Carnegie Mellon University
Software Engineering Institute

Advancing Risk Management Capability Using the OCTAVE FORTE Process

B. A. Tucker

November 2020

TECHNICAL NOTE
CMU/SEI-2020-TN-002
DOI: 10.1184/R1/13014266

CERT® Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM20-0634

Table of Contents

List of Figures

List of Tables

Acknowledgments

There are so many mentors, leaders, and managers that I have spoken with over the course of this journey; there is no possible way that I can properly acknowledge all of them. If I have not mentioned you by name in these remarks, you are certainly there in spirit. Thanks to Summer Fowler and Matthew Butkovic for their leadership and direction. Thanks to Alan Levine for his sage advice. Thanks to the members of my team for their comments and feedback. Thanks to Jeremiah Clifton for giving OCTAVE FORTE the application challenges it needed to "sprout legs." Thanks to Sandy Shrum and Barbara White for their gracious help in making this a better product. Finally, thanks to my family for their support throughout this journey; the sleepless nights were worth it.

Abstract

OCTAVE FORTE (Operationally Critical Threat, Asset, and Vulnerability Evaluation **FOR T**he **E**nterprise) is a process model that helps executives and other decision makers understand and prioritize the complex risks affecting their organization. It also helps organizations identify, analyze, prioritize, and mitigate risks that could impact them.

The Software Engineering Institute (SEI) developed the OCTAVE FORTE process model to help organizations evaluate their security risks and use ERM principles to bridge the gap between executives and practitioners as decision makers. *Executives* use information about risk to develop a governance structure, prioritize risks, make informed decisions, allocate resources, and communicate risks using a tiered governance structure. *Managers*—who support executives in achieving strategic objectives—use elements of FORTE to identify and manage risk in their divisions and departments. *Practitioners* learn to apply their subject matter expertise in a way that enhances their analysis and helps them communicate their greatest concerns to management.

The process model guides organizations that are new to risk management in building an ERM program, and it helps mature organizations fortify their existing ERM program, making it more reliable, measurable, consistent, and repeatable.

Besides describing the OCTAVE FORTE process, this report recommends methods and provides a sample risk management policy that organizations can refer to or adapt when writing their own policy. Supplemental materials (available on the SEI website at https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=644636) contain templates that organizations can use when conducting many of the OCTAVE FORTE activities.

1 Introduction

Uncertainty affects how organizations operate and meet their strategic objectives. A fast-paced, uncertain environment creates risks and can preclude organizations from making long-term plans because these plans can quickly be rendered obsolete.

To cope with this situation, organizations should focus on managing their risks and using risk data to make decisions that help them meet their strategic objectives. Since *risk* is another word for *uncertainty*, an organizational focus on understanding risk makes sense. When an organization manages risk, it ensures that it takes only the risks—in the form of opportunities—that help it achieve its strategic objectives while controlling the risks that threaten those objectives.

1.1 How Risk Challenges Organizations

When risks are realized in an organization, business continuity can be disrupted, potentially affecting the organization's critical assets and bringing the organization's critical services to a halt.

Executives are responsible for guiding their organization, steering it toward achieving strategic objectives while avoiding obstacles in its way and protecting its assets. Executives recognize the benefits of making informed decisions that account for the risks the organization faces. They have an enterprise view of the organization that includes the perspectives of its divisions and departments, and often find themselves asking challenging questions like the following:

- How do I choose the right risk-informed options for the organization and its stakeholders?
- How do I identify, analyze, and react to uncertainty?
- How do I know I'm using the right analytic techniques and tools?
- Even if I use the right tools, how do I know they are pointing me in the right direction?
- How do I measure the effectiveness of my risk-based decision making?
- How do I manage enterprise risk?
- How do I demonstrate the value of risk management?
- How do I illustrate the effectiveness of my organization's risk management program?

An organization cannot anticipate every possible disruption that might affect it. However, it can anticipate and respond to changes in its risk environment and create a plan for how to respond to the risks as they are realized. These challenges make it difficult to approach managing risk effectively across the organization.

Regardless of the nature of an organization's business, having a well-considered understanding of its risks weighed against potential rewards provides valuable input to making decisions, especially strategic decisions. For an organization to survive, and even thrive, its approach to managing risk must be comprehensive and integrated throughout the organization.

1.2 Enterprise Risk Management (ERM)

Risks that present threats or opportunities related to achieving the organization's strategic objectives, or that are related to the organization's overall health, are called *enterprise risks*. Enterprise risks can be interdependent, creating cascading effects across the organization. In other words, one realized risk may drive other risks to also come to fruition, thus amplifying or adding to their impacts.

An organization that identifies and manages its enterprise risks before they become issues has a distinct advantage over organizations that can't. Such an organization has a business advantage over its competitors because its executives understand and track its assets and the associated risks, they understand how much risk it can tolerate, and they know how to deal with those risks when they begin to be realized. Poor risk management increases the organization's exposure to disruptive conditions—it weakens the organization's ability to respond and makes it less resilient.

To manage enterprise risks, an organization must establish and operate an effective *enterprise risk management (ERM)* program that identifies, analyzes, and mitigates risks that could impact the organization. To guide the ERM program, the organization's leadership must establish a comprehensive scope for its operation, define priorities based on the organization's resources, and require that the processes developed by the program are broadly applicable and easy to implement.

MAKE THE CASE WITH LEADERSHIP

When trying to convince leadership to create an ERM program and devote resources to it, it's helpful to identify the organization's challenges and map them to ERM solutions. See page 63 for a sample that maps challenges to solutions.

An organization that has a real-time view of risks as well as suitable tools and processes is well positioned to confidently manage risks. When managing enterprise risk, executives benefit from using techniques, tools, data, and methods that

- acknowledge and eliminate bias by providing data
- provide an objective comparison of options for responding to risks
- deliver a consistent service to stakeholders
- evolve with the latest best practices so that the organization can identify new threats and opportunities, and address them quickly and efficiently

1.3 OCTAVE FORTE

To manage enterprise risks, the Software Engineering Institute (SEI) developed a process model called OCTAVE FORTE (**FOR T**he **E**nterprise). OCTAVE FORTE helps executives understand and prioritize the complex risks affecting their organization. It also helps risk managers develop a compelling business case for securing the resources needed to develop, improve, and operate the organization's ERM program.

RECALL THE TRADITIONAL APPROACH

Traditional risk management focused on estimating the likelihood of an event happening and what its impact might be (e.g., monetary value). However, this approach doesn't account for factors such as risk interdependencies, rates of occurrence, vulnerabilities, and the threat environment. These factors are especially important when risks extend beyond individual projects to the organization level.

The remainder of this report is organized into the following sections:

- **Section 2** provides an overview of OCTAVE FORTE.
- **Section 3** describes the 10 steps of OCTAVE FORTE in detail and how the organization can use them to manage enterprise risk.
- **Appendix A** describes common risk concepts; those who are new to risk management should become familiar with these concepts before reading Sections 2 and 3.
- **Appendix B** describes samples of techniques and methods that can be used when implementing OCTAVE FORTE; this report's supplemental materials[1] contain templates to simplify creating many OCTAVE FORTE artifacts.
- **Appendix C** contains a sample risk management policy; this report's supplemental materials contain a risk management policy template that organizations can adapt to form their own policy.

Visual Cues

This document uses sidebars that contain information that can be useful to organizations adopting OCTAVE FORTE. Each sidebar has an icon that identifies the type of information it provides:


example


more information


technique


tip or idea

[1] This report's supplemental materials are available on the SEI website at https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=644636.

2 OCTAVE FORTE Overview

To ensure that risk management is effective, organizations need adaptable, agile frameworks that provide executives with a real-time view of cyber risks, and the related tools and processes they can use to address appropriate risks. Organizations should use ERM principles, tools, and processes to understand and prioritize complex risks that compete for organizational resources.

The SEI developed OCTAVE FORTE, a process model that helps organizations (1) evaluate their security risks and (2) use ERM principles to bridge the gap between executives and practitioners. OCTAVE FORTE helps organizations new to risk management (i.e., *nascent organizations*) and organizations already familiar with risk management (i.e., *mature organizations*). OCTAVE FORTE guides a nascent organization as it builds an ERM program while its techniques and framework help a mature organization fortify its existing ERM program, making it more reliable, measurable, consistent, and repeatable.

OCTAVE FORTE[2] identifies processes that support the achievement of strategic objectives, including ways to help executives and practitioners effectively communicate threats and opportunities across the organization that relate to those objectives. It helps organizations establish an ERM framework that scales to the organization's size and strategy with limited overhead.

2.1 A 10-Step Process

FORTE's 10 steps help an organization achieve the following:

- understand its assets, capabilities, and risks
- form risk appetite statement(s) to document its risk tolerance
- create response plans to manage risks
- form processes to monitor whether risk is being managed effectively
- develop a plan to improve the organization's ERM program

Figure 1 depicts a high-level view of FORTE's 10 steps. Each step is discussed in detail in Section 3.

[2] From this point forward, *OCTAVE FORTE* is referred to simply as *FORTE*.

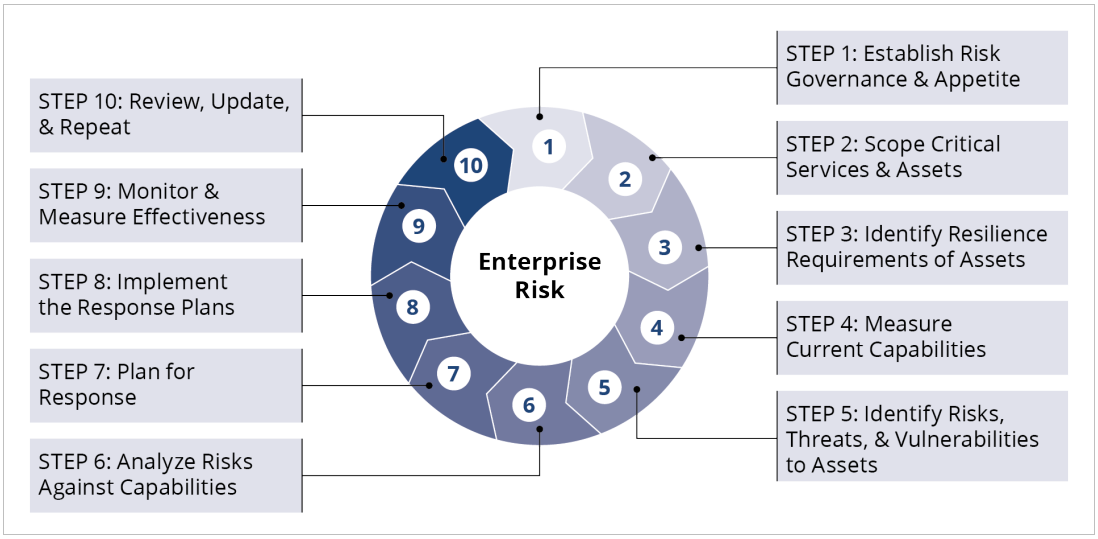


Figure 1: Steps in the FORTE Process

2.2 Standards

FORTE uses a process that is based (in part) on standards published by the Committee of Sponsoring Organizations (COSO), the International Standards Organization (ISO), and the National Institute of Standards and Technology (NIST) while adhering to the fundamental principles of the CERT Resilience Management Model (CERT-RMM) and the Factor Analysis of Information Risk (FAIR) framework.

COSO Framework. In alignment with COSO, FORTE is governance focused and links the organization's risk strategy to its day-to-day activities. The COSO framework advises organizations to create risk appetite statements, and create and manage a portfolio of risk for the organization. It advocates that organizations build risk considerations into their vision, mission, goals, and values. When choosing strategies, COSO recommends considering all possible outcomes to determine if they align with the organization's risk appetite and vision [COSO 2017].

ISO 31000 Framework. ISO 31000 is a risk management framework that provides principles, a framework, and a process for managing risk. It can be used by any organization regardless of its size, activity, or sector. It was not developed for a particular industry group, management system, or subject matter; it provides a best practice structure and guidance to all operations concerned with risk management [Tranchard 2015]. Like FORTE, ISO 31000 provides strategic guidance and emphasizes how important it is for organizations to involve their executives in risk management and integrate risk management concepts throughout the organization.

NIST CSF. FORTE considers principles outlined in the NIST Cybersecurity Framework (CSF), a framework that is broadly applicable and advocates for community consensus. FORTE overlays the CSF principles of identify, project, detect, respond, and recover [NIST 2018].

NIST SP 800-39. The NIST publication *Managing Information Security Risk: Organization, Mission, and Information System View* describes a three-tiered approach to addressing risk across an organization [NIST 2011]. FORTE embraces this approach, especially by recognizing that the highest tier of the governance structure should focus on strategic risk, while the lower tiers should focus more on tactical risk.

NIST SP 800-37. The NIST publication *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* describes how to use the Risk Management Framework (RMF) to manage assets and risks throughout the asset's lifecycle [NIST 2018]. Specifically, the RMF provides a process that categorizes risks and guides the user through the selection, implementation and monitoring of controls related to the risks.

CERT-RMM. The SEI's CERT-RMM defines essential practices that are necessary for organizations to manage operational resilience. Organizations can use CERT-RMM to determine their capability to manage resilience, set goals and targets, and develop plans to close identified gaps. By using a process view, CERT-RMM can help organizations respond to stress with mature and predictable performance [Caralli 2011].[3]

Factor Analysis of Information Risk (FAIR). People quantify risk with different degrees of accuracy and confidence. The FAIR cyber risk framework, designed for cybersecurity and operational risk, helps people understand their ability to estimate values to improve quantitative risk analysis. In FAIR, risk owners estimate data about trivial items and assign a degree of confidence to each answer. Analytics are then used to show how each individual (or each group) can be overly confident in their estimates [Jones 2014].

[3] In 2016, the SEI updated CERT-RMM; the newer version (v1.2) provides the model's process areas, generic goals and practices, a glossary, and acronyms [SEI 2016].

2.3 A Holistic Approach

FORTE addresses all forms of risk with a holistic approach that enables an organization to analyze and manage all risks within its risk portfolio. FORTE also helps an organization establish a robust framework for ERM by providing a feedback loop to complete the risk management lifecycle.

SEE THE CONNECTION TO OCTAVE ALLEGRO

OCTAVE Allegro and OCTAVE FORTE complement each other; Allegro is part of the greater process defined by FORTE.

The SEI recommends that organizations continue to use OCTAVE Allegro and urges risk managers to use the strategic processes that FORTE provides in tandem with Allegro-based work products, including a way to communicate risk to executives.

FORTE benefits all levels of the organization. *Executives* use information about risk to develop a governance structure, prioritize risks, make informed decisions, allocate resources, and communicate risks using a tiered governance structure. *Managers*—including chief information security officers (CISOs), risk managers, and other organizational leaders in both private and public sectors—use elements of FORTE to identify and manage risk in their divisions and departments. *Practitioners* learn to apply their subject matter expertise in a way that enhances their analysis and helps them communicate their greatest concerns to management.[4]

2.4 The Business Case for OCTAVE FORTE

An organization that adopts FORTE improves its ability to meet its objectives and protect itself from threats. As an ultimate goal, organizations that manage their risks gain confidence in their ability to achieve their strategic goals despite the unpredictability of most threats. Furthermore, business partners and customers are more confident working with organizations that have a strong risk culture and a proven ability to incorporate risk management into their business processes. With FORTE, the organization can accomplish the following:

- Implement ERM using an easy-to-follow framework that helps the organization complete risk management activities and measure their effectiveness.
- Establish an ongoing and improving risk management process.
- Establish a governance structure, including policies and procedures, to ensure the ERM program's longevity and consistency.
- Develop a risk appetite statement that executives can use to make decisions.
- Maintain awareness and keep pace with the changing environment as it presents new opportunities, vulnerabilities, and threats.
- Prioritize risks to focus on those that threaten the organization most.
- Identify and respond to interdependent risks, which can have far-reaching consequences.

---

[4] This report focuses on the actions taken by risk managers and executives. The title *risk manager* is a generic placeholder for those in the organization who are responsible for the ERM program and implementing OCTAVE FORTE. Actual titles may vary because roles and role labels differ in different organizations.

- Allocate resources to support the ERM program more strategically.
- Find risks that might otherwise remain hidden.

Ultimately, an organization that adopts FORTE is able to not only manage risk, but it will use risk to its advantage. It will outpace its competitors that do not use an ERM approach, and it will be positioned to leverage the positive aspects of risk.

3 OCTAVE FORTE Process

This section discusses FORTE's 10 steps in detail. In each step, this image highlights the particular step described and a question for organizations to consider to set the context.

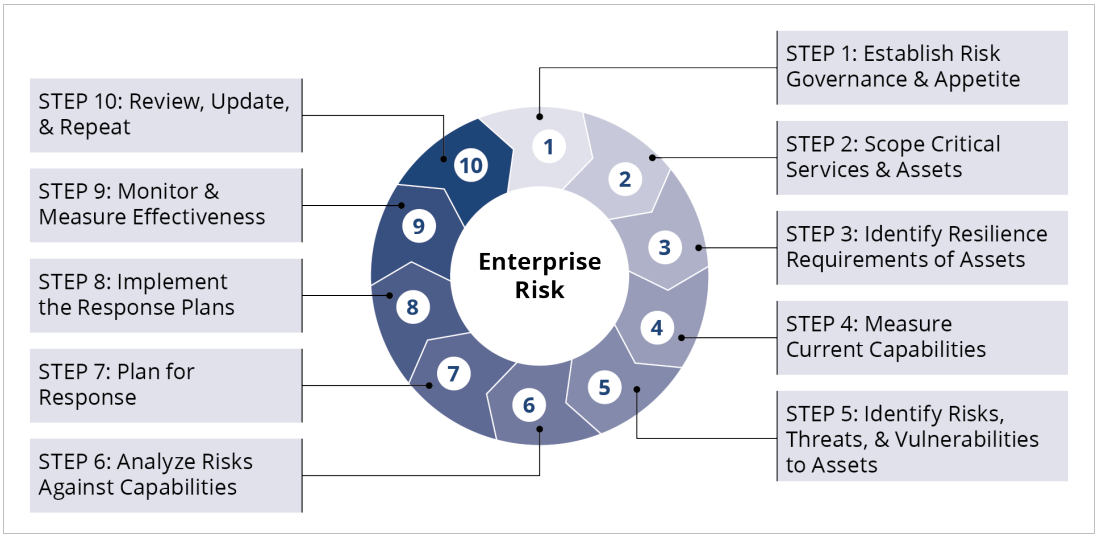


Figure 2: Steps to be Followed in the OCTAVE FORTE Process

3.1 Step 1—Establish Risk Governance & Appetite

In Step 1, Establish Risk Governance & Appetite, the organization asks itself, "How do I begin?" In this step, the organization establishes a governance structure (Section 3.1.1), determines how much risk it's willing to tolerate (Section 3.1.2), and sets policies for how it manages risk (Section 3.1.3).

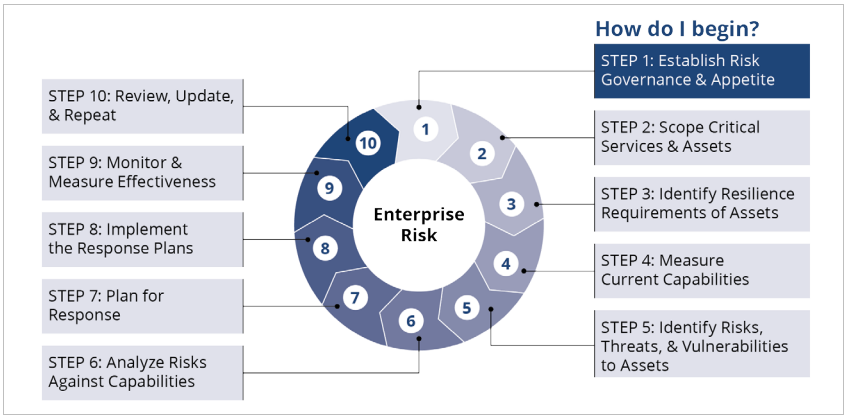


Figure 3: Step 1—Establish Risk Governance & Appetite

3.1.1 Establish a Governance Structure

The organization must establish a governance structure for its ERM program. Since FORTE is designed for the entire organization, the ERM governance structure[5] should have guidance about roles, responsibilities, policies, resources, and information flow.

