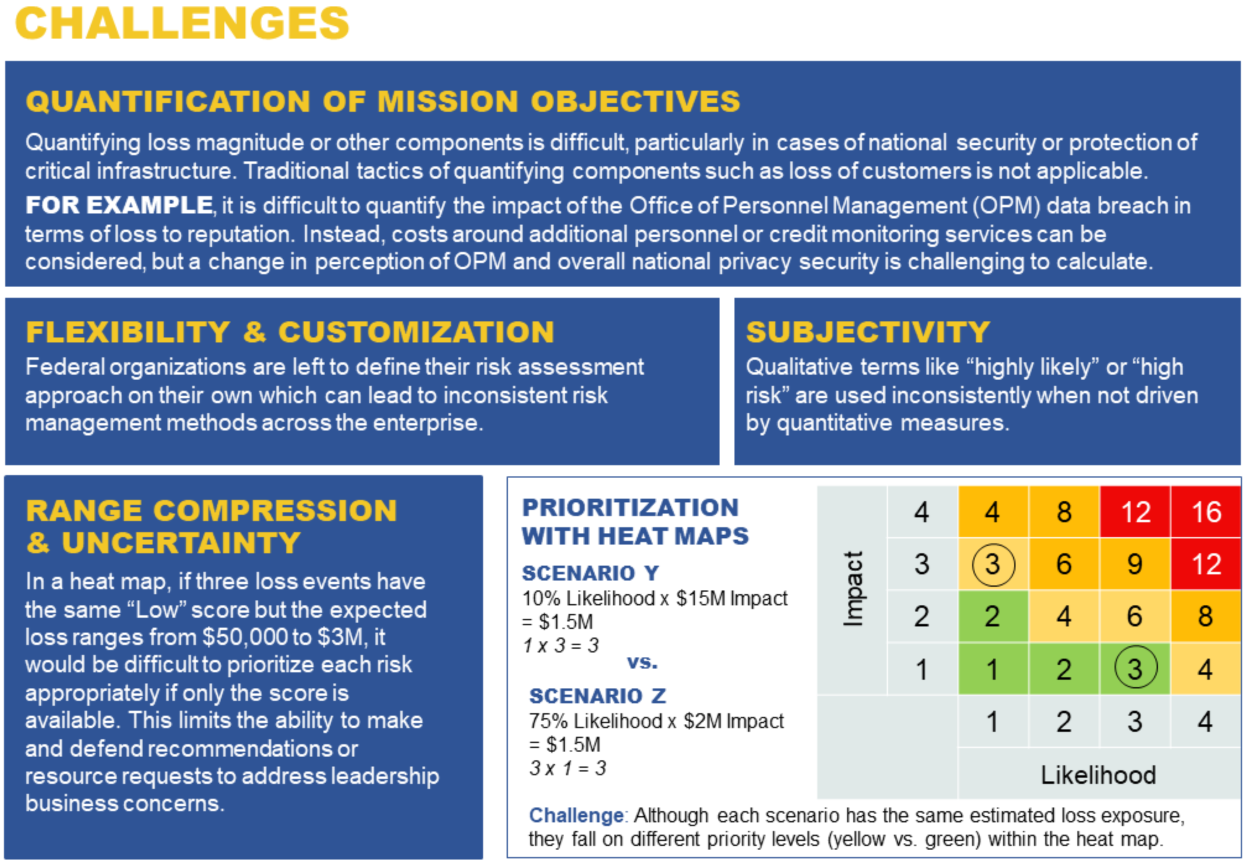
The Methodology's implementation and relevance can further be supported by Federal Information Technology Acquisition Reform Act (FITARA). FITARA is a far-reaching IT reform legislation that expanded the role, responsibilities, and authorities of the CIO to provide enterprise-wide direction for managing IT and cybersecurity. FITARA provides that the CIO is to report directly to the Secretary and Deputy Secretary for carrying out certain CIO functions. It also provides best practices in IT management and cybersecurity. The ability to continuously monitor agency networks using tools to mitigate and remediate cyber threats (i.e., ability to identify, protect, detect, respond, and recover) can be measured using the FITARA score card.

2.0 National Institute of Standards and Technology Cybersecurity Framework

The NIST CSF, required under EO 13800, offers a flexible way for organizations to address cybersecurity risks and track their cybersecurity program maturity. Recognizing that organizations will continue to have unique risks, the CSF is not a one-size-fits-all solution, but an optional model with broad principles, goals, and steps designed to strengthen cybersecurity risk management practices, regardless of an organization's size and maturity level. This Methodology offers amplification guidance to supplement the CSF and other existing risk management practices by providing execution specificity and sequence of events to enable program maturity.

2.1 Shortcomings in Traditional Risk Management

Qualitative risk management methods pose challenges in cybersecurity risk management, particularly when it comes to execution. Some of these gaps create tactile challenges in assessments and reporting, while others present fundamental issues for risk management program implementation. An overview of common challenges is outlined in Figure 6.



CHALLENGES

QUANTIFICATION OF MISSION OBJECTIVES

Quantifying loss magnitude or other components is difficult, particularly in cases of national security or protection of critical infrastructure. Traditional tactics of quantifying components such as loss of customers is not applicable.

FOR EXAMPLE, it is difficult to quantify the impact of the Office of Personnel Management (OPM) data breach in terms of loss to reputation. Instead, costs around additional personnel or credit monitoring services can be considered, but a change in perception of OPM and overall national privacy security is challenging to calculate.

FLEXIBILITY & CUSTOMIZATION

Federal organizations are left to define their risk assessment approach on their own which can lead to inconsistent risk management methods across the enterprise.

SUBJECTIVITY

Qualitative terms like "highly likely" or "high risk" are used inconsistently when not driven by quantitative measures.

RANGE COMPRESSION & UNCERTAINTY

In a heat map, if three loss events have the same "Low" score but the expected loss ranges from $50,000 to $3M, it would be difficult to prioritize each risk appropriately if only the score is available. This limits the ability to make and defend recommendations or resource requests to address leadership business concerns.

PRIORITIZATION WITH HEAT MAPS

SCENARIO Y
10% Likelihood x $15M Impact
= $1.5M
1 x 3 = 3

vs.