Risk governance can be thought of in different ways. For example, NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, describes a three-tiered approach to addressing risk across an organization [NIST 2011]:[6]

- Tier 1 addresses risk at the *organizational level* by establishing and implementing governance structures that are consistent with the strategic goals and objectives of organizations and the requirements defined by federal laws, directives, policies, regulations, standards, and missions/business functions.
- Tier 2 addresses risk from a *mission/business process perspective* by designing, developing, and implementing mission/business processes that support the missions/business functions defined at Tier 1.
- Tier 3 addresses risk from an *information system* perspective. In addition to the risk management activities carried out at Tier 1 and Tier 2, risk management activities are also integrated into the system development lifecycle of organizational information systems at Tier 3. The risk management activities at Tier 3 reflect the organization's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual information systems supporting the mission/business functions of organizations.

FORTE embraces this three-tiered approach, especially by recognizing that Tier 1 should focus on strategic risk, while Tiers 2 and 3 should focus on more tactical risk.

Similar to the tiers in NIST SP 800-39, most organizations should establish risk management roles, responsibility, and authority at each level. However, not all organizations benefit from focusing on information systems only at Tier 3. Rather, the tiers may need to be recast to accommodate the organization's nature and scope.

Figure 4 represents a three-tier structure based on NIST SP 800-39. The FORTE governance structure interprets the tiers in this standard to serve a broader set of stakeholders in any organization.

GET A SAMPLE GOVERNANCE GRAPHIC

See page 72 for a sample governance structure graphic. This report's supplemental materials also contain a template that organizations can use when devising a governance structure.

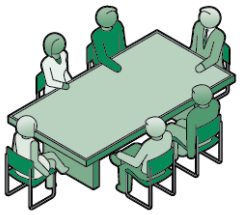
[5] See Appendix A on page 49 for more information about risk governance.

[6] Tier descriptions are excerpted from *Managing Information Security Risk: Organization, Mission, and Information System View* [NIST 2011].

An organization can customize each tier in Figure 4 to match its hierarchy of management and decision makers. Each tier represents a layer of the risk management function that has the authority to make decisions and leverage resources to implement those decisions.

Boards, Committees, and Subcommittees

The organization should create governance boards, committees, and subcommittees that reflect the needs of the organization and support the ERM governance structure. In Figure 4, the tiers that comprise the governance structure are labeled *Executive Board*, *Risk Committee*, and *Risk Subcommittee(s)*; regardless of the label used, each tier must consist of one or more decision-making bodies that weigh risk-based decisions.

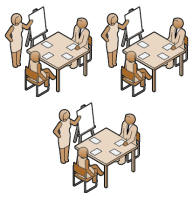


Tier 1: Executive Board

- Roles: senior executives (a subset of the executive board in a private organization; advisory board for a non-profit; or a group of senior executive/appointees in a public organization)
- Responsibilities: sets strategic direction; approves policy
- Authority: institutes authority into the governance structure

Tier 2: Risk Committee

- Roles: executive leaders from across the organization (e.g., chief financial officer, CISO, and chief operations officer)
- Responsibilities: sets policy and procedure; partners with the audit team
- Authority: provides advocacy and resources, such as money



Tier 3: Risk Subcommittee(s)

- Roles: high-performing managers
- Responsibilities: enforces policy; oversees processes
- Authority: oversees risk response plans implementation and risk management performance; advises on technical aspects of specific risks; is chartered based on the organization's functions or locations

Figure 4: Governance Structure for an ERM Program

All committees and subcommittees should operate according to a documented and a board-approved charter, which they review and update periodically. The charter establishes the authority of committees and subcommittees and provides direction for all governance members. A charter should describe procedures, such as how to appoint meeting scribes, determine a quorum, administer voting, and require appropriate training for participation.

A board, committee, or subcommittee can be designated to execute or direct the execution of tasks such as the following:[7]

- Approve the organization's risk management policy.
- Advocate implementing the risk management policy.
- Set the expectations of employees and require that they follow the organization's risk management policy to support the risk culture.[8]
- Ensure response plans are implemented properly and are effective.
- Make critical ERM-related decisions and oversee their implementation.
- Assign risk owners when necessary.
- Prioritize resources for analyzing and responding to risks.
- Periodically review ERM artifacts (e.g., asset catalogs, risk registers, risk appetite statements) to ensure that they are analyzed appropriately.
- Allocate resources to support the ERM program.
- Oversee and ensure that proper training about risk policies and procedures is available throughout the organization.
- Ensure the risk improvement plan is effective.

WRITE A RISK MANAGEMENT POLICY

A *risk management policy* outlines the organization's approach to risk, such as the scope of the ERM program, the business case for the program, the procedures needed to implement the program, and the roles required to support the program.

Members of the governance structure's decision-making bodies must communicate freely and provide direction to the organization. The Executive Board must communicate to the committees and subcommittees about the organization's risk policies, procedures, decisions, etc. Committees and subcommittees must communicate to the Executive Board about identified risks, feedback on the ERM program, lessons learned, and metrics. Figure 5 depicts this information flow.

---

[7] This list is not comprehensive, and the duties may vary from one organization to another based on the organization's size, scope, or culture. In accomplishing these tasks, it may help if committee members consult with stakeholders.

[8] See page 51 for more information about risk culture.

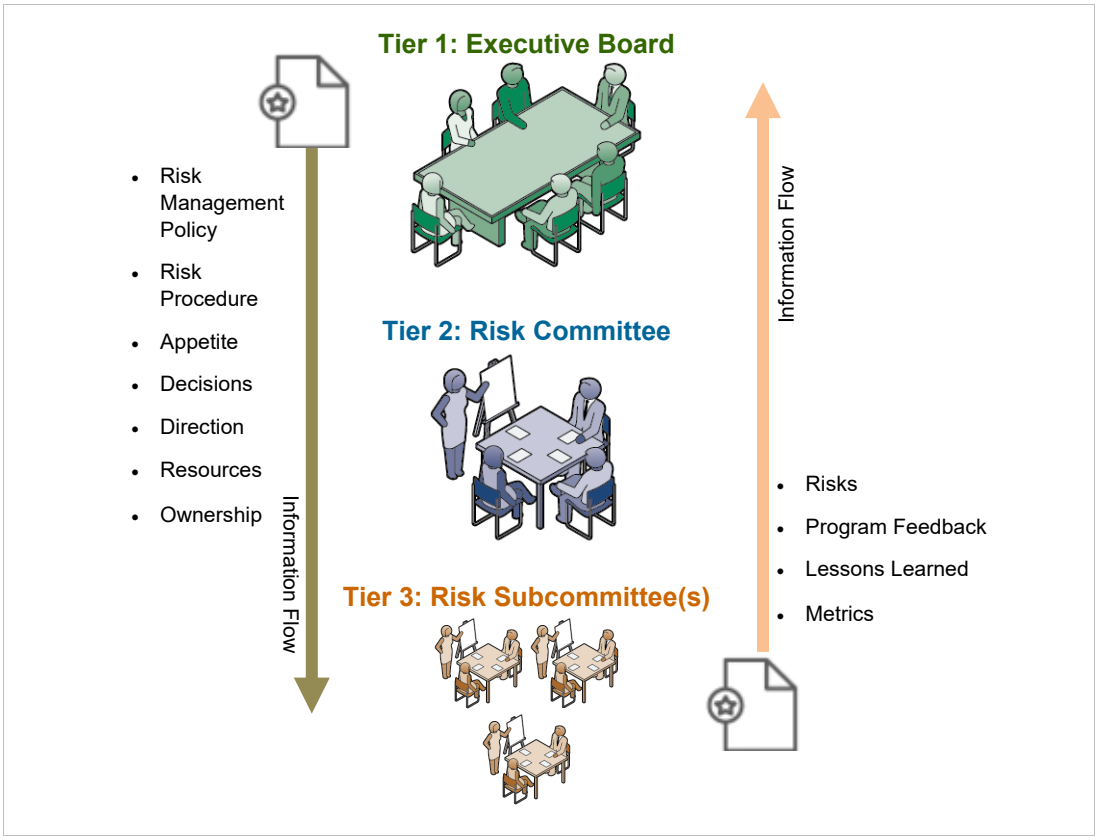


Figure 5: Information Flow Within the Risk Governance Structure

The Role of the Risk Manager

The organization appoints a risk manager or other professional as the central figure in any ERM program. That manager must be involved in developing the organization's strategic objectives. While each organization can vary in the process it uses to build its strategic objectives, the risk manager must fully understand that process and identify critical points where risk management practices can be applied.

The risk manager must understand how to interpret the organization's strategic objectives and support them by (1) advising executives about when they are taking too much risk and (2) limiting drivers that compel executives to take more risk than needed.

Mind the "Tripwires"

Risk managers must also establish "tripwires"—events that signal the need to review and update critical documents (e.g., risk appetite statement, asset catalog, risk management policy, charters, response plans, risk registers, and improvement plans). Examples of "tripwires" include the following:

- changes in committee leadership (Executives come and go; as talent shifts in an organization, the charters may need to shift as well.)
- changes in organizational policies (Some risk management policies depend on other policies; changes to those policies might require changes in risk-related documents.)
- changes to the organization's strategy and strategic objectives (The organization's strategic objectives are strongly linked to its risk policy; therefore, if these objectives or the processes related to them change, the risk policy may need to be adjusted.)
- changes in the sector or industry (New laws being enacted, countries changing policies, new expectations of compliance being mandated are events that should compel the organization to review and update its risk appetite statement and risk management policy.)
- shifts in technology (As technology shifts, risks change, and a process to analyze and understand those shifts may need to change; the organization's appetite for pursuing those technologies may shift as well. These shifts should also trigger a review of the organization's risk appetite statement and other risk-related documents and policies.)
- changes in organizational structure (Mergers and acquisitions are very disruptive to organizations. Risk management, as it relates to significant changes in organizational structure or policy, should focus on the enterprise and identify the interdependency of risks. As the organization adjusts to a merger or acquisition, it should review its risk registers, policy, risk appetites, and procedures.)

Risk managers monitor additional "tripwires" that indicate that risk response plans—plans made to respond to threats or enhance opportunities—need to be revised:

- plan failure (If the planned action isn't working, it may need to be abandoned or changed.)
- cost overruns (The plan may become too expensive. If there is no return on the risk investment, the response plan may need to be updated or abandoned.)
- technology changes (Changes in technology may occur when a solution is overcome by a better solution before the response plan is fully implemented.)
- policy changes (Practices or procedures in policies can shift and might nullify parts of the response plan.)

DISCERN RESPONSE IMPROVEMENT PLANS

A risk *improvement* plan helps the organization manage risks and typically includes guidelines for training, communications, policy changes, contingency planning, organizational changes, or procurement of new assets. A risk *response* plan contains plans for addressing individual risks to help the organization alleviate risk impacts or likelihood.

3.1.2 Determine the Organization's Risk Appetite

The organization must define its risk appetite and develop a risk appetite statement. A *risk appetite* is the general amount and type of risk that the organization is willing to take to achieve its strategic objectives [ISO 2018]. An organization's *risk appetite statement* articulates its risk appetite.

The governance structure's decision makers use the risk appetite statement to help them manage the organization's risks and issues.

CHOOSE A RISK APPETITE STATEMENT

Appendix B provides two types of risk appetite statements. Table 12 on page 76 depicts a risk appetite statement with categories from the organization's strategic objectives and risk tolerances mapped to each one. Table 13 on page 77 depicts a risk appetite statement that focuses on the likelihood of risk realization.

The organization must ensure that stakeholders understand the following two critical elements of a risk appetite statement:

MIND THE "TRIPWIRES"

Refer to page 14 for a list of "tripwires"—events that signal the need for the risk manager to review and update the risk appetite statement.

1. The risk appetite statement must align with the organization's strategic objectives. Ideally, those objectives can be broken into categories, such as revenue, safety, operations, reputation, compliance, and human capital.
2. A risk appetite statement should reflect the dual nature of risks; they can be threats or opportunities.

The organization should periodically review its risk appetite statement and update it as needed.

Risk managers should establish quantifiable *risk tolerances* for each risk category identified in the risk appetite statement. For example, an organization may define its tolerance for loss of revenue as being no more than $10M for any single risk. Therefore, any risk that can result in a negative impact of $10M may be subject to greater scrutiny by members of the governance structure and possibly demand resource investment for mitigation. The more specific and quantifiable the tolerances are, the more likely the organization's decision makers will adhere to the organization's strategy and meet the organization's strategic objectives. These quantified tolerances mean fewer surprises and greater consistency in risk-based decision making. The risk manager must review and validate the risk tolerances with executives.

LEARN ABOUT RISK TOLERANCE

Risk tolerance is "[a] threshold that reflect[s] the organization's level of risk aversion [Caralli 2011].

Developing a Risk Appetite Statement

A risk appetite statement documents the organization's risk tolerance; teams from across the organizations should participate in its development.

At a nascent organization, the risk manager should develop the risk appetite statement and consult with the organization's strategic objectives to get a sense of the critical services and assets necessary to meet those objectives.

At a mature organization, the risk manager should interview stakeholders and prepare for these interviews by researching the strategic objectives to gain insights about already-established risk tolerances. To make it easier to update the risk appetite statement, the risk manager should document all assumptions and information gathered. Categories, such as the ones in Table 12 on page 76 provide context and structure for these interviews.

Regardless of the organization's previous experience with ERM, risk managers should always identify and involve executives and other critical decision makers who will likely use the risk appetite statement. For most organizations, members of Tier 1 of the governance structure usually approve the organization's risk appetite statement. The risk manager should also get input and buy-in from members of all tiers of the governance structure.

When forming the risk appetite statement, the risk manager should educate and interview stakeholders about the following:

- why the risk appetite statement is needed
- how it is used
- how the appetite-development process works

CHOOSE A RISK APPETITE STATEMENT

Instead of interviewing individual stakeholders, the risk manager can organize a facilitated group of stakeholders; however, this process can be challenging. Discussions related to risk can be sensitive and may uncover weaknesses in the organization. As a result, some participants may be intimidated and not provide input. Conversely, those with strong personalities might control the process, which could lead to a biased or unbalanced risk appetite statement rather than one that reflects the input of all the organization's stakeholders.

The risk manager should ensure that each stakeholder understands that they will not be the only one participating in the process. This is a critical step to alleviate surprise if there are disagreements about risk tolerances. Ultimately, disagreements are adjudicated by higher levels of the governance structure, such as the executive board. This adjudication process provides the necessary perspective and information so that the proper risk tolerance can be set.

A risk appetite statement can be established at multiple levels of the organization. At the highest levels, senior leaders must convey their degree of comfort for risk management using risk appetite statements. Risk appetite statements can apply to the entire organization; additional risk appetite statements can be tailored to support a specific part of the organization. For example, the organization might develop a risk appetite statement for its Human Resources department. It is critical that each division or department verifies that the risk tolerance in its risk appetite statement does not exceed the risk tolerances in the organization's risk appetite statement.

3.1.3 Set Risk Management Policy

To ensure that the ERM program is leveraged effectively, the entire organization must contribute to forming and enforcing it. That is why the organization must establish and enforce clear ERM policies and procedures. The risk management policy should include ways to measure the ERM program's efficacy and require that the organization do the following:

GET A SAMPLE RISK MANAGEMENT POLICY

Appendix C on page 81 provides a sample risk management policy. Organizations can customize this sample to fit their culture, scope, scale, and intentions. This report's supplemental materials also contain a template that organizations can use when devising their own risk management policy.

- Provide enough direction for each individual to know their responsibilities for managing organizational risk.
- Answer the "who, what, when, and where" questions related to the organization's risk management policy.
- Contain procedures (or points to separate procedures) that describe how members must comply with the risk management policy.
- Prescribe metrics that indicate the health and effectiveness of the program.

Developing a Risk Management Policy

Organizations should consult the following best practices when developing a risk management policy:

1. Ensure the policy is easy to read and that all stakeholders understand it. (For example, it should avoid using technical jargon that those who are inexperienced with risk might not understand.)
2. Write a policy that is enforceable.
   - Document all related processes.
   - Identify those responsible for each requirement.
   - Specify the procedures and tools needed to support the policy.
   - Focus on the clarity, readability, and relevance of the direction provided.
   - Partner with auditing organizations (internal or external) to learn which artifacts to mandate to help gauge how well the ERM program is working.
3. Leverage existing organizational policies to bolster risk management. (For example, relate the risk management policy to any policy that directs the development of the organization's strategic objectives.)
4. Use the policy to establish a healthy risk culture.

LEARN ABOUT AUDITING

Auditing a risk management policy can involve auditors from inside or outside the organization. Organizations can work with external auditing firms such as the Government Accountability Office (GAO) or Deloitte. Some organizations have their own internal auditing teams. See page 53 in Appendix A for more information about auditing.

- Designate risk owners who advance the ERM program, educate stakeholders, and advocate policy adherence.
- Require all employees to attend risk management training.
- Mandate organization-wide adherence to the policy.
- Provide use cases or examples that relate the policy and procedures to the organization's everyday activities.
- Identify ways to motivate responsible risk management behavior or to penalize irresponsible behavior.

5. Require the policy to be reviewed, updated, and approved periodically.
   - Include a list of all stakeholders who must review, update, and approve the policy.
   - Mandate the policy to document all assumptions that influenced how the policy and procedures were developed.
   - Draft a change management approach that systematically rolls out elements of the new policy. This recommendation is especially critical for nascent organizations, where no risk culture may yet exist.

MIND THE "TRIPWIRES"

Refer to page 14 for a list of "tripwires"—events that signal the need for the risk manager to review and update the risk management policy.

3.2 Step 2—Scope Critical Services & Assets

In Step 2, Scope Critical Services & Assets, the organization asks itself, "What keeps us in business?" As part of this step, the risk manager plans for asset management (Section 3.2.1), identifies and documents assets (Section 3.2.2), and maintains the asset catalog (Section 3.2.3).

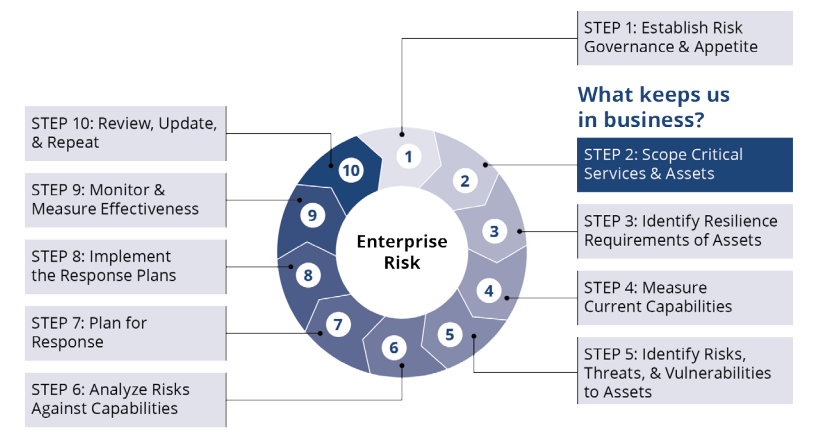


Figure 6: Step 2—Scope Critical Services & Assets

Critical services deliver the products and workflow needed for the organization to achieve its strategic objectives. Identifying these services is the first important step for this phase of the process. Once the critical services are identified, the assets that are used to deliver these services must be identified as well.

An *asset* is something that delivers value to an organization as defined by the CERT RMM [Caralli 2011]. Assets can be grouped into at least four distinct categories: people, information, technology, and facilities. These categories broadly capture the elements needed to deliver an organization's critical services.

The organization manages its critical assets to ensure that it can deliver its critical services.

3.2.1 Plan for Asset Management

Planning is the most critical task of the asset management process. Whether or not the organization uses FORTE to manage assets, its executives must require that critical assets are identified and documented in an asset catalog. They also must provide the funding, oversight, and staffing necessary to operate a comprehensive asset management program.

CONSIDER THIRD-PARTY SUPPLIERS

If the organization contracts with third-party suppliers or purchases equipment or services from them, these suppliers can provide people, information, technology, and facilities. These third-party assets enable the organization to meet its strategic objectives. Therefore, to the risk manager should include these critical assets and critical services when planning for asset management, identifying and documenting assets, and maintaining the asset catalog.

Leadership and advocacy are required to ensure that asset management happens. Asset management requires time and resources that some parts of the organization may not be willing to support because the results of asset management are not immediately apparent, or the task may be thought of as too challenging or costly. No two organizations are alike; each has its idiosyncrasies—cultural and otherwise—that threaten to derail asset management. The organization must consider these idiosyncrasies when planning the asset management process.

3.2.2 Identify Assets and Create an Asset Catalog

The organization must identify its assets—particularly its critical assets—and document them in an asset catalog. As part of this process, risk managers define the information to be gathered about each asset, including the level of detail. (The level of detail can be challenging when describing data-related assets.)

As mentioned earlier, assets can be categorized as people, information, technology, or facilities that provide value to the organization. Regardless of how they are characterized, each asset is best described by identifying the services and processes it supports to directly increase the value of the organization.

The risk manager identifies these services and processes by analyzing the organization's strategic objectives, business plans, contracts, customer requests, and standard work processes.

IDENTIFY AND DOCUMENT ASSETS

The organization documents its assets in an asset catalog that typically includes the following information about each asset:

- identification number
- name (i.e., make and model)
- service(s) supported
- category (i.e., people, technology, information, or facilities)
- location
- owner
- custodian
- business impact rating (in the event of disruption)
- resilience requirements

See the Assets section of Appendix B (page 54) for tips, methods, and samples related to identifying, documenting, and managing assets.

Risk managers can use *value stream mapping* [Plenert 2011] to help identify the organization's assets and collect information about each one. This process creates a detailed picture of the steps in a work process, typically starting with a finished product or service and—working backward through the organization's processes—to identify the assets needed along the way.[9]

[9] For more information about value stream mapping, see Appendix B.

The risk manager should recognize that not all assets are critical to the organization's operation or strategic success, so not all assets need to be documented in the asset catalog.

The risk manager assigns an owner to each asset in the asset catalog. The owner of an asset should be the primary subject matter expert (SME) for managing the risks related to that asset. The SME is responsible for identifying and communicating the requirements for the asset.

ASSIGN ASSET OWNERS

Employees' positions, duties, and physical locations typically change over time. Therefore, it's wise to document the ownership of assets by role or position to maintain a chain of custody. Similarly, asset ownership may naturally translate to risk ownership, so its chain of custody should also be maintained.

The risk manager must also identify a custodian for each asset. A custodian is the asset's caretaker who does not own the asset but stores it on their system. The asset owner develops the requirements, but the custodian implements them.

3.2.3 Maintain the Asset Catalog

The asset catalog supports the management of assets throughout their lifecycle. Therefore, the risk manager maintains the asset catalog as assets change over time.

There are many tools available to help organizations track assets; these tools typically provide an integrated and continuously updated view of core business processes by tracking business resources and the status of business commitments (e.g., orders, purchase orders, payroll).

MIND THE "TRIPWIRES"

Refer to page 14 for a list of "tripwires"—events that signal the need for the risk manager to review and update the asset catalog.

See the Assets section of Appendix B (page 54) for tips, methods, and samples related to identifying, documenting, and managing assets.

Regardless of which tool the organization uses, risk managers must ensure that the organization maintains the catalog. This maintenance might include identifying events that require updating asset records (e.g., preventive maintenance, repairs, replacement, age, change of use).

3.3 Step 3—Identify Resilience Requirements of Assets

In Step 3, Identify Resilience Requirements of Assets, the organization asks itself, "What do we need to keep our assets resilient?" In this step, for each asset in the organization's asset catalog, the risk manager identifies and documents *resilience requirements* (Section 3.3.1) and identifies how the organization will review these requirements (Section 3.3.2).

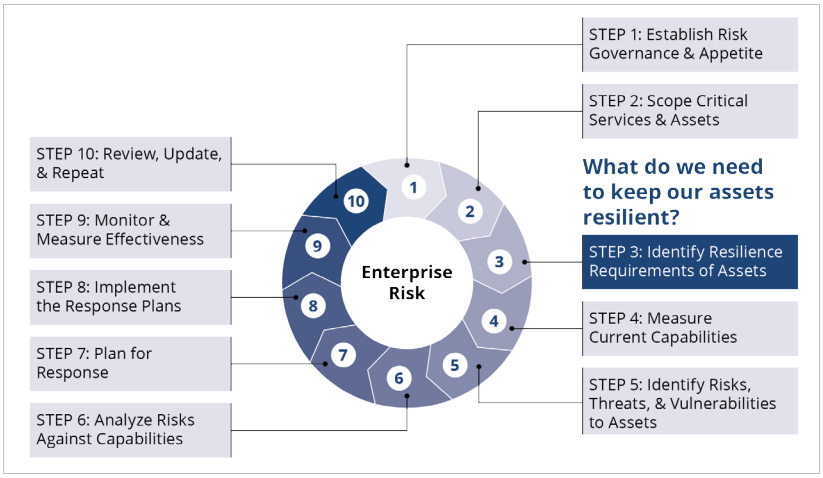


Figure 7: Step 3—Identify Resilience Requirements of Assets

Operational resilience is the ability of a system to maintain the continuity of critical services despite the presence of disruptive events. Resilience is primarily concerned with business continuity and includes managing people, information, technology, and facilities.

3.3.1 Identify and Document Resilience Requirements

Step 2 described the importance of identifying which assets to document and manage throughout their lifecycle. Resilience requirements are similar to asset requirements because the organization must identify and document resilience requirements for each asset in its asset catalog.

DEVELOP RESILIENCE REQUIREMENTS

Resilience requirements have direct and indirect ties to the tolerances established in the organization's risk appetite statement and can provide a solid foundation for developing the organization's risk appetite statement.

Conversely, if these requirements are not known, the risk manager can consult the organization's risk appetite statement to develop them.

To identify resilience requirements, the organization evaluates its cybersecurity risk and defines how risk events can affect the assets in its asset catalog. In particular, it evaluates how these risks affect confidentiality, integrity, and/or availability (CIA); the loss of CIA can negatively affect organizational assets and services.

The risk manager applies CIA to the following asset categories to identify risks:

- **People** apply their critical skills and talents to deliver value to the organization they work for. There are many people-related risks that affect the organization, including weather, illness, employee morale, and working conditions. Even traffic can affect people-related risks.
- **Information** must be available to authorized users when needed. Risks to information, such as threats and vulnerabilities associated with the information systems, can render information unavailable when it's needed. Such risks can disrupt business continuity and affect the organization's ability to deliver its services.
- **Facilities** can have flaws that affect their availability, integrity, and vulnerability. Unlocked doors, poor maintenance, inadvertent limited access, and unsatisfactory design are risks that could result in potentially negative impacts on the organization and its facilities.
- **Technology** automates and supports many of the organization's functions. Technology can become outdated or have vulnerabilities that expose the organization to risks that lead to potentially negative effects on the organization's other assets and services.

LEARN MORE ABOUT CIA

Confidentiality, **i**ntegrity, and **a**vailability are the fundamental resilience requirements for information security. (ISC)^2 defines these terms as follows [ISC 2020]:

Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity – guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity

Availability – ensuring timely and reliable access to and use of information by authorized users

See page 58 for tips on identifying resilience requirements and a sample list of requirements.

Once risks are identified, the risk manager should analyze them to create corresponding resilience requirements that ensure that assets remain viable and sustainable.

The organization can consider the following resilience requirements as well:

- budgetary constraints
- maximum allowable downtime (MAD)
- system performance
- outage coverage
- recovery time objective (RTO)
- recovery point objective (RPO)
- number of and access to system backups
- distance requirements for employees at the main site and backup sites
- business goals and objectives

MANAGE ASSETS

See page 54 in Appendix B for tips, methods, and samples related to identifying, documenting, and managing assets in the asset catalog.

The risk manager should interview asset owners, asset custodians, and other stakeholders to identify resilience requirements for each asset based on its identified risks; the risk manager should then document these requirements in the asset catalog. The organization can adapt Table 1 to help identify its assets' resilience requirements.[10]

Table 1: Sample Resilience Requirements

Asset Name	Confidentiality	Integrity	Availability
Employees	Employee information must be secure, and releasing company information must be prohibited.	An employee should have access to a help desk to address inaccuracies in systems.	An employee succession plan must be up to date, and points of contact must be established.
Customer Data	The customer database requires firewalls, access controls, encryption, and an intrusion detection system (IDS).	Checks on data must be run periodically, and an audit trail of data must be used.	Data must be stored on a secondary external backup server for emergencies or high-volume activity.
Manufacturing Facility	Access to facilities must be limited to employees and permitted guests only.	The site must be monitored for unwanted changes to the data.	Backup site plans must be in place, and facility upkeep must be regulated.
Technology	Access to systems should use multifactor authentication, especially for admin systems and accounts.	Only trusted admin accounts should have access to make changes to critical software.	Backup systems must be established to ensure that critical systems are available to keep operations active.

[10] Table 1 is derived from Appendix B of the report, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process* [SEI 2007].

3.3.2 Review Resilience Requirements

Resilience requirements may change over time, and certain events[11] should trigger the organization to review those requirements. The risk manager should do the following to ensure these requirements are updated regularly:

1. Define how often to review resilience requirements.
2. Document the process for reviewing resilience requirements.
3. Determine the events that trigger a review.
4. Regularly review existing resilience requirements.

RECOGNIZE EVENTS THAT TRIGGER RISK REVIEWS

Events such as the following should trigger the organization to review its resilience requirements:

- staff changes: hiring, firing, laying off, furloughing, or promoting employees
- information changes: creating, deleting, or altering critical data files
- technology changes: adding, altering, updating, or retiring technology assets
- facility changes: purchasing, altering, or selling facility assets
- vendor contract changes: initiating, renewing, or changing contracts
- a merger or acquisition: integrating with new organizations, shifting strategies, changing the services provided

[11] See page 14 for a list of events that should trigger the organization to review its risk-related documents and procedures.

3.4 Step 4—Measure Current Capabilities

In Step 4, Measure Current Capabilities, the organization asks itself, "What measures are currently in place?" In this step, the risk manager reviews the organization's existing controls (Section 3.4.1), assesses control effectiveness (Section 3.4.2), and creates a prioritized list of controls (Section 3.4.3).

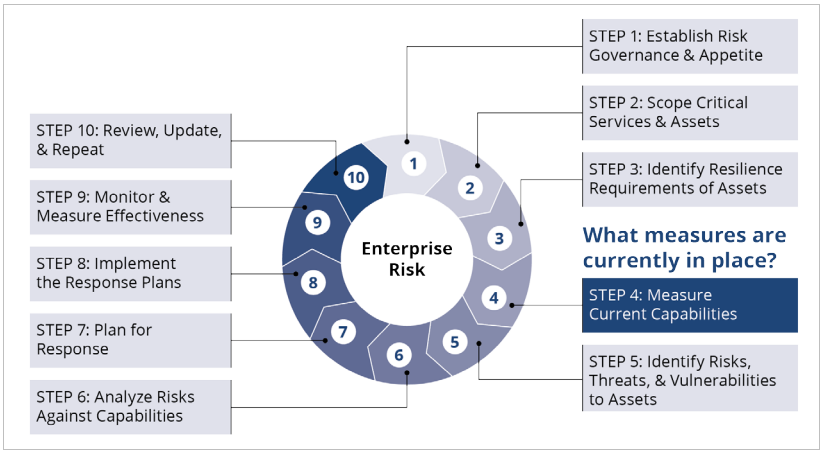


Figure 8: Step 4—Measure Current Capabilities

Controls are the methods, policies, and procedures that the organization uses to respond to risk and meet its strategic objectives. Controls—which can be technological, physical, or administrative—are put in place to enhance the security and resilience of the organization's assets [NIST 2013].

Step 4 is part of an iterative process; it establishes baseline controls when FORTE is first applied and when updates to those baseline controls are made for each iteration thereafter.

REMEMBER THAT CONTROLS VARY

Not all risks use technical controls. For example, risks related to Human Resources may use incentive programs as controls to limit employee attrition. These programs can also serve as a control that addresses insider threat risks. The risk manager should consider the entire organization and all its controls to recognize their interdependence.

3.4.1 Review Controls

To understand the organization's controls and capabilities, the risk manager should do the following:

1. Review the organization's existing controls. For example from a United States Federal Government perspective, these controls can be provided by the organization's system security plan, as prescribed by NIST SP 800-30 [NIST 2012].
2. Determine whether the organization's existing controls meet the resilience objectives established in Step 3.
3. Investigate whether additional research is necessary to identify all the risks. (Risks can extend beyond the cyber domain or the technical controls found in the organization's software. The risk manager must consider the organization's physical and administrative controls as well.)
4. Consult with stakeholders to get additional information about the organization's assets, such as the rationale for the organization's control-related assets. (This rationale also helps the risk manager prioritize the controls as part of creating the list of controls.)

IMPROVE DEFENSE IN DEPTH WITH CONTROLS

A *defense-in-depth* strategy uses layers of controls to help the organization protect its assets and implement protection strategies. Such a strategy reinforces existing controls and establishes a balance that accommodates the organization's risk appetite.

When discussing return on risk investment, risk managers should consider new controls, existing controls, and how all controls combine to respond to multiple, interdependent risks.

For example, the risk manager can demonstrate how to leverage existing controls instead of duplicating them or introducing new controls unnecessarily. Conversely, the risk manager can explain how adding new controls can diversify the security stack. Regardless of the strategy and decision, the risk manager assists the organization with its defense-in-depth [CISA 2005].

3.4.2 Assess Control Effectiveness

The risk manager must assess the effectiveness of the organization's existing controls. They can start by answering the following questions:

1. Are the existing controls meeting the objectives established in Step 3? How do you know?
2. Are all applicable compliance requirements handled sufficiently by controls? If not, can current controls be modified to address compliance requirements?
3. Do the current controls satisfy the organization's crucial objectives? If not, does the organization's risk appetite justify overlooking the gap?
4. Are there gaps where a service objective is not adequately satisfied by a control? If so, can current controls be modified?
5. What is the most cost-effective option to satisfy the organization's objectives?

3.4.3 Create a Prioritized List of Controls

The risk manager must use the above information to create a prioritized list of controls by doing the following:

1. Set targets for performance based on the organization's strategic objectives, risk tolerance, and service/asset resilience requirements. (This step helps the risk manager establish appropriate levels of controls.)
2. Prioritize control objectives. (The risk manager helps the organization determine where resources must be invested first to get the best return on risk investment.)

3.5 Step 5—Identify Risks, Threats, & Vulnerabilities to Assets

In Step 5, Identify Risks, Threats, & Vulnerabilities to Assets, the organization asks itself, "What could possibly go wrong?" The risk manager considers how the organization is affected by changes, such as shifts in technology, evolving environments, fluctuating market conditions, and new attack tactics.

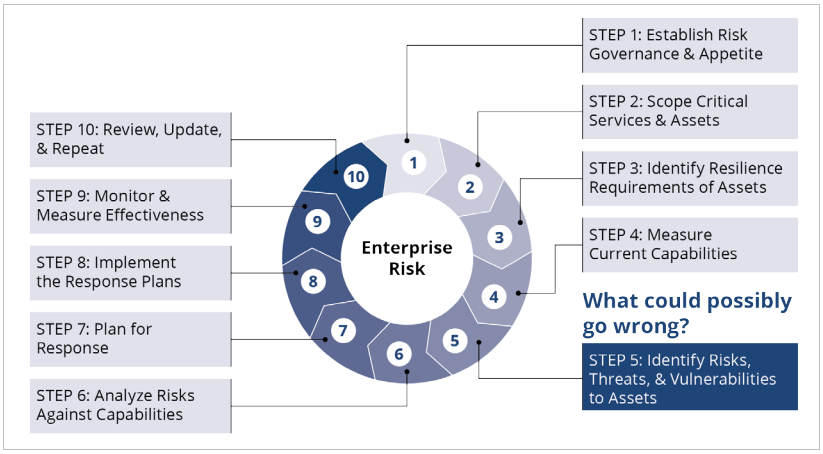


Figure 9: Step 5—Identify Risks, Threats, and Vulnerabilities to Assets

In Step 5, the organization builds on its asset catalog by examining its critical assets and documenting their associated risks, threats, and vulnerabilities.

A *risk* is the effect of uncertainty on objectives [ISO 2011]. A *vulnerability* is a weakness that can be exploited and is not an exploit until acted upon. Vulnerabilities are found in software, hardware, physical structures, and people.

A *threat* is the actor or event that exploits a vulnerability to produce an unfavorable outcome.[12] Many models are available that help organizations identify threats; examples include STRIDE, PASTA, and hTMM.[13] Regardless of the model used, threats can originate from the environment or people. Each threat has the following properties:

- **asset** – something of value to the organization that is typically targeted
- **actor** – who or what can violate an asset's resilience requirements (i.e., confidentiality, integrity, availability)
- **motive** – why the actor acts (whether deliberate or accidental)[14]

LEARN ABOUT ACTORS

Different types of actors can exploit vulnerabilities. Most are people, who are external or internal to the organization. External actors are known as hackers. Internal actors are known as insider threats. Some insider threats are not malicious; they're known as unintentional insider threats and are unaware of the effect of their actions or they just make a mistake [Theis 2019]. Finally, actors are not always people. For example, harsh weather or wildfires are actors that can affect an organization.

[12] For more information about risks, vulnerabilities, and threats, see Appendix A on page 49.

[13] For more information about models that help identify threats, see the SEI blog post, *Threat Modeling: 12 Available Models* by Nataliya Shevchenko [Shevchenko 2018].

[14] Motive and access apply only to human actors.

- **access** – how the asset is accessed by the actor (network access, physical access)[14]
- **outcome** – the immediate result (e.g., disclosure, modification, destruction, loss, interruption) of violating the resilience requirements of an asset

The risk manager elicits information about risks by asking stakeholders to do the following:

1. Review the organization's critical services and the assets that contribute to providing each critical service.
2. List the threats and vulnerabilities related to each asset or asset category. (Keep in mind that risks can also be opportunities that may have positive outcomes.)
3. Identify impacts that would result if each identified risk becomes a reality. (This task helps the organization gauge the "pain it will feel" if the asset or service is unavailable. Explore impacts by conducting a value stream mapping exercise.[15])
4. Forecast the likelihood of each threat or opportunity becoming a reality. (Characterize the likelihood using measures such as high, medium, and low at the very least.)
5. Analyze the consequences of impact. (Use the organization's risk appetite statement to help with this task.)
6. Record these findings in the risk register and asset catalog where applicable. (In this step, Step 5, the risk manager conducts a form of risk identification and qualitative analysis. Although the risk manager builds a risk register as part of Step 6, this is where the roots of the register start to form.)

USE THE RIGHT APPROACH

Until the organization fully embraces an ERM approach where everyone reports risks regularly, the risk manager can use various techniques to identify risks.