SCENARIO Z
75% Likelihood x $2M Impact
= $1.5M
3 x 1 = 3

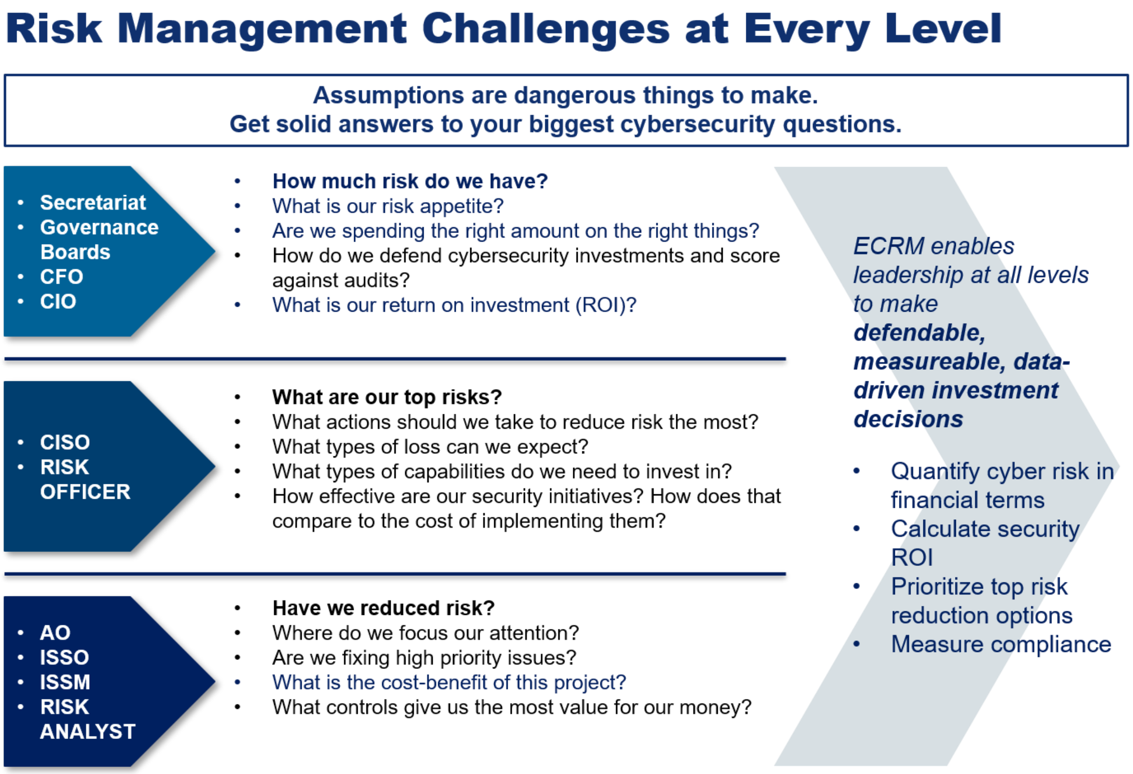
Impact					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		Likelihood			

Challenge: Although each scenario has the same estimated loss exposure, they fall on different priority levels (yellow vs. green) within the heat map.

Figure 6 Challenges of Traditional Risk Management

2.2 Augmenting Traditional Risk Management with Quantitative Methods

To address the gaps presented in traditional risk management frameworks, this Methodology incorporates quantitative methods to augment risk assessment and inform better, more effective, risk management. The infusion of quantitative methods, while enabling great risk analysis precision, can work in tandem with qualitative methods to reduce uncertainty and overcome some of the obstacles presented by traditional methods. Some of the challenges posed by organizational leadership are included in Figure 7.



Risk Management Challenges at Every Level

Assumptions are dangerous things to make.
Get solid answers to your biggest cybersecurity questions.

- **Secretariat**
- **Governance Boards**
- **CFO**
- **CIO**

- **How much risk do we have?**
- What is our risk appetite?
- Are we spending the right amount on the right things?
- How do we defend cybersecurity investments and score against audits?
- What is our return on investment (ROI)?

- **CISO**
- **RISK OFFICER**

- **What are our top risks?**
- What actions should we take to reduce risk the most?
- What types of loss can we expect?
- What types of capabilities do we need to invest in?
- How effective are our security initiatives? How does that compare to the cost of implementing them?

- **AO**
- **ISSO**
- **ISSM**
- **RISK ANALYST**

- **Have we reduced risk?**
- Where do we focus our attention?
- Are we fixing high priority issues?
- What is the cost-benefit of this project?
- What controls give us the most value for our money?

ECRM enables leadership at all levels to make ***defendable, measureable, data-driven investment decisions***

- Quantify cyber risk in financial terms
- Calculate security ROI
- Prioritize top risk reduction options
- Measure compliance

Figure 7 Risk Management Challenges at Every Level

The NIST CSF boasts five Framework Core Functions: Identify, Protect, Detect, Respond, and Recover. These functions aid organizations in aligning and prioritizing their cybersecurity activities with its business or mission requirements, risk tolerances, and resources. The Identify Function supports organizational understanding and visibility to improve risk management. The implementation process outlined in this Methodology supports this alignment and prioritization by supplementing traditional risk management methods with a quantitative approach. This augmentation can be seen in Figure 8. The processes of quantitative risk management encourage a breakdown of siloes within an organization to identify mission-supporting systems and servers, interdependencies that impact business operations, and important controls.

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).