- Interview stakeholders.
- Conduct scenario planning.
- Use facilitation techniques, such as the Gap Technique or the bow tie analysis.
- Use affinity diagrams.
- Perform penetration testing.
- Review the risk register from one part of the organization to identify risks in another part of the organization.
- Document, analyze, and stress-test assumptions made in strategies, policies, processes, and operations.
- Conduct threatcasting.
- Use failure mode effects analysis (FMEA) to analyze assets for potential causes of failure.

Many of these techniques are discussed in Appendix B starting on page 53.

An Iterative Process

The organization's ERM process must iterate and adapt to change. Risk managers must continually revisit which assets are critical as well as the risks, threats, and vulnerabilities that affect those assets.

The organization's governance structure must advocate for risk management that is iterative and continuous, with the ultimate goal of instilling a risk culture throughout the organization. Risk management requires the organization and its members to continuously be aware of risks, prioritize them, and deal with their effect on the organization.

[15] For more information about this technique, see Appendix B.

Not all organizations embrace a risk culture; it must be cultivated. Members of the risk governance structure may need to continually train and familiarize other members of the organization with the organization's risk management policy and procedures until they are incorporated into the organization's risk culture. Similarly, members of the governance structure must review the organization's strategic goals and ensure that the risk management program is aligned with those goals and contributes to achieving them. The policies driving the organization's risk management program should convey the organization's attitude and ethos of its culture.

3.6 Step 6—Analyze Risks Against Capabilities

In Step 6, Analyze Risks Against Capabilities, the organization asks itself, "Where do our current measures fall short?" In this step, the risk manager works with stakeholders to analyze the organization's risk data (Section 3.6.1) and create a risk register (Section 3.6.2).

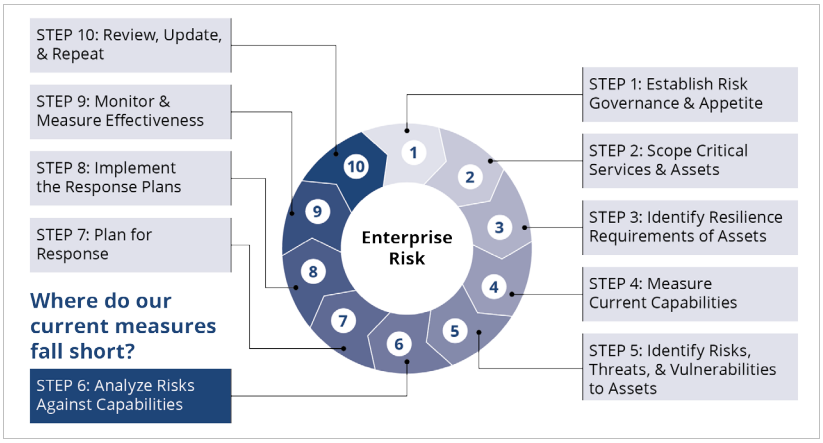


Figure 10: Step 6—Analyze Risks Against Capabilities

3.6.1 Analyze Risks

The risk manager works with stakeholders to review the organization's risk appetite statement and analyze the organization's risks.

However, risk analysis is subjective and rarely dictates what the organization must do or how its executives should allocate resources. Instead, risk analysis identifies the risks that represent the largest risk exposure for the organization in terms of impact and likelihood.

The risk manager and stakeholders do the following to analyze risks:

Mine the Data. Controls (e.g., firewalls and anti-malware systems) are important sources of data that inform the risk analysis process. Part of mining data involves comparing the data from the organization's current controls to the organization's risk appetite statement to analyze which solutions are working well and which ones could be improved.

USE THE RIGHT STRATEGIES AND CONTROLS

Since controls can be technological, physical, or administrative, it's important for risk managers to identify which defense-in-depth strategies to use; however, identifying these strategies can be a challenging and complex process.

For example, to protect an organization's data, risk managers might use a firewall to provide technological control over the flow of data. However, they might also consider requiring employees to sign a non-disclosure agreement to administratively control what data employees can share. FORTE Step 6 should not focus analysis on only one type of control or risk. Stakeholders from across the organization must be involved to maximize the efficacy of the process.

Determine the Impacts and Likelihood of Risk. Previous steps focused on identifying the organization's critical assets.[16] Working with stakeholders, the risk manager determines the likelihood of risks being realized, but this task can be difficult. The risk manager can use different methods to perform this task: probability of occurrence, category ranking (classifying risks into categories such as high, medium, low), ordinal ranking (listing risks in order of likelihood), and relative likelihood (comparing risk likelihood to that of another understood risk).

ESTIMATE RISK

In estimating risk, risk managers can use FAIR, a technique that helps the organization estimate risk and understand the factors that contribute to it. Appendix B (page 67) describes FAIR in detail.

Plot Risks Against Current Capabilities.[17] To help perform this task, the stakeholders and risk manager should use ERM software, which typically offers features such as threat identification, vulnerability analysis, compliance requirements identification, vendor or supply chain risk management, governance, and incident management. The risk manager should select ERM software that closely aligns with the organization's goals and operational needs.

3.6.2 Create a Risk Register

Using the organization's risk appetite statement and the results of risk analysis, the risk manager creates a *risk register*—an annotated list of the organization's risks in priority order. The tolerances in the organization's risk appetite statement provide data to help the risk manager perform a risk analysis and form the register.

The risk manager ensures that the organization's risk register includes information about each identified risk, such as the following:

- nature of the risk that provides the scope and is best characterized using an if-then statement
- the assets impacted by the risk coming to fruition
- the ranking of the risk with others in the register
- who owns each risk
- the planned responses that are in place to respond to the risk

MIND THE "TRIPWIRES"

Refer to page 14 for a list of "tripwires"—events that signal the need for the risk manager to review and update the risk register.

For example, if an organization identifies a risk to the safety of its employees, a risk manager could easily see that the organization should provide resources to mitigate risks that could result in death over those that could result in only bumps and strains.[18]

---

[16] See Appendix B for an example of how risk managers can do this using value stream mapping.

[17] Capabilities are the prioritized controls created in Step 4.

[18] See the Safety row in Table 12 on page 76 for an example.

The risk register should be a comprehensive catalog of the organization's risks and objectives. Some risk registers are organized according to the organization's reporting structure; this approach makes it easier for some organizations to manage their risk register.

3.6.2.1 Managing High Volumes of Risk

When the number of risks becomes large, not only can the risk register become overwhelming to analyze, but it can also intimidate and frustrate the organization's executives. To help, the risk manager should consider using a risk breakdown structure (RBS), which focuses on deliverables and breaks the project into smaller components.

The RBS may be decomposed in different ways. For example, an organization might categorize its risks broadly; some of those categories may mirror those found in the organization's risk appetite statement. Other RBSs categorize risks functionally; this approach makes it easier delegate risks to appropriate risk owners in the organization. This approach might make it easier to identify the risk owner, and it also identifies subject matter experts who may be equipped to analyze and own particular risks.

The number of risks an organization identifies may be so overwhelming that, although they are triaged and understood at a high level, a detailed analysis may not be possible for every single risk. In this case, an RBS can make it easier for the organization to prioritize risk analysis. If risks are categorized properly, the risk manager can prioritize which risks need the most attention as they are compared to the bounds of the risk appetite statement.

3.6.2.2 The Risk Register Is a Living Document

Since the organization continually changes, its risk register should also change and be updated. The person who drafts the risk management policies and procedures must "place themselves in the shoes" of the various stakeholders in the risk management process. That exercise should provide insight into the following:

- who should be given access to the register
- who should be given edit rights to the register
- the type of information that should be included in the register
- how often the register should be reviewed
- the procedure for entering risks into the register
- the criteria for removing a risk
- change control management of existing risks
- the tools expected to be used in building the register

How an organization reviews its risk register varies from organization to organization and might be driven by the context and drivers of each risk. Regardless, the risk register should include review dates to help the risk manager notify managers when reviews are needed. The information should be as accurate as possible. However, this level of accuracy may not always be possible, so assumptions made in the risk analysis process should be documented.

3.7 Step 7—Plan for Response

In Step 7, Plan for Response, the organization asks itself, "How do we respond to risks?" So far, the FORTE process has focused on identifying and analyzing risks to identified assets and services. In this step, knowing how the current controls compare to the organization's risks, the organization begins forming response plans. To accomplish this, the risk manager must educate stakeholders on how to develop response plans (Section 3.7.1), identify interdependent risks (Section 0), gather governance support (Section 3.7.3), and maintain response plans (Section 3.7.4).

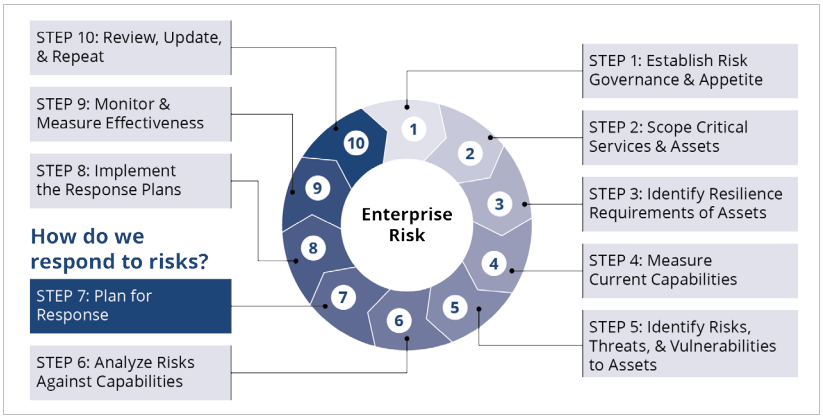


Figure 11: Step 7—Plan for Response

3.7.1 Develop Response Plans

To reduce the organization's exposure to a threat-related risk or to optimize the benefit from an opportunity-related risk, the organization creates response plans. These plans are typically created at the division or department levels by risk owners, who are closest to the risk and its possible impact. Each response plan addresses a risk, or multiple risks that are interdependent.

EXAMINE DECISION-MAKING METHODS

Using decision matrices and decision trees are two effective methods that aid in prioritizing and selecting risks for the response plan. See pages 64-65 in Appendix B for more information about these methods.

A response plan predetermines what the organization will do to reduce risk and respond to risk when it becomes an issue. Response plans seek to disrupt, reduce, or avoid the following:

- risk triggers from taking place
- consequences from making meaningful impact
- conditions aligning that would allow risks to become a reality

Before stakeholders can develop response plans, the risk manager must educate them about risk. For example, remind them about residual risk and that the organization's response to risk affects its bottom line. This type of education is challenging because some stakeholders may not be willing to plan for something that might never happen.

Therefore, it is critical that risk owners form response plans that (1) are consistent with the organization's risk policy, risk register, and risk appetite statements; and (2) have a business case in mind.

Referring to the organization's *risk management policy*, each risk owner creates a risk response plan when a risk is first identified. In the plan, the risk owner assigns a *risk response strategy* to each risk from one of the seven risk response strategies. These strategies include Accept, Avoid, Transfer, Mitigate, Share, Enhance, and Exploit. Each of these strategies typically becomes a project with a defined scope, a schedule, and budget that must be monitored, tracked, and managed.

Because most organizations have numerous risks but finite resources, it's typically not possible to respond to all risks. The risk manager, referring to the organization's risk appetite statement, works with stakeholders to decide whether each risk in the risk register should have a response plan, or if another strategy (e.g., Transfer or Avoid) should be used.

A risk owner does the following as part of developing a response plan:

1. Identify risk triggers (i.e., events or actions that might initiate a risk event).
2. Document and analyze each risk trigger to identify key risk indicators (KRIs), which are signs or metrics that indicate a risk is imminent.

APPLY THE SEVEN RISK RESPONSE STRATEGIES

Mitigate – Take actions to limit the likelihood that the risk will occur, or limit its impact if it does occur.

Transfer – Distribute the exposure of the risk to others to minimize the risk's impact.

Avoid – Cease activity or avoid conditions that may enable the risk to become an issue.

Accept – Take no action to mitigate the risk while continuing activities that constitute it.

Enhance – Take action to bolster the positive impacts of the risk when it becomes a reality (typically used for opportunistic risks).

Exploit – Take action to raise the likelihood of a risk becoming a reality (typically used for opportunistic risks).

Share – Partner with others to divide the impacts of a risk among amenable parties.

Because it's easy, a common strategy to use is Accept; however, when considering using it, be sure that stakeholders recognize the ramifications of accepting the risk. Risk acceptance must be meaningful, planned, and documented.

ACCEPT A RISK

Some organizations Accept a risk if it's the only one of the mitigation strategies that meets the its strategic objectives. Acceptance becomes an eventuality with all risks because residual risk will likely exist despite all actions taken. The key is for the organization to understand what residual risk it can accept to limit its spending and maximize its return on investment (ROI).

CHOOSE THE RIGHT TECHNIQUE

To develop responses to the identified risks, it may be helpful to use a method such as bow tie analysis, business impact analysis (BIA), or a heat map.

Appendix B contains information about of bow tie analysis (page 60), business impact analysis (page 59), and heat maps (page 74).

3. Document the consequences expected if the risk is realized.
4. Establish projects for each risk strategy with requirements and objectives, or simply list the actions the organization should take to implement the strategy.

3.7.2 Identify Interdependent Risks

Risks don't operate in a vacuum; they often interact or affect one another, and when they do, they're called *interdependent risks*. If interdependent risks become issues, the consequences can initiate a ripple effect across the organization and affect operations.

Before writing a response plan, the risk owner must realize that risks can be interdependent. The risk manager or analyst must comb through input from the risk owners about their risks to identify interdependent risks, which the risk manager leverages and uses to develop a response plan.

Response strategies (e.g., Mitigate) typically provide a better ROI if they are applied to interdependent risks, not just a single risk. Applying one of the response strategies to interdependent risks can reduce risk exposure across a significant portion of the organization, often across departmental boundaries.

When developing responses to interdependent risks, the risk manager should consult with stakeholders across the organization. As illustrated in the example on the right, stakeholders can offer details about the risks, controls, and interrelationships that the risk manager may not necessarily know.

UNDERSTAND RISK INTERDEPENDENCE

The following is an example of risk interdependence. Most organizations have varied workforces with many disciplines and skill sets. Talent attrition is a challenge that often reflects interrelated risks across the organization. Examples of risks at a software company include the following:

- Legal wants to reduce the risk of protecting the intellectual property of workforce members.
- Software Development wants to reduce the risk of projects not having the skilled workforce it needs to meet project goals.
- Human Resources wants to reduce the risk of losing part of the workforce to more competitive offers from other organizations.
- Workforce Development wants to reduce the risk that its investments in training the workforce will not pay off because part of the workforce might leave the organization.
- The chief financial officer (CFO) has ideas about acceptable salaries, paid time off, and billing rates.
- The CISO contributes thoughts on insider threat from disgruntled employees.

Risk managers should leverage this interdependency by partnering with departments to analyze the risks related to talent attrition and document their risks (and their interrelationships) in the risk register.

The risk manager can create a decision tree for risk (explained on page 65) to create a graphical list of interdependent risks.

3.7.3 Gather Governance Support

Every response plan must incorporate a compelling business case because it needs to persuade the governance structure to provide resources to implement it and its related projects. In particular, the risk manager must capitalize on responding to risk interdependencies by constructing the business case for responding to these risks in the response plan for interdependent risks to provide a better ROI.

Some plans might leverage qualitative and quantitative techniques. Qualitative techniques can include comparing operating necessity or addressing the competitive necessity for responding to a particular risk. Quantitatively, analysts can use profitability models such as payback period,

Net Present Value (NPV), or Internal Rates of Return (IRR). Unfortunately, these particular quantitative models require data (e.g., reduction in risk exposure), which may not be readily apparent or calculable. In those cases, scoring models can be used, which means that the risk analyst develops critical factors related to the risks in their register (e.g., response plan costs, estimates of reduction in risk exposure, and confidence in the analysis). Each risk can be rated using these factors with a numeric scale—weighted or unweighted. Those scores can help the organization rank and prioritize how it invests resources to manage those risks.

To focus on the business case, risk managers and risk owners collaborate to develop specific, measurable, attainable, relevant, and timely (SMART) goals for the response plans.

CHOOSE THE RIGHT TECHNIQUES

For an example and information about SMART goals, refer to Appendix B, page 72.

If possible, the risk manager or risk owner should involve committees that are part of the governance structure in their planning. Doing so helps secure governance buy-in more easily and completely. To get governance support, the risk manager or risk owner should consider using techniques such as the ones offered in the Executive Support for Projects Model.[19]

3.7.4 Maintain the Response Plans

The risk manager must ensure that risk owners maintain their response plans. Therefore, the risk manager must revisit them periodically. Stakeholders and the governance structure must buy into how often the plans should be reviewed and updated.

MIND THE "TRIPWIRES"

Refer to page 14 for a list of "tripwires"—events that signal the need for the risk manager to review and update the improvement plan and for risk owners to review and update their response plans.

[19] For information about the Executive Support for Projects Model, refer to the paper, "How to Accelerate Executive Support for Projects" [O'Brochta 2010].

3.8 Step 8—Implement the Response Plans

In Step 8, Implement the Response Plans, the organization asks itself, "How do we ensure that our responses reduce overall risk exposure?" In this step, the risk manager ensures that the governance structure allocates resources to implement the response plans (Section 3.8.1), the organization forms projects to implement the plans (Section 3.8.2), and project managers measure and report performance (Section 3.8.3).

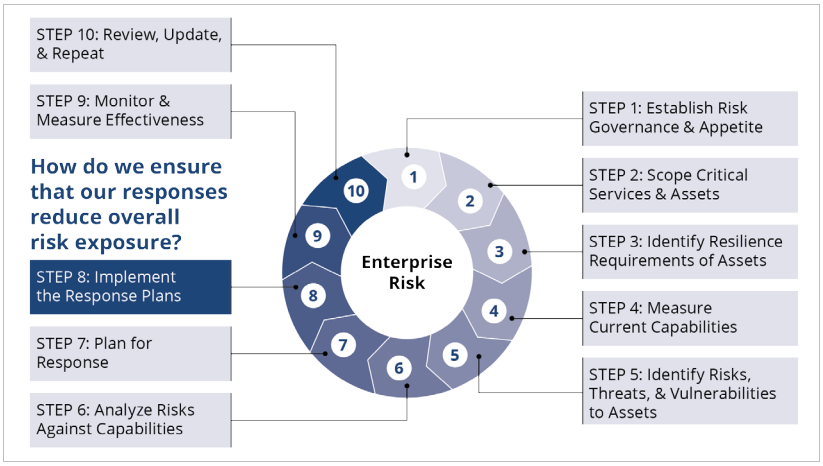


Figure 12: Step 8—Implement the Improvement Plan & Response Plans

3.8.1 Ensure Resources Are Allocated

The risk manager is responsible for ensuring that the organization implements its response plans. The first part of doing that is ensuring that the governance structure allocates resources to the response plans and their projects to enable that implementation. Recall that the organization can choose to Accept a risk and enter it into their risk register as such; Accepted risks do not require project implementation. However the status of Accepted risks should be properly documented and tracked.

This responsibility is critical because the organization's normal operations or other events can distract it from delivering on risk responses outlined in its response plans.

Although the governance structure supported the response plans as part of Step 7, it allocates resources to make the plans happen in this step.

3.8.2 Form Projects

The organization must plan and form projects to execute the work outlined in the response plans. Who establishes and performs projects varies depending on the organization. The organization might have a policy or process that mandates how projects are formed; if not, the governance structure must appoint someone who has the authority, responsibility, and resources to implement the plan and coordinate the work.

USE SOUND PROJECT MANAGEMENT

Organizations should follow project management best practices as prescribed by groups such as the Project Management Institute (PMI). The PMI's hallmark publication, the *Project Management Book of Knowledge* (PMBOK), emphasizes managing scope, schedule, and budget [PMI 2017].