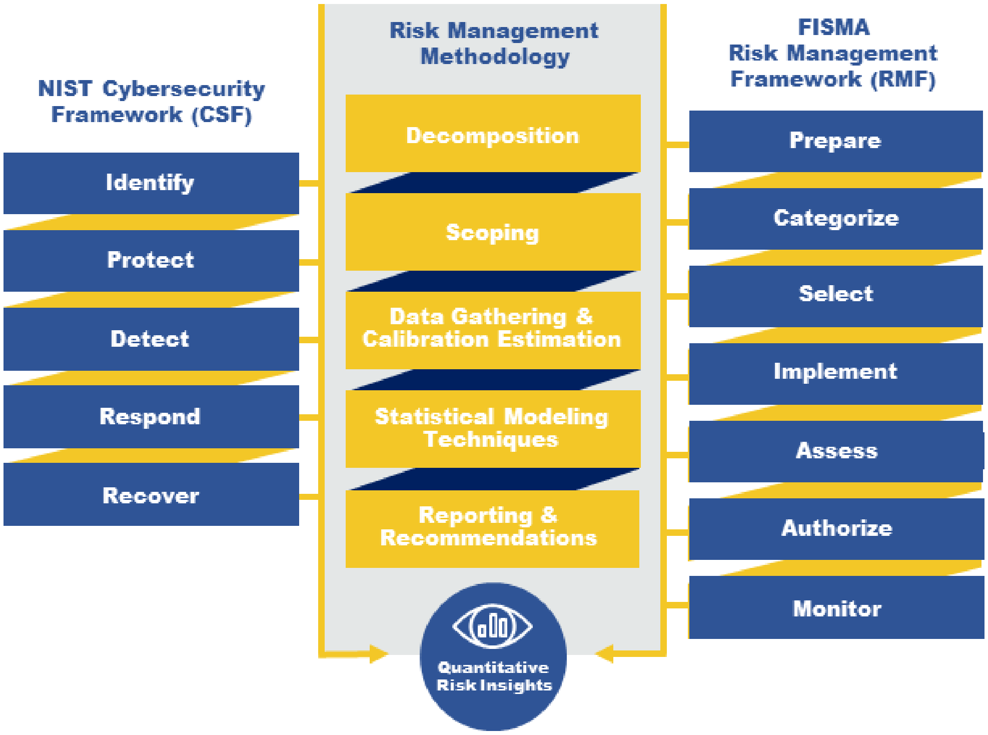

NIST Cybersecurity Framework (CSF)
Identify
Protect
Detect
Respond
Recover
Risk Management Methodology
Decomposition
Scoping
Data Gathering & Calibration Estimation
Statistical Modeling Techniques
Reporting & Recommendations
Quantitative Risk Insights
FISMA Risk Management Framework (RMF)
Prepare
Categorize
Select
Implement
Assess
Authorize
Monitor

Figure 8 Augmenting Traditional Frameworks

Quantitative approaches also help achieve many of the outcome categories outlined in the NIST CSF Identify Function, including vulnerability assessment, asset management, and risk tolerance. The discovery phase of risk quantification alone can help an organization with vulnerability assessment through attack chain mapping and data gathering sessions. Assessment results can support asset management and risk tolerance by providing data-driven assignments of criticality and prioritization.

The NISTIR 8286A Draft outlines a quantitative approach to identification and estimation of Cybersecurity Risk for Enterprise Risk Management (ERM). The document emphasizes the importance of cybersecurity risk management (CRM) as a key aspect within ERM. An additional quantitative risk management approach leveraged is Factor Analysis of Information Risk (FAIR). FAIR involves the creation of scenarios outlining threat event frequency, vulnerability, primary loss, and secondary loss associated with a risk. The outcome of the FAIR Risk Assessment is a quantitative measure of risk in financial terms.

Such as in NISTIR 8286A and FAIR, quantitative risk management translates risk impact and likelihood factors into numerical terms to quantify the potential business impact of a risk. Quantifying the potential impact and likelihood of a risk event enables leaders to prioritize risks for remediation, assess the efficacy of risk mitigation investments, and gain a better understanding of the most pertinent risks to their operations and missions. Quantitative approaches and models often feature the following elements:

- An ontology of risk factors and their relationships to one another with standardized definitions;
- Risk factor cost measurement through organizational and industry benchmarks and estimates; and
- Scenario modelling through statistical methods, such as Monte Carlo simulations, to capture dynamic and complex changes and forecast risk event likelihood and costs.

By using quantitative data to bolster qualitative data for risk and risk factor analysis, evaluation, and prioritization, risk mitigation can be viewed as an investment decision. Investments can be defended through scenario modeling and documented cost-savings and efficiency gains to empower leadership and strategic planning. Through techniques such as calibration, data points and estimates can be used in tandem with stakeholder interviews and subject matter expert (SME) insights to build credibility in risk recommendations. Statistical modeling techniques are leveraged to understand the impact of risk and uncertainty on a given risk event or scenario and support decisions on prioritization and resource utilization.

3.0 Challenges of Risk Management

One of the challenges of risk management is the need for a standardized ontology, which often redefines traditional risk factors and terminology. In this context, ontology refers to a way of showing the properties of a subject area and how they are related. Redefining traditional risk factors and terms requires organizations to either adopt the entire ontology overall, or carefully refine and document their own blended ontology to complement and interplay with existing methodologies and taxonomies. For example, NIST, which has been the traditional source of risk management guidance by Federal organizations, defines vulnerability as a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.” This stands in contrast to a quantitative understanding of vulnerability as a “the probability that a threat event will become a loss event.” Other areas where the quantitative ontology differs from traditional risk management terminology includes the use of “frequency” instead of “likelihood,” and “magnitude” instead of “impact.”

Establishing a common understanding of risk extends beyond building a standardized ontology. A common definition and understanding of risk sets the foundation for a common attitude and perspective around cybersecurity risk management. Within this Methodology “risk” refers to how likely an adverse threat event is to occur, and how much loss will be experienced if it does. The way this risk can be represented—as an estimate of monetary loss within a specific timeframe—stands in contrast to traditional concepts of risk that may not have tangible values to defend labels of “high” or “low” risk and are based on subjective measures.

This departure from traditional concepts of risk increases the challenge of introducing new risk management methods due in part to necessary re-learning to overcome established perceptions. Effective risk management demands mutual understanding of what “risk” is, from system owners providing inputs to data gathering sessions to Chief Financial Officers receiving briefs of top cybersecurity risks in the organization. This can require a significant cultural shift in institutionalized behaviors around risk.

The DOE’s federated model poses additional unique challenges because the existing definition may vary from organization to organization depending on the mission. This organizational variance increases the difficulty of getting buy-in from stakeholders across the enterprise.

An additional challenge in implementing a new program—even introducing new elements to existing practices—lies in the requirement of upfront investments of resources, such as training. For organizations with limited risk management resources, resistance may occur when presented with new frameworks, even when optional. Particularly in the Federal space, where new policies and guidance dictate modifications and improvements, stakeholders may be reluctant to increase an already heavy risk management burden with new processes. However, these initial investments aim to simplify a complex practice by aligning efforts and ultimately streamline cybersecurity risk management efforts.

In the Federal space and beyond, risk management frameworks must be flexible by nature to adapt to an evolving threat landscape. Too rigid of a framework may leave organizations unprepared for unforeseen trends in risk. Too imprecise of a framework, and organizations are without direction for implementation.

4.0 Implementation Process Guidance

The blended approach outlined in this Methodology intends to equip organizations with the tools necessary to mitigate, avoid, and respond to risks. Implementation of this approach maps to an assessment process designed to leverage existing risk management activities and resources such as data sources and reporting requirements to inform risk management recommendations at each level of leadership. This process serves as amplification guidance to the steps outlined in the NIST CSF, RMF, and GAO Green Book.

4.1.1 Decomposition

Beginning the risk analysis process requires decomposition of an organization or office’s mission, goals, and objectives to identify risk scenarios of importance. Decomposing an organization’s mission supports identification of mission-critical business operations and assets that enables proper risk prioritization and management. Once mission-critical systems or operations are identified, common areas of risks or vulnerabilities may arise. Decomposing these areas further allows for a more granular, tactical view of broader topics or themes.

For example, an organization whose mission is national security may view cloud security as an area of concern. Addressing this concern requires decomposition of both national security-supporting operations and relevant cloud security. An organization would need to identify: what type of information is stored in the cloud to begin with, and what subset of that information is most targeted by adversaries? What is the cloud configuration security level? What other sensitive or classified information is stored in the same space or to what extent is information connected to other operations, systems, or functions? Could an adversary make an impact with this information alone, or would they require additional pieces? This decomposition enables quantification of the critical pieces that make up the larger components of an organization’s mission and the area of risk at hand to begin analyzing and prioritizing action.

To begin the scoping process, prioritize probable targets of a loss event with significant impact for analysis. Also consider current decisions organizational leadership faces—are there upcoming investment decisions for new services or subscription renewal? Have new Federal requirements been introduced that require reallocation of resources? The prioritization of the scoping and analysis of practical, time sensitive issues can demonstrate the value of risk quantification and inform better decision making.

4.1.2 Risk Scenario Scoping

The analysis scope can be decomposed using four factors: threat, effect, asset, and method. Following this structure supports a shared lexicon and understanding of what "risk" is by demanding precision when articulating details of a loss event, including the attack chain. Decomposition of a risk scenario into these components provides a deeper layer of precision to initial risk register outcomes.

When scoping a scenario, it is important to map an attack chain to prioritize paths of least resistance with maximum impact and identify attack chains that arrive at the same outcome. This step helps focus assessments on probable loss events and consider alternative attack paths. In addition, mapping attack chains supports discovery and visibility by revealing potential vulnerabilities and the significance of certain controls.

Organizations can leverage their risk registers to inform scoping by selecting risks with higher prioritization ratings for assessments. Information collected for risk registers can also help identify the components of a scenario. The risk description can help identify the threat, effect, asset, and method. The affected controls and impacted CSF functions can further narrow the specific effect and asset.

Further, information from assessments can be used to update risk registers. Assessment findings can be incorporated to increase the precision of likelihood and impact ratings, and prioritization.

4.1.3 Data Gathering and Calibration

The Methodology leverages historical data and SME insights to calibrate or refine estimates and reduce uncertainty. Often, leadership and organizations underestimate the amount of data points and knowledge at their disposal. Consider data inputs from as many relevant sources as possible including audit, inspection, and incident reports; required assessments of control testing; quarterly data calls; reporting requirements; and continuous monitoring and cybersecurity threat detection service providers. Leveraging existing data sources not only maximizes the efficacy and utility of these activities, but also minimizes the burden on stakeholders to duplicate or redirect efforts.

For example, Plan of Action and Milestones (POA&M) are a management tool for tracking the mitigation of cybersecurity program and system level findings and weaknesses. POA&Ms are used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. POA&Ms can be leveraged in the data gathering process to provide insights at the program or system level on security controls and vulnerabilities.

To augment these data points, or even supplement them in instances where data points are unavailable, engagement with SMEs is key. SMEs (e.g., system architects or product owners) can be integrated into the risk assessment process to provide insights and context around loss event frequency, susceptibility, and potential loss magnitude. SMEs can be any readily available resources with knowledge of the system or operations under review. The following recommendations are provided to minimize delays or obstacles to SME engagement:

- Conduct research in advance. Make the most of every stakeholder's time by using available resources, such as Powerpedia, incident reports, and audit findings, to get as much context as possible;
- Organize questions into categories for general (background such as system architecture), frequency (how often this loss event could occur or be attempted), and magnitude (probable fallout, such as response costs); and
- Schedule in-person data gathering sessions. Try alternative communication methods to get in touch if your points of contact are unresponsive. Set aside enough time, typically an hour, or multiple shorter meetings.

The incorporation of SMEs and institutional knowledge, both qualitative components, add a confidence dimension and greater depth to the quantitative data points and metrics obtained while also building engagement and support.

In data gathering, recurring resistance themes include the belief that something cannot be quantified (e.g., this type of loss event has never happened so we cannot calculate our response cost) and the conception that the asset in question is too unique to fit the risk quantification process. These beliefs can be overcome through the following recommendations:

- Emphasize that the problem is not as unique as believed, and there is more data than believed;
- Scope specific scenarios and decompose its elements. Broad or vague scenarios are difficult to quantify;
- Start with the absurd and eliminate highly unlikely values; and
- Use historical knowledge and industry estimates as guides.

Calibration can then be used to break down data points that are difficult to estimate by using existing data or benchmarks to create ranges for each component, such as loss event frequency and magnitude. The following example serves as a model and not an official source. Consider the question: How many ransomware attacks target a given server within a year, given the absence of incident reporting? To start calibrating, consider the information already available. While a ransomware attack has not been documented, there is a record of at least 500 malware attempts. With the first information, a lower and upper bound estimate of 1–500 is established as a range.