Projects must have the following characteristics:

- have a project plan that includes its scope, schedule, budget, requirements, and risks
- establish and measure success criteria
- set milestones toward project completion
- be assigned to a project manager who leads the project and is responsible for its operation and completion

The risk owner (or another expert who understands the risk) is a good candidate for implementing the plan, coordinating with project managers, and staying engaged in the process to ensure that proper risk response takes place. Each project manager must work with the risk owner and keep them informed of project activities. Each risk owner, in turn, informs the risk manager of progress and delays.

DEAL WITH REALIZED RISKS

A realized risk is referred to as an *issue*.[20] Some actions in the organization's implementation plan are initiated only after risks become issues. Therefore, risk owners should monitor KRIs and/or metrics that show that a risk is being realized. If a risk begins to emerge, the organization should consult its response plan since it should include (1) disaster response guidance that reduces the potential impact of issues and (2) steps for maintaining business continuity.

After the organization recovers, risk managers should conduct a post-mortem analysis to understand how the risk became an issue, how to improve risk analysis to avoid repeating the issue, and whether KRIs were effective.

The risk manager, coordinating with risk owners, reports on the progress of projects to the governance structure throughout each project's lifecycle, including when each project is completed.

The project manager should periodically review their assigned response plan to ensure that the work is on course. Likewise, members of the governance structure should periodically review the response plans to ensure that the related projects receive adequate resources and advocacy throughout their lifecycle.

[20] Of course, a realized risk that is an opportunity is not an issue, but is considered a benefit.

3.8.3 Measure and Report Performance

To report on the performance of their projects, project managers should consider using schedule performance index (SPI) and cost performance index (CPI) metrics.[21] Since the organization is likely to have many response plan projects, SPI and CPI metrics provide a normalized means of comparing projects and assessing the overall effectiveness of the organization's risk response.

Risk Response Is Ongoing

The strategies implemented by these projects reduce the organization's risk exposure, risk impact, and/or likelihood that risks become issues. However, since risk can never be completely eliminated, the organization's risk response is not finished just because the organization has implemented response plans. Updated plans should already be in the works, and the environment will present new risks to tackle.

MIND THE "TRIPWIRES"

Refer to page 14 for a list of "tripwires"—events that signal the need for the risk manager to review and update the risk management policy and/or other risk-related documents.

[21] Learn more about SPI and CPI in the context of earned value management systems (EVMS) in a 2006 paper by Chance W. Reichel [Reichel 2006].

3.9 Step 9—Monitor and Measure for Effectiveness

In Step 9, Monitor and Measure for Effectiveness, the organization asks itself, "How effective is the ERM program?" With FORTE, the organization uses measurement to keep informed of the effectiveness of the organization's ERM program.

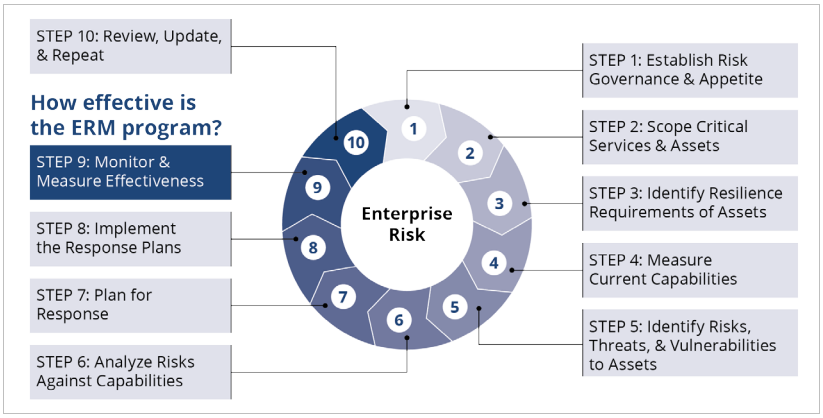


Figure 13: Step 9—Monitor and Measure for Effectiveness

In FORTE's Steps 2-8, the organization focused on identifying risks, vulnerabilities, and threats to its critical assets and services. It then formed plans to respond to the identified risks. In Steps 9 and 10, the organization shifts gears to evaluate its ERM program. It develops metrics to gauge the efficacy of the program so that it can produce meaningful data that supports change and improvements; it documents its findings in an improvement plan that it forms in Step 10.

To accomplish Step 9, organizations must define metrics to measure the right things (Section 3.9.1), measure the ERM program's effectiveness (Section 3.9.2), and monitor risk exposure and impact (Section 3.9.3).

3.9.1 Define Metrics

Metrics not only keep the organization apprised of general project performance, but they also provide insight into the performance of the ERM program. Risk metrics are typically tailored to the organization's objectives and its ERM program. The risk manager uses the risk tolerances in the organization's risk appetite statement to develop metrics that examine how well the organization is responding to risk over time.

To identify metrics, the risk manager starts by determining which risk-related results and progress can be measured. In a cybersecurity organization, examples of these kinds of measures include the following:

- the percent of employees who responded to a test phishing campaign before and after implementing a training program
- the percent of employees who entered their credentials before and after a system was changed to use multifactor authentication
- the percent of employees who reported test phishing emails to IT security before and after a new standard procedure was added to the IT security policy

Similarly, other functions outside of information security may have metrics that relate measures of risk management performance such as the following:

- The **Human Resources Department** might use attrition rates related to the risk of decreased morale.
- The **Treasury** might use the amount of funds remaining in the organization's risk and contingency fund.
- **Contract Management** might use the number of complaints submitted about third-party providers and/or their products or services.
- **Compliance** might use the change in the number of audit findings from one audit to another.

When a risk manager develops metrics, it's helpful to use a standardized method, such as the Goal, Question, Indicator, Metric (GQIM) method. This method identifies organizational objectives, asks questions about meeting those objectives, identifies performance indicators, and defines which metrics the organization should monitor.[22] GQIM is one method; others involve conducting formal assessments that measure risk management maturity.[23]

3.9.2 Measure ERM Program Effectiveness

Metrics help the risk manager evaluate how well the ERM program is doing by monitoring the following metrics in an order of precedence most relevant to their program and organization:

USE METRICS TO PLAN IMPROVEMENTS

The risk manager uses the metrics gathered in Step 9 as input to forming the organization's improvement plan in Step 10.

Response plan implementation. Monitoring the progress of implementing response plans helps the organization track the progress of the teams involved. Implementation issues may be specific to a project or indicate a problem in the overall ERM program. For example, if part of the plan is not fully implemented, it might indicate that the governance structure did not advocate well for the ERM program, the risk manager did not adequately educate the project manager, or the project manager did not communicate well to the project team. Similarly, the organization may track metrics related to improvements to the ERM program itself rather than for risks in the risk register. For example, a shift in risk management policy may require significant training for the whole organization. Clearly, such an effort requires some project management and monitoring to ensure that the program is advancing as planned.

Risk exposure. Monitoring the organization's risks as they begin to be realized shows how improvements have affected the organization's risk exposure. Measuring and responding to KRIs

[22] More information about the GQIM method is available on page 73.

[23] Examples of other methods include the ITIL Service Management Process Maturity Framework, the Institute for Supply Management (ISM) Stage of Maturity Framework, and the Gartner IT Management Process Maturity Model.

is a way to accomplish this kind of monitoring. By monitoring KRIs, risk owners and managers are notified that a risk may be turning into an issue.

Impacts from risk exposure. Monitoring the impact from risk exposure provides critical feedback that the organization should use to improve its risk appetite statement and risk register. For example, if an impact is less than expected, the priority of the risk may change. If an impact involved unexpected parts of the organization, stakeholders from that part of the organization should be included when the improvement plan for that particular risk is being updated. The risk manager should conduct post-event reviews to understand how response plans, disaster recovery plans, and business continuity plans affected that risk exposure.

3.9.3 Monitor Risk Exposure and Impact

Risk managers should gauge trends in risk exposure and impact. These types of measures may be more specific to the context of the risk itself. For example, an organization's talent attrition risk may depend on attrition rate statistics of the organization. Monitoring that attrition rate over time as the talent attrition risk is addressed provides a measure of improvement.

Examples of other metrics that can be used to measure improvement in the organization's risk exposure and impact include the following:

- the percent of risks analyzed of the ones identified in the response plans
- the percent of risks with response plans of the ones identified in the risk register
- the percent of risks that became issues of the ones with implemented response plans

Gathering and maintaining trend data from the time a risk is identified through each ERM program action to the present requires persistent effort. Consequently, the ERM program must have adequate resources, establish guidelines for how resources should be effectively allocated, ensure appropriate ownership, and conduct periodic reviews.

3.10 Step 10—Review, Update, & Repeat

In Step 10, Review, Update, & Repeat, the organization asks itself, "Is our ERM program successful?"

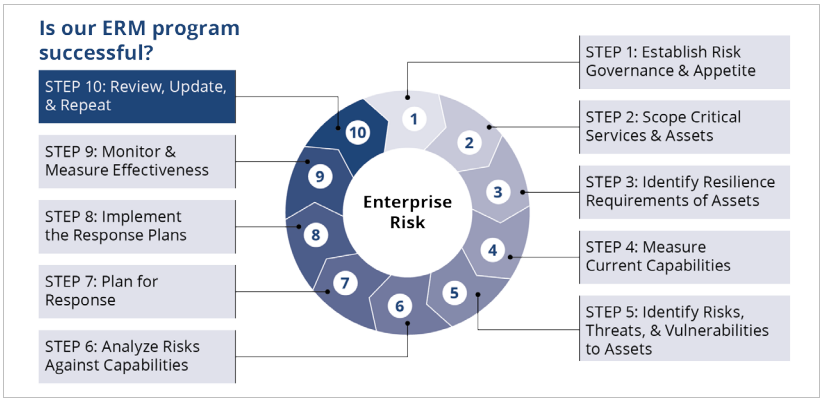


Figure 14: Step 10—Review, Update, and Repeat

During Step 10, with input from the Tier 1 leaders of the organization's governance structure, the risk manager reviews and evaluates the ERM program's effectiveness (Section 3.10.1), develops the improvement plan (Section 3.10.2), implements the improvement plan (Section 3.10.3), and repeats the FORTE process (Section 3.10.4). How often the organization conducts these reviews depends on factors such as the organization's risk appetite and the maturity of its ERM program.

The organization can perform this step at any point in the process; however, it is FORTE's last step to help the risk manager review the results of the process after a complete iteration of the ERM program.

3.10.1 Review the ERM Program's Effectiveness

The risk manager meets with stakeholders, such as asset owners and risk owners, to determine if the ERM program has controlled known risks effectively. The risk manager plans how to elicit this information so that participants can offer input candidly.

The risk manager gets stakeholder input by interviewing them, asking for their written input, or conducting sessions with groups of stakeholders. The advantage of using the last approach is the immediate two-way communication, which improves the risk manager's ability to facilitate the work. The disadvantage of this approach is that those with strong personalities might dominate the conversation, which could lead unbalanced risk input.

The risk manager should prepare questions to ask stakeholders about whether the ERM program is operating the way it should. Example questions include the following:

1. How well did ERM policies and procedures support related activities?
2. Was the method the ERM program used to select metrics for measuring the organization's risk exposure effective?
3. When resources were needed, was it clear who to talk to?
4. Were the right committees and subcommittees named to support the ERM program?
5. Did the risk manager use appropriate techniques to conduct activities, such as eliciting input, gathering metrics, and analyzing data?
6. Did the risk manager use an effective method to form the risk appetite statement? Should the risk manager use a different method?
7. Did the governance structure support the risk manager throughout the process?
8. Was the schedule for reviewing artifacts (e.g., asset catalog, risk register) clear?
9. Does the risk appetite statement align with the organization’s strategy?
10. Is the organization’s risk management policy easy to understand?
11. Was it easy to form projects to support the activities outlined in the response plans?
12. When a threat or vulnerability was discovered, did a response plan provide the right guidance to respond to the risk?
13. Were stakeholders adequately educated about accurately estimating risk?
14. Were members of the executive committee aware of the organization’s residual risk?
15. Were there adequate KRIs to make it easy to recognize when a risk was being realized?
16. Was there enough training available? Was it clear how to register for training?
17. Did “tripwires” alert the risk manager to review critical risk-related documents?

ELICIT INPUT

Post-mortem analyses and lessons learned exercises are opportunities for risk managers to explore what went well and what did not.

The risk manager can use a balanced scorecard approach to examine the ERM program’s efficacy. This approach yields a holistic view of the program’s performance, aligns the program’s goals with employees’ work, prioritizes products and services, and measures and monitors progress towards strategic goals.

A balanced scorecard can vary from program to program and organization to organization, but the spirit of measuring customer perspectives, financial considerations, and value creation in a risk context remains [Kaplan 1992].

3.10.2 Develop the Improvement Plan

The risk manager develops and writes the improvement plan for the ERM program to increase its maturity and improve its performance. Typically, these plan activities require resources and comprise the elements of the ERM program.

The improvement plan should address elements, including the following:

- investment
- training
- communication
- policy changes
- contingency planning
- organizational changes (e.g., new teams)
- asset procurement

The risk manager distributes a draft of the improvement plan to stakeholders for input. The risk manager gathers and organizes the input, identifies opposing viewpoints that need further discussion, and incorporates the input into the plan. This process iterates until the plan is generally accepted.

3.10.3 Implement the Improvement Plan

Once the improvement plan is generally accepted, the risk manager coordinates with the governance structure to secure the resources needed to implement the plan. The improvement plan includes actions like the following examples:

1. Update the governance structure to add a new committee.
2. Update a committee's charter.
3. Add a new staff member to the ERM program to focus on problem areas.
4. Recommend more effective methods for forming the risk manager to use to form the risk appetite statement.
5. Revise the risk management policy to make its message clear for all users.
6. Research and recommend more effective techniques for eliciting requirements and facilitating meetings.
7. Update the process for aligning the appetite statement with the organization's strategic objectives.

3.10.4 Repeat the Process

The improvements the organization makes to its ERM program are designed to reduce the following:

1. the organization's risk exposure
2. impact from risks that become issues
3. likelihood that risks the organization faces will become issues.

However, risk management is ongoing, so the organization's ERM program is always a work in progress. As the organization improves its ERM program and reduces risk exposure and impact, it also improves its ability to continually evaluate its operation and make improvements.

The ERM program is not finished just because the organization completes a cycle of risk management; in fact, it is never finished. The organization must see risk management as an iterative process that must be repeated regularly to do the following:

- Learn from past experiences to leverage wins and improve from mistakes.
- Improve the ERM program to refine related processes and plans.
- Continuously monitor the ERM program, and refine how the organization prevents risk and responds to issues as they occur.

Appendix A: Risk Concepts

Before undertaking the FORTE process, it's helpful to understand the risk concepts it relies on. If you are new to risk management, this appendix explains some basic risk-related concepts and terminology that will help organizations adopt FORTE.

About Risk

Risk is the effect of uncertainty on objectives [ISO 2011]. Risk is an uncertainty that is largely made up of a threat exploiting a vulnerability that results in an impact on the organization. Uncertainty stems from a lack of information, experience, or controllability.

A *realized risk* is called an *issue* because it is affecting the organization and is no longer simply a risk. The result of that realized risk is called a *consequence* (e.g., slow network, denied access to critical systems, malfunctioning sensors). The *impact* of that realized risk is the "pain" (e.g., lost revenue, increased productivity, legal fees) caused to the organization because of the consequence. That impact can be positive (an opportunity) or negative (a threat). Consequences translate to different impacts depending on the context of the event and the organization.

A *vulnerability* is a potential exposure or weakness that can be exploited. Vulnerabilities determine the susceptibility of an organization to disruption; they are found in software, hardware, physical structures, and people. A vulnerability is not an exploit until an actor acts on it.

An *opportunity* is a situation, strength, or condition that can be exploited to produce a favorable outcome. Most people perceive a risk as a negative event; however, an organization's executives and practitioners must have a shared understanding of risk as an uncertainty that may result in a negative or positive outcome for the organization.

A *threat* is the actor or event that exploits a vulnerability to produce an unfavorable outcome.[24] Threats can originate from the environment or people.

A *risk trigger* is an event that indicates a risk is starting to be realized. A risk manager can plan actions that prevent risk from occurring. Similarly, a risk manager can use the consequences of risks to provide context when discussing the actions that limit the impacts to the organization if the risk becomes an issue.

A *risk event* is one or more occurrences that affect the organization's assets and have the potential to disrupt its operations. Consequences to risk events can include loss of availability of a facility, breach of confidentiality for intellectual property, or a lapse in integrity of a particular data set.

[24] For more information about risks, vulnerabilities, and threats, see Appendix A on page 49.

Risk interdependency is the interaction of risks with one another; risks can often be interdependent. When interdependent risks are realized, the consequences can initiate a ripple effect across the organization and affect operations. This ripple effect can also be referred to as a cascading risk event.

Residual risk is risk that remains and is accepted by the organization after response plans are implemented.

About Risk Management

Risk management is an essential business activity for all organizations. Organizations that manage risks effectively tend to thrive and produce high-quality products or services [ISO 2011]. Risk management is a continuous process of identifying, analyzing, and responding to risks that could adversely affect the operation and delivery of an organization's services and assets.

Risk management cannot simply be defined and addressed by policy. In most organizations, risk scenarios can be developed at any time, identifying new threats, vulnerabilities, and outcomes. Executives must set the tone and expectations for how the organization should think about and manage risk. When making decisions, weighing risks should drive executives to be more analytical, questioning and testing their assumptions. Executives should also explore and question any biases when managing risks.

REMEMBER THAT ASSUMPTIONS ARE GAPS

The risk manager should participate in reviews of the organization's strategic objectives to ensure that any assumptions that are used to formulate these objectives are documented and tested. These assumptions represent gaps where data or information may not exist. It's acceptable to make reasonable assumptions; however, the risk manager should develop scenarios that stress the limits of those assumptions.

For example, a marketing team may assume that approximately 10,000 customers will buy a new product in the coming year. The risk manager can test that assumption by developing outcome scenarios, much like those used in sensitivity analysis. After identifying questionable assumptions, the risk manager converts them to risks to enable executives to make stronger, risk-based decisions.

Part of managing risk is being aware of the organization's *risk environment*; by nature, the complexity and number of the organization's risks will increase. Since all organizations live in a risk environment at some level, they must learn to live with uncertainty. To effectively live with risk, the knowledge and awareness of risk issues must be distributed throughout an organization. Traditional tools, techniques, and methods may not work in a risk environment, and existing organizational structures may not be agile enough to adapt.

Managing risk is best accomplished by instituting a *risk management program*—an initiative that enables the organization to manage risks and risk-related activities, and seize opportunities to achieve its objectives. Risk management programs can be divided into a variety of functional subject matter areas. The areas vary in scope depending on factors such as the specific organization, the industrial sector, or the organization's objectives. Some areas are universal; for example, organizations that rely on third-party suppliers to achieve their objectives may require a Supply Chain Risk Management (SCRM) program.

An SCRM program typically leverages the organization's strategic objectives and their association with its supply chain by (1) understanding related risks that might threaten achieving those objectives and (2) responding to those risks to reduce that exposure. SCRM uses a narrow scope to consider the risks that threaten the services and related assets that third-party providers might use. The goal of successful SCRM is to manage risks and make the organization more resilient. Given this goal, the risks in the organization's risk register do not need to be treated equally in terms of analysis and prioritization. All risk programs should follow the same premise.

Enterprise Risk Management

Enterprise risk management (*ERM*) is the culture, capabilities, and practices—integrated with strategy-setting and performance—that organizations rely on to manage risk in creating preserving, and realizing value [COSO 2017]. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (threats and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. ERM can also be described as a risk-based approach to managing an organization.