To start compressing that range to increase accuracy, statistics on ransomware incidents at other similar agencies are used as a benchmark. Benchmarks from similar agencies show a maximum of 50 ransomware attacks on the average server, which compresses the range estimate from 1–500 to 1–50.

Discussions with SMEs, such as system owners and incident response teams, show that ransomware attacks have been trending down with only one identified instance within the last 5 years. To be cautious, and allowing for at least a monthly attempt, this information compresses the range even further from 1–50 to 1–12.

With a more digestible estimate range built on information obtained from the constituent parts of the original variable, the accuracy of the measurement is increased by combining quantitative metrics with qualitative contextual evidence.

4.1.4 Reporting and Recommendations

Risk registers, risk scenario scoping, data gathering, and statistical modeling techniques all ultimately inform risk response strategies. Analysis results can be translated into business impact by putting the values into relevant context for your organization, such as prioritizing top risk reduction opportunities or calculating a service's return on investment (ROI). Key analysis values of importance often include, but are not limited to:

- Loss magnitude values per event which calculate the potential across primary and secondary loss magnitude values and can be used to obtain annualized loss exposure;
- Annualized loss exposure which takes the "per event" cost and multiplies it by the number of loss events expected in a year to provide an estimated yearly cost or investment for future needs; and
- Vulnerability or "susceptibility" to assess how likely a threat event (or attempted attack) will be successful and become a loss event.

Translating cyber risk into business risk can overcome communication challenges within an organization, particularly when relaying risk priorities to leadership. Specifically, quantitative analysis results can support communication of risk in financial terms to provide recommendations in response to questions such as:

- How much risk do we have?

- Are we spending our budget the right way?
- What is the cost benefit or ROI of this project or service?
- Have we reduced risk?
- How is risk trending versus appetite?
- What are our top forms of loss?
- What are our top risks? Are we addressing high priority issues?

Recommendations backed by quantified assessment results carry more weight than traditional speculative qualitative methods by assigning dollar values to business priorities. These quantitative recommendations recognize that compliance does not guarantee effective cybersecurity practices, challenge current security patterns that may no longer match the IT landscape, and limit the negative impacts from unnecessary security controls. Collecting meaningful measurements can inform effective comparisons, ultimately leading to well-informed decisions around appropriate risk response strategies.

Risk response strategies align with the following definitions:

- **Acceptance:** Recognizes an identified risk and acknowledges that the potential loss does not exceed the organization’s tolerance. Acceptance of the risk does not mean that the risk is ignored
- **Mitigation:** Reduces the likelihood of occurrence and / or impact of an identified negative risk or threat to an acceptable level
- **Avoidance:** Plans activities or rejects an approach to eliminate a risk. Avoidance strategies often involve a change in requirements, specifications, or practices to eliminate the risk
- **Transfer / Share:** Transfers the service, operation, or control associated with the specific risk to another project or Program Office

Acceptable risk response strategies consider the probability and magnitude of a risk, as well as an organization’s risk acceptance.

4.1.4.1 Risk Register

The risk register is a tool for documenting an organization’s most pertinent risks and prioritizing actions to manage each risk. The risk register is essential to the successful management of risk, and a critical foundational step to align National Laboratories’, Sites’, and Program Offices’ priority areas of risk. Per DOE O 205.1C, a risk register process must be established to include annual submission of a risk register by each Departmental Element. Updates to risk register submissions must be completed quarterly to support enterprise-wide cybersecurity awareness and visibility into changing operational conditions, priorities, and programmatic capabilities.

At the National Laboratory, Site, and Program Office level, the risk register functions as a tactical compilation of risks across the program.

The Risk Register serves as the first step to implementing the CSF's first function, "Identify" and the RMF's first step, "Prepare," to develop an organizational understanding of the cybersecurity risk landscape across systems, people, assets, data, and capabilities.

However, the Methodology recommends risk register inputs to be informed by quantitative analyses. This supports data-driven decision making and consistent prioritization for coordinated action or escalation across the enterprise. The risk register is a key component of the Department's approach to monitor risk over time.

As part of the ECRM program, the Office of Cybersecurity reviews each risk submission and holds working sessions with the stakeholders from Headquarters to identify potential enterprise mitigations of the most common reoccurring risks submitted. Furthermore, the top identified risk themes from the risk register submissions will be used as potential candidates for the ECRM program to conduct quantitative assessments on.

5.0 Program Maturity

The maturity of a National Laboratory, Site, and Program Office's cybersecurity risk management program will dictate the necessary level of effort for their risk assessments. This maturity progression is mapped in Figure 9.

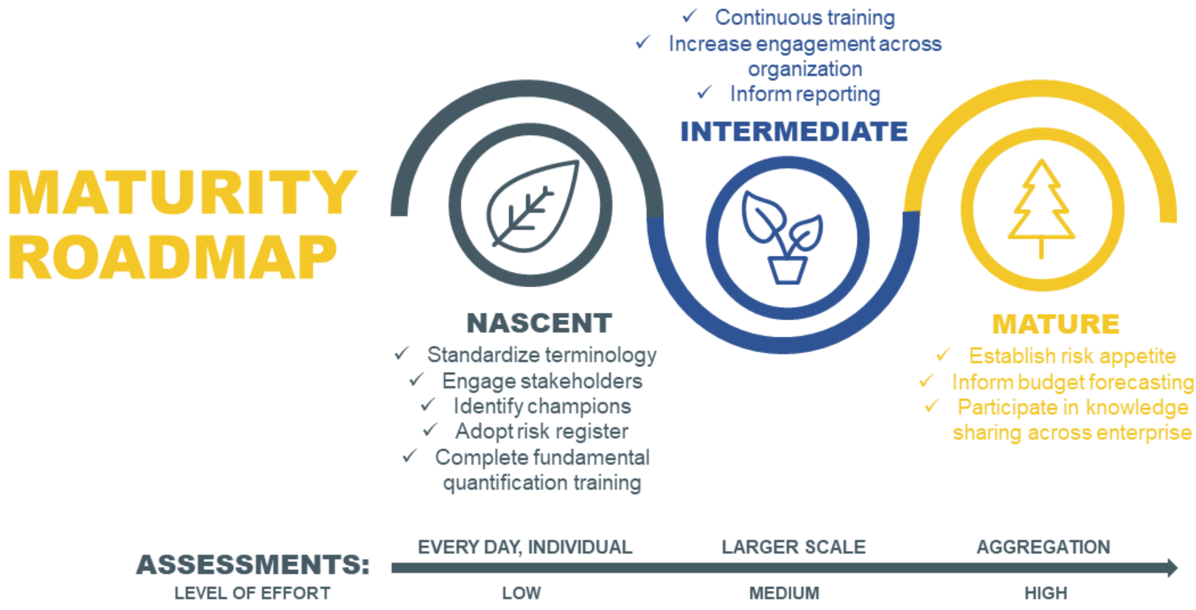


Figure 9 Risk Management Maturity Roadmap

5.1 Assessment Use Cases

As an organization's cybersecurity risk management program matures, the level of effort and complexity of risk analyses will increase. Use cases provided below are for exemplary purposes only.

Low Effort (e.g., individual service valuation, tool cost benefit analysis):

- Cost benefit analysis (CBA) on a personally identifiable information detection service discovered its controls were already provided by an existing service, saving $80k annually, this demonstrated the strength of current controls.
- CBA focused on a risk intelligence service. Analysis demonstrated the service was duplicative with capabilities of another service which featured greater capabilities and features. Subscription costs of $162K can be reinvested in resources and alternative security controls. Analysis revealed no increase in loss exposure with the license cancellation.
- Penetration test flagged a control as "critical." Analysis discovered an exploitation of the control would have minimal impact. As a result, other vulnerabilities were prioritized.

Medium Effort (e.g., investment decision, operational value of system):

- Current and future state analysis of on premise versus cloud-based solution to determine potential increase in risk exposure.
    - Current and future state analysis challenged assumptions of guaranteed security from cloud migration.
    - Determined cloud is not always better; traditional assumptions and trends should be reviewed early and often, there is no one-size-fits-all solution.
- Comparison of three cluster replacement options to inform an investment decision. Analysis showed that the value of the cluster's function was not worth the replacement costs:
    - Balanced investment costs with lifecycle and value of needs;
    - Identified the need to thoroughly scrutinize estimates to quantify the value of services and investment options;
    - Identified accountability and performance criteria to track ROI on investments; and
    - Investment decision showed replacement costs exceeded value of function.

High Effort (e.g., organization-wide, aggregated analyses):

Three-day in-person workshop assessment to evaluate the damage caused by a potential server cluster outage. Inspired by a similar incident at the organization, the assessment revealed not only key controls and processes that substantially lowered the likelihood of the incident, but also exposed gaps in asset valuation, prioritization, and classification processes. The workshop assessment:

- Brought together over 10 offices, exposing interdependencies and knowledge gaps;
- Quantified the cost and value of an asset to the organization and identified a super control that can be applied to additional assets to substantially lower likelihood of an outage;
- Identified the need to re-assess their classification and valuation criteria and perform additional configuration reviews for similar assets; and
- Re-defined “criticality” to consider operations and applications supporting mission-essential functions, not just mission-essential functions themselves.

6.0 DOE Enterprise Cybersecurity Risk Management Program Current State

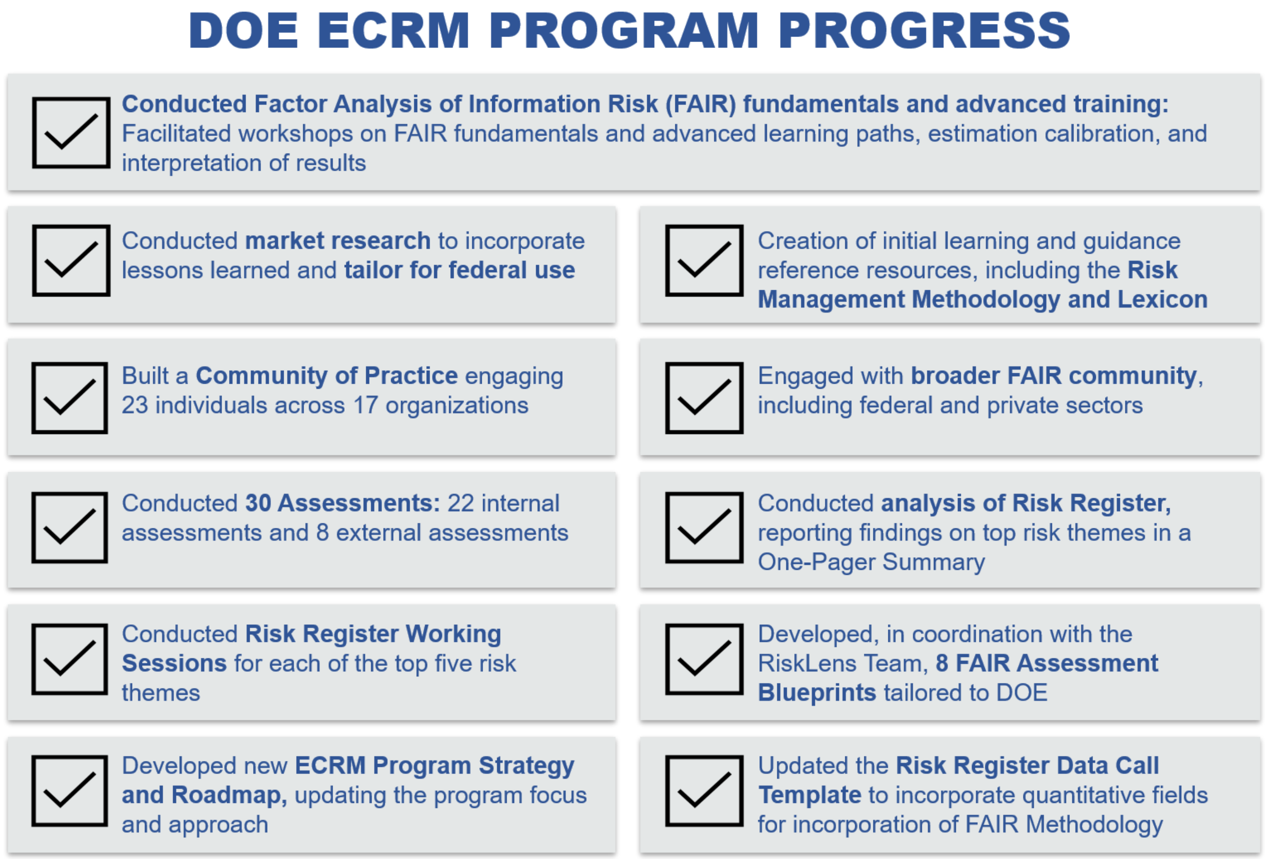
Through its ECRM program, DOE has conducted numerous risk assessments based on this Methodology and shared best practices with cybersecurity risk communities of practice both inside and outside of government.