Risk governance is an overseeing body that provides authority and advocacy, and makes decisions about risk in an organization.

Risk culture can mean different things to different organizations. *Culture* typically drives behaviors in the organization despite management direction or existing policies. A savvy risk executive can use measures of employee engagement, process utilization, and documentation as indications that the risk culture is healthy and working. Awareness campaigns, easily accessible tool sets, and mandatory risk analyses for certain business processes can help an organization develop good habits.

READ ABOUT RISK CULTURE

Suppose a CISO must approve the acquisition and implementation of a new technical security control. In an organization with a healthy risk culture, the acquisition process requires that the security team document and analyze related risks before purchasing a tool. Policies dictate that approving executives must insist on reviewing that analysis before approving the purchase.

An *asset* is anything that delivers value to an organization [Caralli 2011]. A *critical asset* is an asset that supports the critical services of an organization and is critical to the organization's business continuity. The CERT-RMM definition categorizes assets as people, information, technology, or facilities. Third-party providers can use assets from these categories as well to assist a parent or customer organization to deliver their critical services. Ultimately, a disruption to a third-party provider is just as much a threat to the customer organization; therefore, organizations should be sensitive to supply chain risk management concerning customer assets. An organization should inventory its assets and document them in an *asset catalog*. See Appendix B for tips, methods, and samples related to identifying and documenting assets.

A *critical service* is a service that is critical or necessary for an organization to operate.

A *risk appetite* is the general amount of risk that the organization is willing to take when seeking to achieve its strategic objectives [ISO 2018]. An organization articulates its risk appetite in a *risk appetite statement*. The statement also helps the organization qualify, prioritize, and decide who ultimately has decision authority for managing associated risks.

There are two types of risk appetite statements provided in Appendix B. Table 12 on page 76 depicts a risk appetite statement with categories from the organization's strategic objectives with the risk tolerances mapped to each one. Table 13 on page 77 depicts a risk appetite statement that is concerned with the frequency (or likelihood) of risk realization.

CHOOSE THE RIGHT TECHNIQUES

FORTE guides organizations through forming strategic categories and risk tolerances using samples and templates that they translate into their risk appetite statement. See Appendix B for samples and this report's supplemental materials for templates.

Risk tolerances "reflect the organization's level of risk aversion by providing levels of acceptable risk in each […] risk category that the organization established" [Caralli 2011]. Risk tolerances are documented in the risk appetite statement. The risk manager identifies the strategic objectives that can be impacted by risks and quantify the tolerance of risk related to achieving those objectives.

A *risk register* identifies potential risks to organizational assets. It includes information about each identified risk, such as the nature of the risk, the level of risk, who owns it, and what response strategy (e.g., Avoid or Accept) is in place to respond to it.

To manage its risk as part of the ERM program, the organization maintains *response plans.* These plans are created at the division or department levels and address risks that were identified to be managed. The purpose of this type of plan is to reduce the organization's exposure to a threat-related risk or optimize the benefit from an opportunity-related risk. The risk owner writes the risk response plan since they are the person closest to the risk and its potential impact. Referring to the organization's *risk management policy*, and working with the risk manager, the risk owner creates the risk response plan when the risk is first identified. The plan assigns a *risk response strategy* to each risk. These strategies can include Accept, Avoid, Transfer, Mitigate, Share, Enhance, and Exploit. Each of these activities typically becomes a project with a defined scope, a schedule, and budget that must be monitored, tracked, and managed.

Resilience is the ability to quickly adapt and recover from uncertain, difficult circumstances.

Resilience requirements are constraints that the organization places on the productive capability of an asset to ensure that it remains viable and sustainable [Caralli 2011].

Operational resilience is the ability of a system to maintain continuity of critical services despite the presence of disruptive events [Caralli 2011].

A *risk management policy* outlines broad areas of the organization's stance on risk, such as the scope of the ERM program, the business case for the program, the procedures needed to implement the program, and the roles required to support the program.

Risk management policy auditing evaluates how well the organization is adhering to its risk management policy. This auditing is conducted by an auditor or audit team, which can be internal or external.

The organization may have its own internal audit team that is responsible for auditing the organization's compliance to regulations, government policy, etc.

Audit teams are typically linked to compliance; they know what's needed to comply with external rules, laws, and mandates; similarly, auditors can identify specifically how well the organization is complying with its own risk management policy. If the organization has such a team, the risk manager requests that the audit team add a new audit to evaluate the organization's adherence to the risk management policy.

If there is no internal audit team, the organization can hire an outside auditor, such as the Government Accountability Office (GAO), usually for government organizations or government contractors, or other audit firms such as Deloitte, PwC, Ernst and Young, or KPMG.

When writing risk management policies for an ERM program, the risk manager should meet with auditors early in the process. They can help identify artifacts and their format that they look for when determining compliance.

The risk manager establishes an *improvement plan* for the ERM program to increase its maturity and improve its performance. The risk manager writes the plan and includes activities such as training staff, communicating about risk, adjusting the organization's policies, planning contingencies, directing capital investment, procuring new assets, or creating new teams or organizational structures. Typically, these plan activities require resources and comprise the elements of the ERM program.

Appendix B: Techniques and Methods

This section describes techniques and methods that risk managers might use as they follow the steps of FORTE. Some of these techniques and methods help risk managers elicit information from their organizations or make a compelling business case for ERM to present to their executives and set realistic goals; some of the techniques and methods might help risk managers better analyze risk information.

Each technique and method is specifically mentioned in the places in Section 3 where they might be useful. However, they are presented here in alphabetical order so risk managers can browse them as a starting point for learning more about the techniques and methods that support FORTE.

This report's supplemental materials[25] contain several templates that correspond to many of the techniques and methods provided in this appendix; organizations can use/adapt these templates when creating FORTE artifacts.

Appendix B Contents

[25] This report's supplemental materials are available on the SEI website at https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=644636.

Assets

This section describes techniques and methods that can be used to identify assets and their resilience requirements, prioritize assets, create asset profiles, and document assets in an organizational asset catalog. For a deeper discussion of these activities, refer to the *CERT Resilience Management Model (RMM)* [Caralli 2011]. The connection between OCTAVE FORTE and CERT-RMM is natural in that they both help organizations make risk-based decisions to improve the resilience of an organization. Using CERT-RMM as the basis, the steps and examples in the following sections illustrate how an organization can identify and manage assets to aid in its ERM program activities.

Identify Critical Assets by Importance

The organization must identify its critical assets to ensure it can deliver its critical services. As part of this identification process, risk managers should define the types of information that should be gathered about each asset. As part of identifying critical assets, it's helpful to answer the following questions.

1. What are the organization's most important services, and what assets are used to deliver those services?
2. Which assets are used daily?
3. Which assets, if lost, would significantly disrupt the organization's operations and goals—delivering the critical services?

Table 2: Sample Critical Assets List—by Importance

Critical Asset	Why This Asset Is Important	Consequences if the Asset Is Compromised
Firewall	Critical to protecting assets that the organization uses to conduct its day-to-day activities	Loss of data; system downtime; ransom; retooling costs; loss of reputation
Payroll information	Helps the organization pay employees and taxes accurately and on time	Inaccurate pay; late pay; cost of verification and fixing payroll problems
Customer contact information	Helps sales and advertising leverage historical information to target customers	Loss of data; retooling costs; loss of reputation; loss of customers
Off-site storage	Provides a baseline for disaster recovery	No backup data if there is a catastrophic fail of primary systems and data

Identify Critical Assets by Category

A critical asset is an asset that supports the critical services of an organization and is critical to the organization's business continuity. The risk manager should list the organization's critical assets, sorting them by the following categories: people, information, facilities, and technology (PIFT). Each of these asset categories can also be considered from the perspective of belonging to a third-party service provider. In that regard, the internal asset and external asset perspective should be used when considering their contribution to the overall organization. In this case, this consideration could be an additional category called *external*.

The following sample list of critical assets by category shows how this information can be recorded. A template for creating a similar table is available in this report's supplemental materials.

Table 3: Sample Critical Assets List—by Category

Category	Asset(s)
People	employees with needed skills/abilities/knowledge (e.g., security clearances, technical skills, experience in needed areas)
Information	payroll data, customer data, software code, strategic plans, product instructions, accounting data, compliance verification data
Facilities	office space, servers, printers, research labs, systems dedicated to secret work, employee workstations
Technology	firewall, VPN, accounting systems, development systems, backups, approved software baselines, security cameras, access badging system
External	suppliers, distribution centers

Create an Asset Profile

An asset profile identifies threats and risks to critical assets, describes the unique characteristics of each asset, and lists the assigned SMEs.

The following sample list of critical assets shows how this information can be recorded. A template for creating a similar table is available in this report's supplemental materials.

Table 4: Sample Asset Profile

Asset	Risks if Jeopardized	Unique Characteristics	Subject Matter Experts
Firewall	Network breached by an attacker	Controlled by limited group of IT admin users	Chris Small (IT networks) Leslie Werther (IT security)
Payroll information	Employees paid late or paid inaccurately	Depends on interface of data with ADP	Riley Lincoln (HR)
Customer contact information	Release of personally identifiable information (PII), leading to loss of reputation and possible liability	Only accessible by authorized members in multiple departments	Quinn Martindale (Sales) Angel Morales (IT)

Prioritize Assets

The organization should determine which assets, if compromised, would have the biggest impact on its goals and operations by prioritizing the organization's critical assets. Each of these asset categories can also be considered from the perspective of belonging to a third-party service provider. In that regard, the internal asset and external asset lens should be used when

considering their contribution to the overall enterprise. In this case, this consideration could be an additional category, *external*.

Prioritization can be thought of in different ways. It can be costly to replace an asset. In some cases, the amount of time it takes to replace the asset is a bigger consideration. Possibly most importantly, there could be additional risk exposure if a single asset is lost where there is significant interdependency. For example, suppose a skilled worker was classified as a critical asset to the organization. However, the worker is forced to the leave the organization for breaching a computer security policy. In this case, the organization lost the critical skills of the worker, who may be challenging to replace. The organization also likely suffered additional impacts to its information assets. Regardless of the criteria used to prioritize the assets, a scoring scheme can be applied when an asset that fits into multiple categories achieves a higher score than others, thus being prioritized higher.

The following sample list of prioritized critical assets shows how this information can be recorded. A template for creating a similar table is available in this report's supplemental materials.

Table 5: Sample Prioritized Assets List

Organizational Asset	Asset Rank (1-5: 1 Most Critical)
Firewall	1
Payroll information	3
Customer contact information	2
Off-site storage	4
Software development server	5

Define Resilience Requirements

To define resilience requirements, the organization must evaluate its cybersecurity risks and determine how risk events can affect the critical assets in its asset catalog.[26] For the critical assets identified, the organization should identify requirements for confidentiality, integrity, and availability. It should also identify which requirement is the most important. Table 6 lists sample resilience requirements. A template for creating a similar table is available in this report's supplemental materials.

Table 6: Sample Resilience Requirements

Organizational Asset	Asset Rank (1-5: 1 Most Critical)
Firewall	1
Payroll information	3
Customer contact information	2
Off-site storage	4
Software development server	5

Create an Asset Catalog

The organization should inventory its critical assets and document them in an asset catalog. For each asset, the organization should identify characteristics, such as the following:

- identification number
- name (i.e., make and model)
- services supported
- category (i.e., people, technology, information, or facilities, both internal and external)
- location
- owner
- custodian
- resilience requirements
- backup location
- business impact (in the event of disruption)
- importance to the organization

The following sample asset catalog shows how this information can be recorded. A template for creating a similar table is available in this report's supplemental materials.

[26] See Section 3.3.1 for more information about resilience requirements.

Table 7: Sample Asset Catalog

		Asset 1	Asset 2	Asset 3	Asset 4
Name		Firewall	Payroll information	Customer contact information	Off-site storage
Description		Protects the organization's computer systems from cyber attack	Contains PII, tax, and payment information for all employees	Contains PII and purchase history for the organization's customers	Protects the organization's data at a site separate from where the data is used to operate the organization
Importance		Is critical to protecting assets that the organization uses to conduct day-to-day activities	Helps the organization pay employees and taxes timely and accurately	Helps sales and advertising leverage historical information to target customers	Provides a baseline for disaster recovery
Services Supported		Web browsing, file sharing, and remote console access.	Payment of employees and consultants	Direct sales, advertising, maintenance, service	Disaster recovery
Type (e.g., Internal or External, PIFT)		Technology	Information	Information	Facilities
Location		Windows Server in DMZ	Windows Server in DMZ	Windows Server in DMZ	Peoria, Illinois
Owner		Avery Barry (IT)	Jordon Cash (HR)	Reese Sky (Sales)	Amari Campbell (IT)
Custodian		Dallas Short (IT)	Madison Cents (Payroll)	Spencer Bowl (IT)	Rowan Martin (Facilities)
Format		Electronic	Electronic, mag tape	Electronic	Mag tape
Security Classification		Secret	Confidential	Confidential	Confidential
Backup/DR Location		Secondary server farm (Riverdale)	Secondary server farm (Springfield)	Secondary server farm (Castle Rock)	Secondary server farm (Smallville)
Business Impact Disruption (Asset Value)	Loss of Revenue	$14 million	n/a	$4 million	n/a
	Additional Expenses	$130,000	$40,000	$560,000	$140,000
	Regulatory & Legal	n/a	$50,000	$1,200,000	$680,000
	Customer Service	n/a	n/a	$560,000	n/a
	Goodwill	$3 million	$10,000	$5 million	n/a

Bow Tie Analysis

Bow tie analysis provides a high-level visual representation of a risk that can be presented to executives and managers. More importantly, this analysis yields information that helps the organization form a risk response.

The following steps and example illustrate how an organization might conduct and record bow tie analysis of the organization's risks. A template for creating a similar representation is available in this report's supplemental materials.

In this type of analysis, the scope statement articulates the context, conditions, and consequences of risk [Caralli 2011]. When crafting the scope statement, the organization should think about the threats and opportunities the risk presents. In Figure 15, the scope statement identifies major interruptions in a supply chain. The converse of that threat is an opportunity to exceed expectations for resilience in the supply chain. In Figure 15, the triggers, conditions, and consequences columns represent next steps for minimizing residual risk.

After the required information is gathered, the risk manager gathers risks for bow tie analysis, and does the following:

1. Identify the risk triggers.
2. Analyze each risk trigger to identify one or more key risk indicators.[27]
3. Document the risk triggers.
4. Document the consequences of the risk materializing.

The risk manager can also consult with an SME and/or asset owner to supply information, such as a brief description of the risk (i.e., the risk title) and the associated risk category. The risk category can be selected from the organization's risk appetite statement that has the most impact.

A risk manager can use the risk triggers listed on the left side of the figure to discuss the actions that will prevent the triggers from occurring. Similarly, a risk manager can use the consequences listed on the right side of the figure to provide context when discussing the actions that limit the impacts to the organization should the risk become a reality.

[27] Bow tie analysis is typically qualitative; however, it is good practice to think about the quantitative measurement of the key risk indicators (KRIs). KRIs notify risk owners and managers when a risk may be turning into an issue. Similarly, when thinking about how the consequences equate to impacts for the organization, quantification is necessary to help the organization understand the "pain it feels." This approach helps the organization prioritize its response plans.

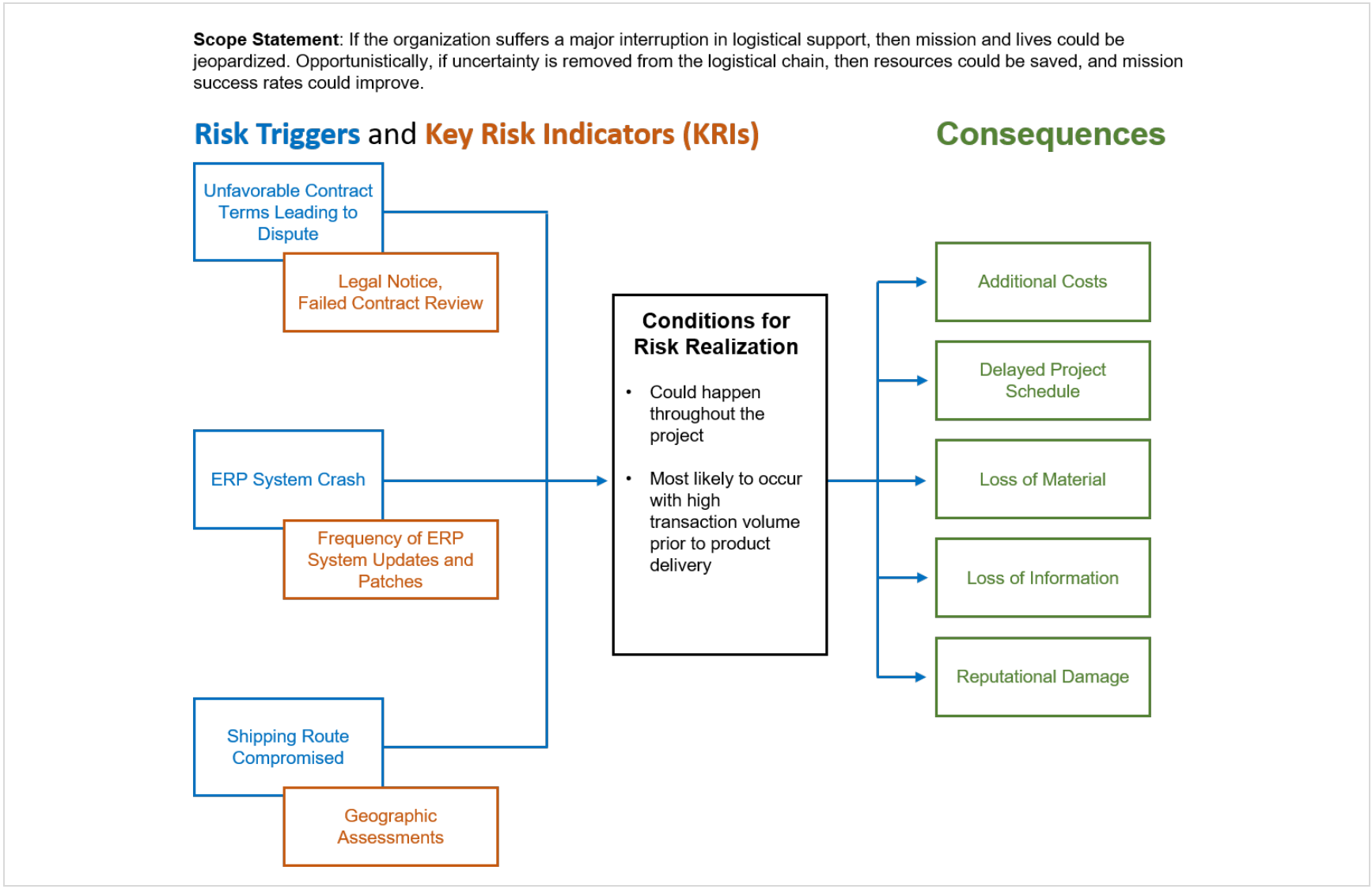


Figure 15: Sample Bow Tie Analysis

Business Impact Analysis

A business impact analysis (BIA) is a process that helps organizations identify (1) impacts (e.g., operational and financial effects) of a service or asset becoming unavailable and (2) the processes and resources needed to recover.

There are no formal standards for conducting a BIA, but it generally includes the following steps:

1. **Gather information**. The organization reviews policy, identifies strategic goals, and interviews or surveys stakeholders to gather information to assess the effects of disruptions to the organization. For the service/asset, the type of information to gather includes the following:
   a. name and description
   b. where/how it is used
   c. description of users
   d. tools/resources used as part of the service/asset
   e. impacts on finances and operations
   f. legal or compliance impacts

2. **Evaluate the information**. The organization reviews and analyzes collected information, and then it documents the following:
   a. prioritized list of the organization's critical services and assets
   b. resources needed to maintain business continuity
   c. the timeframe for recovering and returning the service or asset to normal
   d. the potential losses experienced if assets were lost and caused a failure to meet organizational objectives

3. **Document findings**. The organization produces a report that documents the findings. The report should prioritize the most important services/assets, examine the impact of interruptions to those services/assets, describe any legal and regulatory requirements, list acceptable levels of downtime, and identify the actions necessary for recovery.

4. **Present findings**. The risk manager presents the findings to senior management, who then reviews the report and devises a (1) business continuity plan and (2) disaster recovery plan.

Challenges Mapped to ERM Solutions

When trying to convince leadership to create an ERM program and devote resources to it, it's helpful to identify organizational challenges and map them to ERM solutions.

The following steps and example illustrate how an organization might map its challenges to ERM benefits/solutions. A template for creating a similar table is available in this report's supplemental materials.

To map ERM solutions to the organization's most pressing challenges, the risk manager does the following:

1. Identify the most critical challenges that affect their organization.
2. Identify how an ERM program will address these critical challenges and deliver benefits if implemented.

Table 8: Sample Challenges and Corresponding ERM Solutions

Organizational Challenges	ERM Program Will Deliver
Achieve business objectives	Productivity and profitability
Coping with operational threats and minimizing impact	Better decision making
Managing budgets	Informed budgetary decisions
Finding meaningful ways to measure performance	Safety, health, and satisfaction of customers and employees
Constantly changing the work environment	Improved compliance with standards
Keeping up with a changing technical landscape	Organizational resilience

Decision Matrix

Organizations can use a decision matrix to analyze and prioritize options, and make informed decisions. In a decision matrix, data is formatted in columns and rows to make it easier to visually compare values and weigh/prioritize them.

The following steps and example illustrate how an organization can use a decision matrix to identify the risks it faces. A template for creating a similar table is available in this report's supplemental materials.

The risk manager does the following to create a decision matrix.

1. Select a few critical risks that affect the organization, possibly those of highest importance or priority.
2. Choose criteria related to how the organization should handle these risks. These criteria may be standard risk response strategies (e.g., Accept, Avoid, Transfer, Mitigate), which can provide gross categorization for response plans. A second matrix can be established with more specific criteria (e.g., a series of response plans) such as the one in Table 9.
3. Determine a weighted score for how the organization should manage each risk. Each organization may determine its own means of scoring. Some may opt for a simple Likert scale (i.e., 1-5) where 1 is least desired and 5 is most desired. These scores can also be averaged to get an overall ranking of the controllability of the risk. Regardless of the scale selected, it should be applied consistently across the organization.

Table 9: Sample Decision Matrix

Criteria → **Problems ↓**	Distribute Risk	Educate Employees	Hire Consultants	Make a Legal Agreement	**Average Scores—Controllability Priority Score ↓**
Scarce availability of software development resources	3	5	5	4	4.25
Phishing that steals customer PII	0	5	2	0	1.75
Single-source supplier for key product line	5	3	1	5	3.5
Hurricane season	4	5	2	0	2.75

Decision Tree for Risk

An organization can use a decision tree to visually represent decisions and the decision-making process. A decision tree maps the possible outcomes of a series of choices and helps an organization compare and weigh possible actions based on factors such as risk, cost, and benefits. This approach helps organizations deconstruct complex decisions into component parts, and analyze and identify solutions efficiently.

The example in Figure 16 shows how an organization can use a decision tree to decide whether to buy risk COTS tools or tailor the organization's existing risk tools. A template for creating a similar table is available in this report's supplemental materials.

The risk manager does the following to form a decision tree.

1. Document the decision needed.
2. Identify the decision nodes (i.e., options).[28]
3. Identify condition nodes (i.e., possible results).
4. Determine the likelihood of each condition.
5. Calculate the costs and savings for each condition given the identified likelihoods.
6. Determine the net path value using a method such as expected monetary value (EMV) analysis.[29]

[28] See Appendix A for more information about risk triggers.

[29] Read more about EMV analysis on the PMI website: https://www.pmi.org/learning/library/decision-tree-analysis-expected-utility-8214 [Hulett 2006].

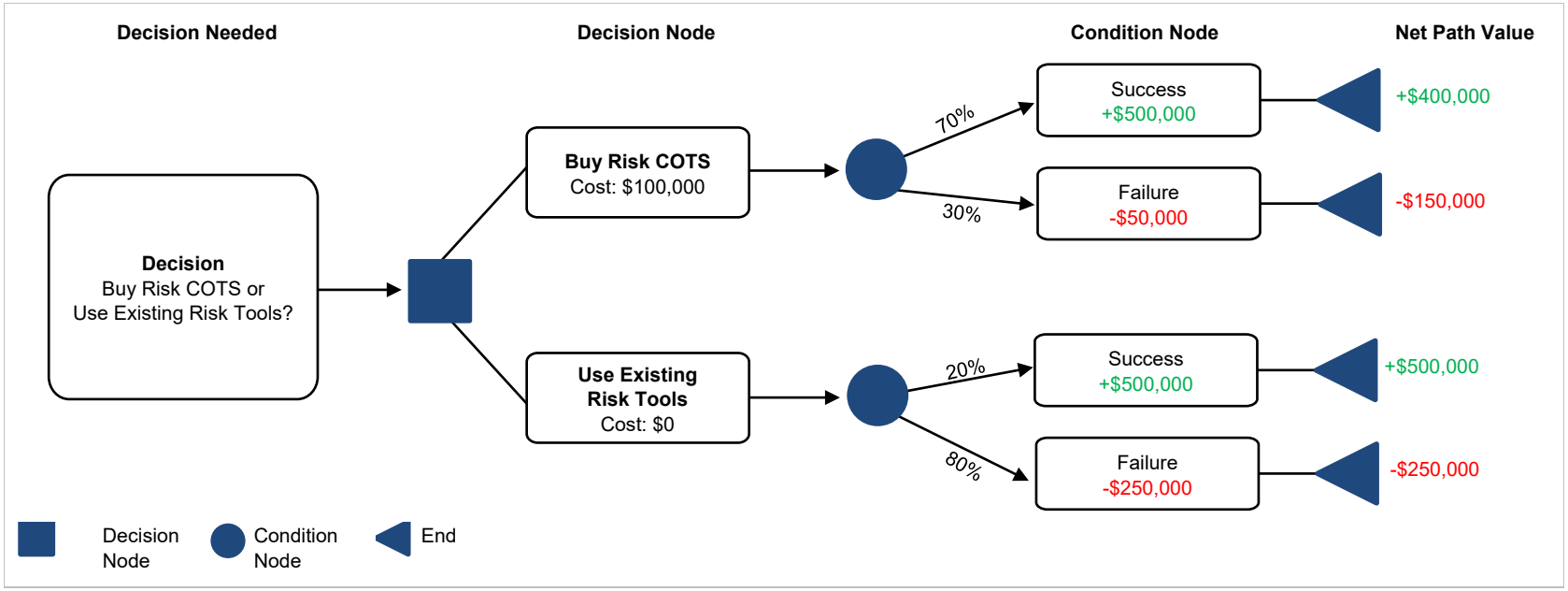


Figure 16: Sample Decision Tree for Buying or Reusing Tools

Factor Analysis of Information Risk (FAIR)

People estimate with different degrees of accuracy and confidence. The FAIR (Factor Analysis of Information Risk) cyber risk framework, designed for cybersecurity and operational risk, helps people understand their ability to estimate. FAIR helps organizations understand, analyze, and measure information risk.

In FAIR, risk owners estimate data about trivial items and assign a degree of confidence to each answer. Analytics are then used to show how individuals (and even groups) can be overly confident in their estimates [Jones 2014].

The following steps show how an organization can use FAIR to develop a risk scenario. A sample implementation of FAIR is available at https://www.fairinstitute.org/what-is-fair.

FAIR's 10 steps are completed in the following 4 stages.[30]

Stage 1: Identify Scenario Components

1. Identify the asset at risk.
2. Identify the threat community under consideration.

Stage 2: Evaluate Loss Event Frequency (LEF)

1. Estimate the probable Threat Event Frequency (TEF).
2. Estimate the Threat Capability (TCap).
3. Estimate Control strength (CS).
4. Derive Vulnerability (Vuln).
5. Derive Loss Event Frequency (LEF).

Stage 3: Evaluate Probable Loss Magnitude (PLM)

1. Estimate worst-case loss.
2. Estimate probable loss.

Stage 4: Derive and Articulate Risk

1. Derive and articulate risk.

[30] These steps were excerpted from the CIO Index website [CIO Index 2019].

Failure Mode and Effects Analysis (FMEA)

FMEA is a process-analysis tool that helps identify possible failures in a system or subsystem, or component levels. It is useful in different circumstances, such as when the organization is

- applying an existing process, product, or service in a new way
- developing control plans for a new or revised process
- planning improvement goals for an existing process, product, or service
- analyzing failures of an existing process, product, or service

The following steps and example show how an organization can use FMEA to develop a risk approach for a critical asset or service. A template for creating a similar table is available in this report's supplemental materials.

To use FMEA, the risk manager follows these steps:

1. Select one of the organization's services or assets.
2. Brainstorm potential failure modes.
3. List the potential effects of each failure.
4. Assign severity rankings.
5. Determine potential causes.
6. Assign occurrence rankings.
7. Identify existing process controls to prevent or detect the failure mode.
8. Assign detection rankings.
9. Calculate a "risk priority number" (RPN).[31]
10. Develop an action plan.
11. Take action.
12. Calculate the resulting RPN.

[31] The RPN is a numeric value representing the risk assigned to the process being evaluated. Refer to the FMEA-FMECA website for more information about calculating RPNs [FMEA-FMECA 2006].

Table 10: Sample Failure Mode and Effects Analysis (FMEA)

Name of Service or Asset Develop and distribute software updates to users to prevent cyber attacks
Process Step (What is the step?) Distribute updates to users
Potential Failure Mode (What are ways the step can go wrong?) Wrong update is sent; update is not sent
Potential Failure Effect (What is the impact on the customer if failure mode is not prevented?) Customer has older, more vulnerability version
Severity (1-10) (How severe is the effect on the customer?) 10
Potential Causes (What is the cause of the failure mode?) Distribution process fails
Occurrence (1-10) (How frequently is the cause likely to occur?) 1
Current Process Controls (What are the existing controls for prevention or detection of the failure mode?) Process verification
Detectability (1-10) (How probable is detection of the failure mode or its cause?) 6
Risk Priority Number (Risk priority: SEV x OCC x DET) 60
Action Recommended (What actions can reduce occurrence of the mode or improve its detection?) Improve the process verification mechanism

GAP Technique

FORTE uses the Gap Technique to elicit risks and their fundamental elements.[32] With this technique, participants perform tasks to record objectives and related uncertainties, identify consequences, agree on the likelihood that identified events will happen, and analyze the consequences and impacts of events.

The following steps and example show how an organization can use the Gap Technique to deconstruct the components of a risk.

Using the Gap Technique, the risk manager works with stakeholders to complete the following tasks:

Task 1. Record the participants' objectives. (The facilitator records the objectives in a way that is visible to all participants). Objectives can vary depending on the participants and the purpose of the exercise. This facilitation technique can be used for identifying risk in any variety of exercises. For example, the participants could be executives who are identifying risks related to the organization's strategic objectives; in that case, the objectives would be strategic. Another example is an audience of project team members who provide their project's scope, schedule, and budget as their objectives for consideration.

Task 2. The facilitator asks participants to list the risks related to each objective. Recall that risks are uncertainties that can be either a threat or an opportunity that produces events, resulting in a positive or negative impact. Therefore, it is good practice to identify "what is the worst that could happen" as well as "what is the best that could happen" for each objective.

Task 3. Participants who are SMEs or asset owners identify the consequences. This task is qualitative. The participants should focus on what they think *could* happen. (The last task in this exercise, Task 5, focuses on the magnitude of the impact.)

Task 4. Participants agree on the likelihood that each identified event will happen. Some participants can identify data that supports the likelihood of an event happening; if that data is not available, the facilitator should ask the participants to make an informed guess about the event's likelihood (e.g., high, medium, and low).

LEVERAGE INFORMATION FROM TASKS 1-3

Tasks 4 and 5 build on Tasks 1-3. In Tasks 4 and 5, the participants build on the information from Tasks 1-3. Participants fill in gaps with quantitative information to define (1) the probability that an event will happen and (2) the extent of the consequences.

Task 5. Participants analyze the consequences of each event and quantify their impact. When data doesn't exist that correlates impact to each identified event, it is useful to refer to the organization's risk appetite statement (see page 76).

[32] The Gap Technique discussed here is not necessarily intended for executive-level consumption. It is used to decompose a set of objectives into their related risks.

Participants can link the objectives from Task 1 of this Gap Technique exercise to the categories in their organization's risk appetite statement.

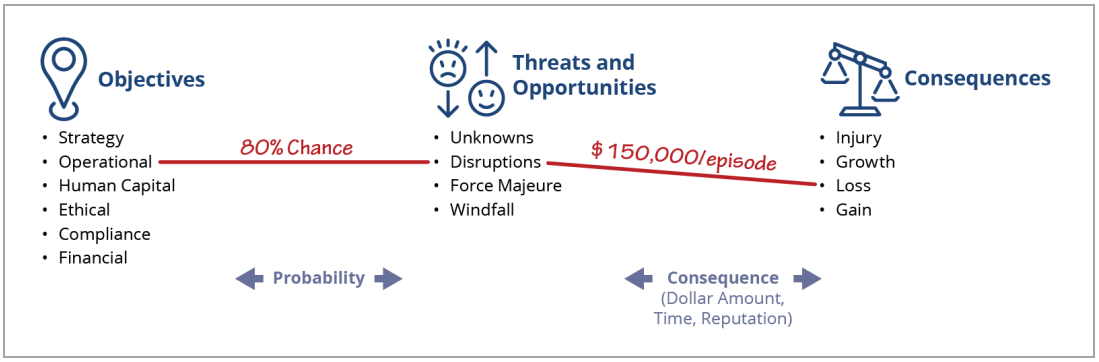


Figure 17: Sample Gap Technique

Governance Structure

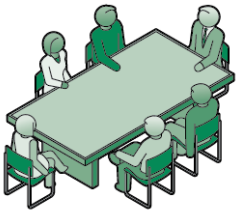
To establish an ERM program, one of the most important elements to develop is a governance structure that will oversee the program's operation.

The following steps and sample illustrate a governance structure. A template for creating a similar representation is available in this report's supplemental materials.

When designing this structure, the risk manager must consider the following:

- Who represents each layer of the structure?
- What are their roles and responsibilities?
- How does the structure tie into the overall organization?

In Figure 18, each layer of this structure represents a decision-making body. Each level captures the roles, responsibilities, and authority of the governance bodies needed to drive the ERM function of the organization.

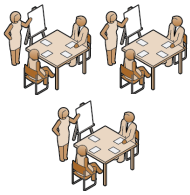


Tier 1: Executive Board

- Roles: senior executives (a subset of the executive board in a private organization; advisory board for a non-profit; or a group of senior executive/appointees in a public organization)
- Responsibilities: sets strategic direction and approves policy
- Authority: institutes authority into the governance structure

Tier 2: Risk Committee

- Roles: executive leaders from across the organization (e.g., chief financial officer, CISO, and chief operations officer)
- Responsibilities: sets policy and procedure, partners with the audit team
- Authority: provides advocacy and resources, such as money



Tier 3: Risk Subcommittee(s)

- Roles: high-performing managers
- Responsibilities: enforces policy and oversee process
- Authority: oversees risk response plans implementation and risk management performance; advises on technical aspects of specific risks; is chartered based on the organization's functions or locations

Figure 18: Sample Governance Structure

GQIM Method

GQIM is a method that helps organizations decompose their operational resilience needs into a set of metrics that are tied to the organization's success as a result of a given process. That is, the metrics quantify the capability of a process to build operational resilience.

The following steps and sample illustrate how GQIM can be used for developing metrics for a risk. A template for creating a similar table is available in this report's supplemental materials.

To use the GQIM method, the risk manager follows the four phases described below.[33]

- **Objectives**. The organization identifies business objectives that establish the need for resilience and cybersecurity.
- **Goal**. The organization develops one or more goals for each objective.
- **Question**. The organization develops one or more questions that, when answered, help determine the extent to which the goal is met.
- **Indicator**. The organization identifies one or more pieces of information that are required to answer each question.
- **Metric**. The organization identifies one or more metrics that will use selected indicators to answer the question.

Table 11: Sample GQIM Method

GQIM Factor	Description
Objective	Prepare for phishing attacks via email.
Goal	Install software that identifies potential phishing email to employees.
Question	What software is available that will identify phishing email that we can install on our system?
Indicator	Phishing email software available on the market
Indicator	Requirements and limitations of our system for installing new software
Indicator	Effectiveness of email software
Metric	Number of emails blocked by software installed on the organization's system

[33] These phases were excerpted from a report (*Applying the Goal-Question-Indicator-Metric [GQIM] Method to Perform Military Situational Analysis*), published by the SEI in 2016 [Gray 2016].

Heat Map

A heat map is a graphical representation of data where values are communicated with gradated color. Heat maps are valuable tools since they convey important information at a glance, making it easier show relationships among variables and direct readers to the data that matters the most.

The following steps and sample illustrate a heat map. A template for creating a similar representation is available in this report's supplemental materials.

To create a heat map, the risk manager follows these steps:

1. Identify risks to the organization.
2. Document the risks in short phrases.
3. Place these short phrases on the heat map, positioning them based on their likelihood and impact.
   - The red areas are high likelihood and high impact.
   - The green areas are low likelihood and low impact.
   - Other colors represent the areas in between these extremes.

A more extensive analysis can be conducted to refine and improve the use of this tool. For example, suppose that the risk manager facilitates the likelihood and impact of each risk. Those results can provide a quantitative scale to plot each risk on the X and Y axis of the heat map. The benefit is an "at a glance" representation of the risk register.