The ECRM program's initial discovery accomplishments include:

- Engagement in industry-leader methodology and framework research and training to identify best practices, considerations, and guidance for risk management program scaling and adoption;
- Establishment of a Working Group with membership from early adopter and interested National Laboratories, Sites, and Program Offices which continues to expand;
- Execution of initial risk analyses to gain traction and prove upfront value for real-time investment decisions and risk scenario concerns;
- Identification and establishment of best practices for risk assessment based on cursory assessments;
- Creation of initial learning and guidance reference resources, including this Methodology and lexicon; and
- Sharing of lessons learned and continuing challenges across the Department and with external Federal agency counterparts to address common pain points.

6.1 Program Progress

An overview of DOE ECRM program progress as of May 2021 is shown in Figure 10.



DOE ECRM PROGRAM PROGRESS

☑ **Conducted Factor Analysis of Information Risk (FAIR) fundamentals and advanced training:** Facilitated workshops on FAIR fundamentals and advanced learning paths, estimation calibration, and interpretation of results

☑ Conducted **market research** to incorporate lessons learned and **tailor for federal use**

☑ Creation of initial learning and guidance reference resources, including the **Risk Management Methodology and Lexicon**

☑ Built a **Community of Practice** engaging 23 individuals across 17 organizations

☑ Engaged with **broader FAIR community**, including federal and private sectors

☑ Conducted **30 Assessments:** 22 internal assessments and 8 external assessments

☑ Conducted **analysis of Risk Register,** reporting findings on top risk themes in a One-Pager Summary

☑ Conducted **Risk Register Working Sessions** for each of the top five risk themes

☑ Developed, in coordination with the RiskLens Team, **8 FAIR Assessment Blueprints** tailored to DOE

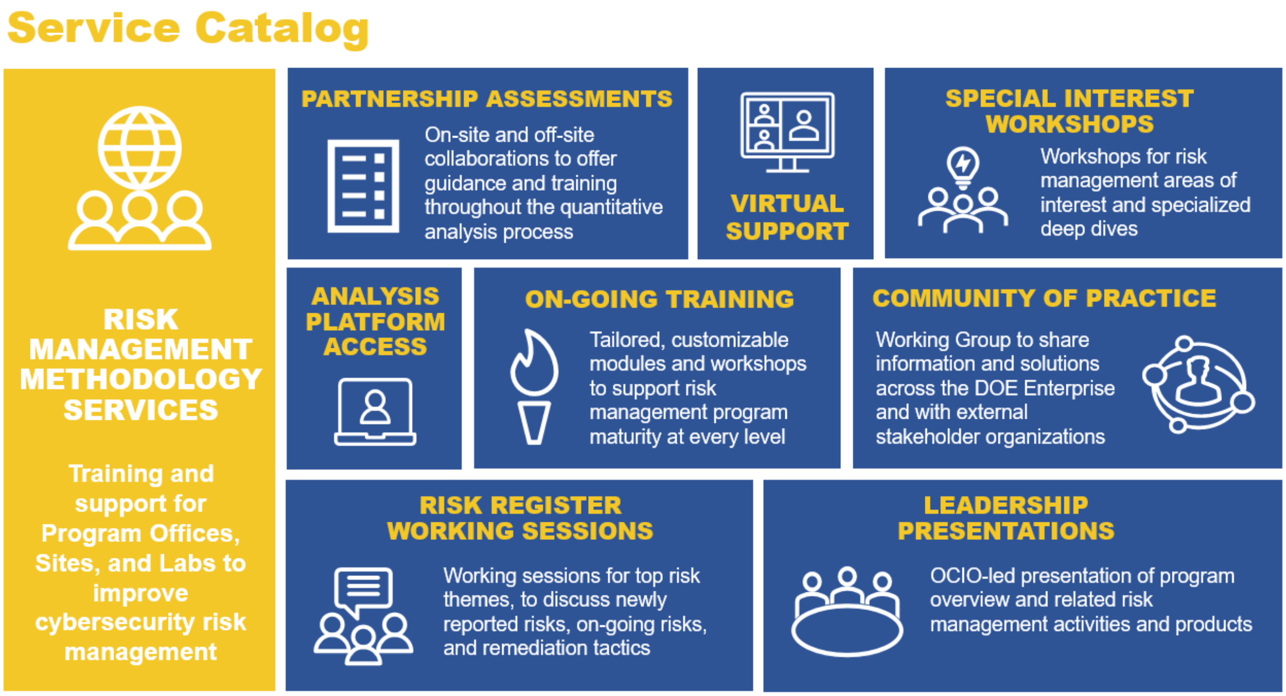
☑ Developed new **ECRM Program Strategy and Roadmap,** updating the program focus and approach

☑ Updated the **Risk Register Data Call Template** to incorporate quantitative fields for incorporation of FAIR Methodology

Figure 10 DOE ECRM Program Progress

6.2 Services Offered

To support the adoption of a cybersecurity risk management methodology at each level of maturity, the Office of the Chief Information Officer (OCIO) offers a menu of services. Services are as of May 2021 and can be used as stand-alone offerings or as a suite, as shown in Figure 11.



Service Catalog

RISK MANAGEMENT METHODOLOGY SERVICES

Training and support for Program Offices, Sites, and Labs to improve cybersecurity risk management

PARTNERSHIP ASSESSMENTS

On-site and off-site collaborations to offer guidance and training throughout the quantitative analysis process

VIRTUAL SUPPORT

SPECIAL INTEREST WORKSHOPS

Workshops for risk management areas of interest and specialized deep dives

ANALYSIS PLATFORM ACCESS

ON-GOING TRAINING

Tailored, customizable modules and workshops to support risk management program maturity at every level

COMMUNITY OF PRACTICE

Working Group to share information and solutions across the DOE Enterprise and with external stakeholder organizations

RISK REGISTER WORKING SESSIONS

Working sessions for top risk themes, to discuss newly reported risks, on-going risks, and remediation tactics

LEADERSHIP PRESENTATIONS

OCIO-led presentation of program overview and related risk management activities and products

Figure 11 Risk Management Methodology Service Catalog

The following Figure displays the Service, Description, and Maturity Level offered by the Office of the Chief Information Officer (OCIO). Services shown are up to date as of May 2021.

Service	Description	Maturity Level
Analysis Platform Access	Access to RiskLens analytic platform to conduct Risk Assessments	All levels
Community of Practice	Working group established to share information and solutions across the DOE Enterprise and with external stakeholder organizations	All levels

Service	Description	Maturity Level
Partnership Assessments	On-site and off-site collaborations to offer guidance and training throughout the quantitative analysis process	Intermediate
Leadership Presentations	OCIO-led presentation of ECRM Program overview and related risk management activities and products	Intermediate/Mature
Risk Register Working Sessions	Working sessions for top risk themes, to discuss newly reported risks, on-going risks, and remediation tactics	Ongoing
Special Interest Workshops	Workshops designed around risk management common areas of interest and specialized deep dives	Mature
On-going Training	Tailored, customizable modules and workshops to support risk management program maturity at every level	All levels
Virtual Support	Remote assessment sessions to guide you through analyses	Nascent/Intermediate

Appendix A. Key Terms and Definitions

Key Term	Definition
Advanced Persistent Threat (APT)	A group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific IT system or network.
Asset	Device, process, software, person, information, material, or process that has value.
Attack Chain	The steps that lead to loss; the steps a threat actor must take to cause the desired effect on the asset
Bayesian Probability	The process of evaluating the probability of a hypothesis through 1) the specification of a prior probability and 2) modification of the prior probability by incorporation of observed information to create an updated posterior probability.
Consequence	The resulting effects of a cyber event with some measurable severity.
Categories	The subdivisions of a NIST CSF Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”
Contact Frequency	Over the next year, how many times will the threat come into contact with the asset to the extent needed to launch a threat action?
Control	Any measure or action that modifies or regulates risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk. Risk treatments become controls, or modify existing controls once they are implemented.
Cyber Criminal	Threat actors who leverage IT systems to perform malicious activities for financial, political, or other motives. Examples of activities might include: spreading viruses, data theft, identity theft, or extortion.
Cyber Event	The result of any single unauthorized effort, or the culmination of many such technical actions, that engineers, through use of computer technology and networks, a desired primary effect on a target. The event can be further classified into disruptive events or exploitive events.
Cybersecurity	The organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems.

Key Term	Definition
Factor Analysis of Information Risk (FAIR) Methodology	A methodology for quantitative analysis of risk that produces results in financial terms, enabling cost-effective management of risk across the enterprise
Functions	Organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.
Informative References	Specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.
Inherent Risk	The current risk level given the existing set of controls rather than the hypothetical notion of an absence of any controls.
Loss Event Frequency	Over the next year, the number of loss events an organization will face.
Loss Event Magnitude	The cumulative effect of a loss event on an organization.
Monte Carlo	A statistical simulation technique used to understand the impact of risk and uncertainty in financial, project management, cost, and other forecasting models.
Primary Effect	The direct impacts to the target organization’s data or IT-enabled operations engineered by the threat actor on the specific target organization and IT systems.
Probability of Action	The percentage of contact events that will turn into threat events.
Residual Risk	Whatever risk remains after additional controls are added.
Resistance Strength	On a scale between 0-1, the measure of strength of a Threat Actor.
Risk	Forecasted annualized losses based on estimates of loss, event frequency, and loss magnitude.
Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Key Term	Definition
RiskLens Platform	Analytic platform that leverages the FAIR Methodology to conduct risk assessments and provide quantitative measures of risks in financial terms
Risk Management Methodology	Amplification guidance to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.
Risk Management Methodology Process	A formally approved set of policies and guidance expressed as department policy.
Risk Management Methodology Program	Organization-wide approach to manage cybersecurity risk. This includes processes, policies, and procedures. Includes consistent methods of assessing and managing changing risk, as well as informed staff who possess the knowledge of how to measure and communicate those changes.
Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions that are established and used to support operational risk decisions.
Risk Register	A tool for documenting risks and actions to manage each risk. The risk register is essential to the successful management of risk. As risks are identified they are logged into the risk register and actions are taken.
Second Order Effect	Impacts that reach beyond the targeted organization to generate effects on the physical environment, the supply chain, or even distortions an attack might have on an individual's attitudes, preferences, or opinion deriving from the release of salacious information.
Secondary Effect	Financial impacts to the targeted organization derived from the primary effect on the organization's IT systems. Impacts might include financial costs of replacing equipment damaged in an attack, or remediation and response costs incurred from the attack. Measured in dollars.
Secondary Effect Frequency	The percentage of loss events that lead to a secondary effect.
Secondary Effect Magnitude	The dollar loss associated with a secondary effect.
Severity	The quantifiable measurement of impact a cyber incident imbues on an asset, mission, or business function.

Key Term	Definition
Susceptibility	The percentage of threat events that will be successful in producing losses over the next year.
Threat Actor	An entity that is partially or wholly responsible for an incident that impacts, or has the potential to impact, an organization’s IT systems.
Threat Capability	Measured on a spectrum between 0-1; this is the value of capability a specific threat actor maintains.
Threat Event Frequency	The number of times in the next year that threat actors will attempt to cause loss to the asset.

Appendix B. Terms and Acronyms

Acronym	Description
AO	Authorizing Official
CBA	Cost Benefit Analysis
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
DOE	The Department of Energy
ECRM	Enterprise Cybersecurity Risk Management
EO	Executive Order
FAIR	Factor Analysis of Information Risk
FISMA	Federal Information Security Modernization Act
FITARA	The Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
O	Order
OCIO	Office of the Chief Information Officer
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
ROI	Return on Investment
SME	Subject Matter Expert
SP	Special Publication