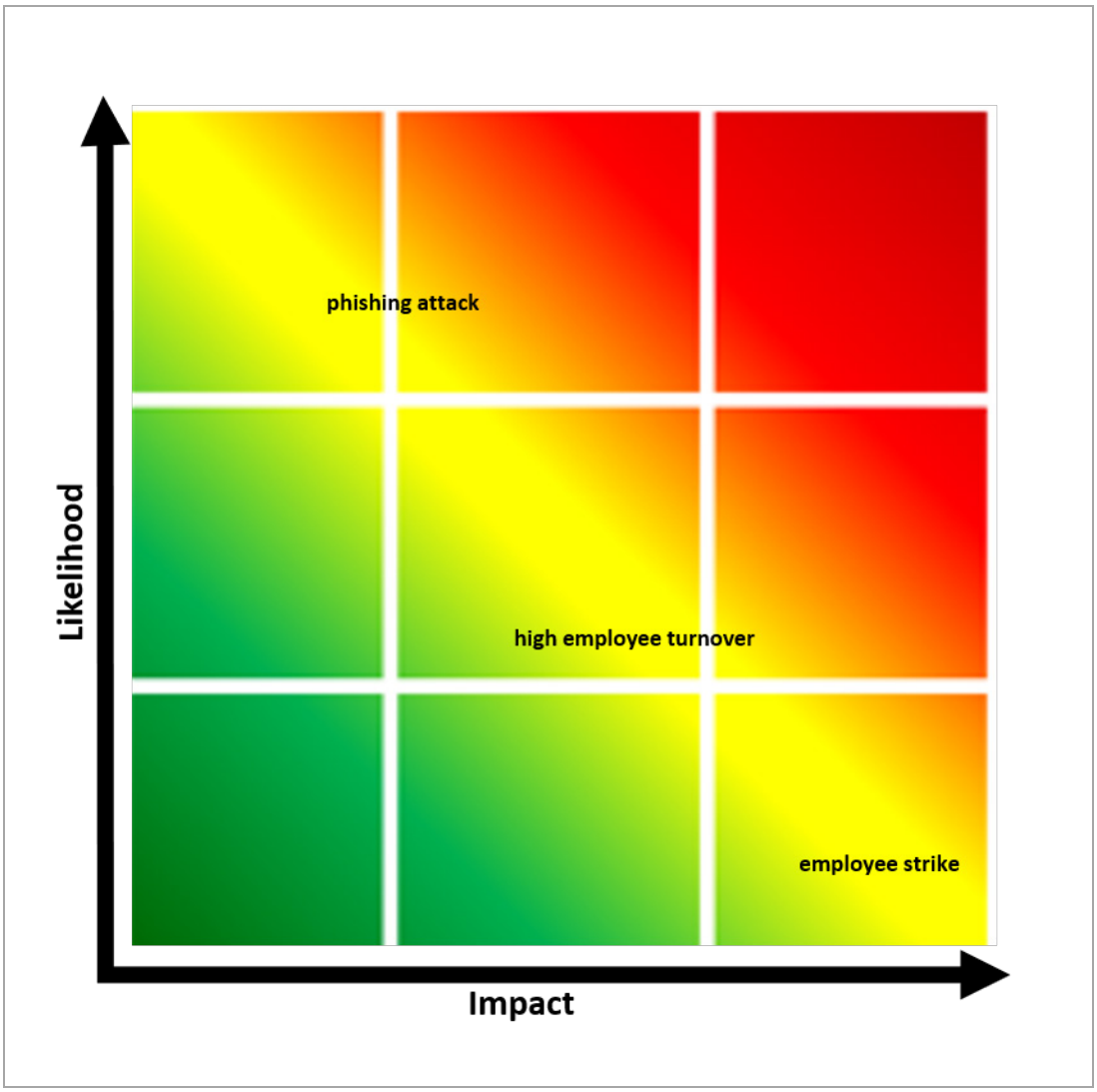


Figure 19: Sample Heat Map

Risk Appetite Statement

A risk appetite statement documents the organization's risk tolerance. The statement provides a baseline that is helpful when developing risk responses and conducting other ERM tasks. The following steps and samples illustrate risk appetite statements. Templates for creating similar tables are available in this report's supplemental materials.

There are two types of appetite statements depicted below. The first uses the categories from the organization's strategic objectives and maps risk tolerances to each one. The second focuses on the likelihood of risks being realized. An organization should review both and determine which best fits its needs.

Risk Appetite Statement Sample 1: Focus on Categories

The categories along the left of Table 12 should correspond to the strategic objective areas defined in the organization's strategic objectives. These categories are listed in priority order so that if the organization has two risks with the same level of concern but in different categories, the one higher on the list takes precedent when allocating resources.

The top row of the statement indicates the level of authority needed to make decisions about the corresponding risk, as delineated in the organizational risk management governance structure.

Table 12: Sample Risk Appetite Statement Focusing on Categories

		Level of Attention		
		Executive	**Management**	**Front Line**
Category	**Revenue**	Any more than a 10% deviation from planned revenue for a quarter	Any more than a 7% deviation from planned revenue for a quarter	Any deviations from planned revenue for a quarter
	Safety	Loss of life or permanent disability	Time away or another reportable incident	Bumps, strains, bruises
	Operations	No more than 5 days of lost operations	No more than 3 days of lost operations	No more than 2 shifts of lost operations
	Reputation	Loss of market segment with multiple customers	Loss of customer	Customer complaints or negative social media buzz
	Compliance	Debarment from a particular market segment linked to regulatory violation(s)	Any fines or other penalties linked to regulatory violation	Any warnings linked to regulatory violation
	Human Capital	Any more than 7% high performer attrition from any business unit in a quarter	Any more than 5% high performer attrition from any business unity in a quarter	Any developing trend in high performer attrition

The risk tolerances in Table 12[34] are largely quantified, or are at least as objective and broadly applicable as possible. For example, the CISO may be most concerned with risks that impact operations. Thus, the CISO would likely contribute values for days of lost operation under the Operations category. This contribution is not unlike what the chief operating officer (COO) would contribute regarding production plant operations.

Risk Appetite Statement Sample 2: Focus on Likelihood

Table 13 is an example of a risk appetite statement based on the frequency (or likelihood) of risk realization.

The appetite statements in Table 13[35] are broad and cover a large part, if not all of, an organization. These statements can be tailored to support specific parts of an organization. Sometimes risks have tolerances built into them, specifically for managing them. Regardless of the scope covered by the risk appetite statement, the risk manager must review and validate the tolerances with senior leadership to ensure the integrity of the governance structure.

Table 13: Sample Risk Appetite Statement Focusing on Likelihood of Risk Realization

	Level of Attention		
	Executive	**Management**	**Front Line**
Range of Likelihood of Risk Occurring	Risk is between 75 - 99% likely to occur. Alternatively, this risk has come to fruition (i.e., become an issue) within the organization within the past quarter.	Risk is between 30 - 74% likely to occur. Alternatively, this risk has come to fruition (become an issue) within the organization within the past month.	This risk is between 1 - 29% likely to occur. Alternatively, the risk has come to fruition (become an issue) within the organization within the past week.

There are other types of risk appetite statements that can be constructed depending on the maturity of the organization, including the following:

- Controllability applies to risks that have the least number of response options or greatest demand of resources. These risks could be thought of as "less controllable" and thus demand more attention from executives. They contrast with other risks that may have cheap and easy solutions to reduce exposure and require only front-line attention to manage.
- Velocity is a measure of those risks that are more likely to happen sooner rather than later. Velocity is concerned with the conditions that can support the risk coming to fruition. A risk with high velocity could be imminent compared to a risk with low velocity. Executives may want to remain informed about those risks and their impact on the organization.

---

[34] This table focuses on establishing tolerances related to negative impacts to the organization. However, these statements may be rephrased to accommodate opportunistic appetite.

[35] Table 12 is derived from Appendix B of the report, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process* [SEI 2007].

SMART Goals Method

The SMART goals method helps organizations define goals that are specific, measurable, achievable, relevant, and timely. This method ensures that goals contain enough information that they are easy to understand and achieve.

The following characteristics and sample illustrate a set of SMART goals. A template for creating a similar table is available in this report's supplemental materials.

SMART goals always have these five characteristics:

- **Specific** goals are well defined, clear, and unambiguous.
- **Measurable** goals include specific criteria that measure progress toward meeting the goal.
- **Attainable** goals are possible to achieve.
- **Relevant** goals make sense for the organization.
- **Timely** goals have a clear, defined timeline.

Table 14: Sample SMART Goals

S Smart	**M** Measurable	**A** Attainable	**R** Relevant	**T** Timely
In the next year, the organization will train its employees on social engineering tactics to lower phishing exposure.	The organization will collect data about instances of phishing attacks and response to in-house phishing campaigns.	Employee training will be required.	Providing adequate training demonstrates beneficial results for the organization.	Employees will be required to take training in the next three months.

Value Stream Mapping

Value stream mapping is a process that helps an organization create a detailed visualization of all steps in a work process. Value stream mapping, used in Lean Management, is useful for identifying organizational assets, particularly critical assets, which, if lost or damaged, bring the critical service to a halt.

All value streams should meet at least one of the organization's overall strategic goals. The organization may start with the finished product or service and work its way back through the production process, identifying needed people, information, technology, or facilities. Third-party providers can be the source of people, information, technology, or facility assets. Non-essential assets can be documented, but they should be lower priority for risk analysis and consideration.

Using the value stream mapping concept, the organization can also document assets in different states: the current state, one that represents the related asset revision, or one that represents a modeled state (e.g., for a piece of software or hardware). The organization can determine intermediate and future states of assets as the risk analysis matures. For example, the risk analysis of the current state of a software asset may uncover vulnerabilities. The risk profile may improve in a future state of that asset once appropriate patches are applied.

Figure 20 provides a sample of value stream mapping applied to software development. An example for creating a similar representation is available in this report's supplemental materials.

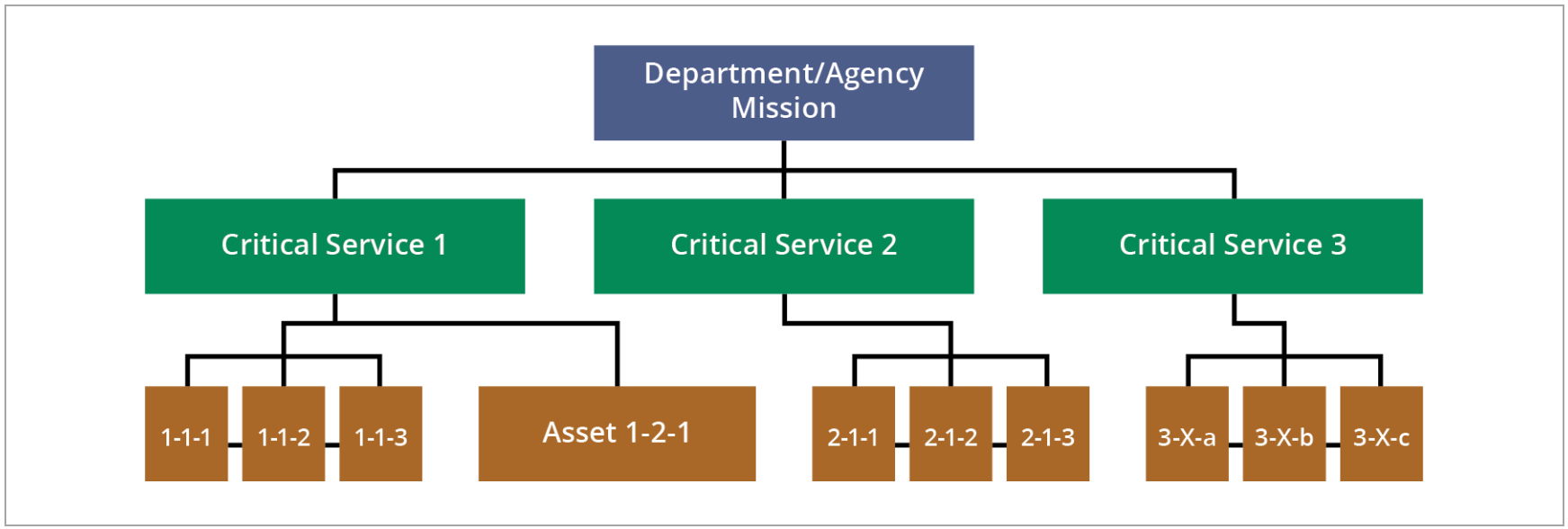


Figure 20: Sample Value Stream Mapping

Appendix C: Example Risk Management Policy

Background

This appendix contains an example of a risk management policy for Lagoon Navigations, Inc., a fictional company used only for demonstration purposes. Organizations can use this example to develop a policy for establishing an ERM program.

This example is not comprehensive; instead, it helps illustrate the FORTE concepts described in this document. Organizations should use the template available in this report's supplemental materials[36] to account for their own risk culture, organizational structure, mission, and strategic goals. Organizations can also change the scope of this policy to account for risk management planning in specific organizational divisions or departments.

[36] http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=644119

Enterprise Risk Management (ERM) Policy for Lagoon Navigations, Inc. (LNI)

November 1, 2020

Signature Approving the Policy (May be More Than One Individual)

Signature of CEO	November 1, 2020
Dana Evergreen	devergreen@lni.com

Signature Approving the Policy (Optional)

Signature of CFO	November 1, 2020
Elizabeth Campastino	ecamp@lni.com

Change Control Log

Section	Change Description	Approval	Date
Scope	Revised scope and business case content	Executive Board	02/23/2020
Scope	Revised governance section	Executive Board	03/02/2020
Training	Added information about training requirements	Training Subcommittee	03/09/2020

Scope

This policy establishes the governance, tools, process, and responsibility for enterprise risk management (ERM) at Lagoon Navigations, Inc. (LNI). The purpose of this policy is to help LNI enhance its ability to achieve its mission, vision, and strategic objectives and strengthen its competitive position. The policy fosters an organization-wide culture of risk and opportunity awareness and provides a structured, consistent, and continuous process for the early and proactive identification and reporting of material risks and opportunities to senior management and trustees.

The scope of this policy is on an organization that provides services. A description of LNI, its culture, number of employees, customer base, market share, and risk appetite are included. See Part C for a discussion of risk appetite.

Implementing this policy will help LNI develop and apply an ERM structure to the organization that includes the adoption of an accepted and tailored ERM framework.

Team members implementing this policy should meet frequently to (1) share-data collection results; (2) consult with the team's manager and report on team progress, including the achievement of project milestones; and (3) assign tasks to develop the ERM program.

ERM is a process designed to anticipate and analyze potential opportunities and threats that could affect LNI's ability to achieve its objectives. ERM is integral to the management and future direction of the organization, and should be structured, consistent, and continuous across the entire organization.

ERM includes identifying, assessing, deciding on responses to, and reporting on risk exposures. These exposures include risks that might hinder LNI's ability to attain its strategic goals and hinder its opportunities that could help it achieve its strategic goals.

Guidelines for ERM come from ISO 31000 and COSO and are actively practiced by LNI, including the following:

- Senior Leadership
- Operations
- Finance & Treasury
- Legal
- Human Resources
- Engineering

Although a number of roles are listed here and may apply to a number of employees and third-party providers in the organization, this policy applies to all LNI employees and third-party providers. Therefore, all questions regarding the content and direction should be forwarded to the chief risk officer, or the most senior risk manager in the organization administering the ERM program.

Business Case to Establish this Policy

ERM creates and protects LNI's value by helping it achieve its objectives and improve its performance in areas such as the following:

- human health and safety
- security, legal, and regulatory compliance
- public acceptance
- environmental protection
- product quality
- project management
- efficiency in operations
- governance
- reputation

To be effective and deliver impact, LNI's ERM program must have the following characteristics:

Is integral to the organization. ERM must be an integral part of LNI's processes. It is not a standalone activity that is separate from LNI's the main activities and processes. ERM is one of management's responsibilities and is an integral part of all organizational processes, including strategic planning and all project and change management processes.

Helps with decision making. ERM enables the decision-making process by helping decision makers make informed choices, prioritize actions, and distinguish among alternative courses of action.

Addresses uncertainty. ERM explicitly accounts for uncertainty, the nature of that uncertainty, and how it can be addressed.

Is a systematic approach. ERM should be systematic, structured, and timely so that it contributes to efficiency and consistent, comparable, and reliable results.

Uses available information. The ERM process should leverage all available information. Inputs to ERM processes include information sources such as historical data, experience, stakeholder feedback, observations, forecasts, and expert judgment. However, decision makers should be aware and informed of the limitations of the data or modelling used. Decision makers should also recognize that experts don't always agree. Some divergence of opinion may be avoided by setting expectations and facilitating meetings and processes well.

Is tailored to the organization. ERM should be tailored to the LNI's needs and structures, and should be aligned with its external and internal context and risk profile.

Accounts for cultural factors. ERM accounts for human and cultural factors. It recognizes the capabilities, perceptions, and intentions of external and internal people who can help facilitate or hinder achievement of the organization's objectives.

Is transparent and inclusive. ERM should involve stakeholders in appropriate and timely ways. In particular, decision makers at all levels of LNI should be involved in the process to ensure that ERM remains relevant and current. This involvement also ensures that stakeholders are properly represented and their views are considered when determining risk criteria.

Dynamically responds to change. ERM is dynamic, iterative, and responsive to changes. ERM continually senses and responds to changes such as when external and internal events occur, context and knowledge change, and risks are monitored and reviewed. ERM also responds when new risks emerge, existing ones change, or others disappear.

Continually improves. ERM facilitates LNI's continual improvement. The goal of ERM is to develop and implement strategies that improve risk management maturity and all other aspects of LNI.

Associated Policies and Standards

Some existing policies may augment this ERM policy and program. This policy focuses specifically on ERM and is supported by the following roles:

- risk management executive sponsors
- risk analysts[37]
- project managers
- functional managers[38]
- enterprise risk owner[39]
- risk management team members

LNI's ERM community gets high-level guidance and direction from authorities and sponsors through a governance structure. The risk committee empowers and delegates the ERM team with the responsibility to implement the processes and activities within this policy, including managing the governance structure.

Governance

All LNI employees play a role in ERM, including identifying and understanding the risks LNI faces, assessing risk exposure, and effectively responding to risks to preserve LNI's

---

37 A risk analyst can be a manager or individual who qualifies or quantifies risk. They may build a risk response plan or conduct a BIA, among other related activities.

38 A functional manager is a general term for a manager in an organization.

39 An enterprise risk owner (i.e., risk owner) is anyone who is responsible to participate in risk analysis, help and/or independently develop and present a risk response plan, and monitor the risk. In some cases, the risk owner is also the person who responds during a risk event.

reputation and maximizing its value. Additional detail regarding the authority and responsibilities related to ERM are provided in this section.

Risk Committee (RC). LNI's RC supports the board of directors by sponsoring the implementation of ERM organization-wide. Among its other duties, the RC sets and approves LNI's risk governance and risk policies, determines its risk appetite, and authorizes allocating resources to manage risk exposures. See Part A, *Risk Committee Charter* for more information.

Risk Subcommittee (RSC). The RSC directs the use of the ERM process for managing risks related to strategy, finances, human capital, business, and operations. See Part B, *Risk Subcommittee Charter*, for more information.

Compliance Subcommittee (CSC). The CSC oversees the processes for prioritizing and managing risks related to ethics, trade compliance, environmental compliance, technology control, and other regulatory requirements. [40]

Enterprise Risk Manager. The enterprise risk manager is the person responsible for executing the program. They lead the ERM team and have the authority to direct all ERM activities as documented in this policy.

Enterprise Risk Team. The responsibilities of the ERM team include the following:

- Integrate the ERM methodology and standards with strategic planning and performance management processes, establishing the context.
- Oversee and facilitate the assessment and review of commercial, regulatory, financial, human resources, operational, and strategic risks as well as any others that may arise.
- Lead the risk community in standardizing risk-related training, executing risk responses, and managing risk.
- Maintain policies and procedures with guidance from the RC and its subcommittees.
- Establish methods and tools for analyzing and managing risks.
- Determine LNI's risk training needs and lead the development of courses and training requirements.
- Approve RC or subcommittee meeting attendance by individuals other than official members.
- Report to the RSC and RC on risk-related topics.
- Hold RC and subcommittee members and participants accountable for their actions.
- Promote continuous improvement of the ERM and its processes.
- Organize, facilitate, and lead RC and subcommittee meetings and events.

---

[40] This subcommittee focuses on compliance, but other subcommittees can be formed to focus on other aspects of risk and the organization.

- Verify actions by risk owners to ensure their compliance and effectiveness in monitoring and executing risk improvement plans.

Enterprise Risk Owner. The chair of the RSC determines which group is responsible for risk ownership when it is in question. The enterprise risk owner's parent organization is responsible for the following tasks:

- Designate a responsible individual to manage a particular risk (i.e., name a risk owner).
- Identify and prioritize the organization's risks, presenting those with the most significant impact and/or velocity to the RSC.
- Monitor key risk indicators (KRIs) and, where appropriate, report significant changes that may indicate a risk event is occurring. The enterprise risk owner assesses risks as they are identified and responds to the risk using Mitigate, Transfer, Avoid, or Accept for threats as appropriate. Similarly, the owner may consider enhancement, exploitation, sharing, or acceptance for opportunities.
- Use resources as necessary to develop a greater understanding of risks and properly execute response plans. They must do the following:
  - Assess the risks, a task that might be facilitated by a member of the risk community. This assessment includes performing detailed identification, analysis, and response planning.
  - Monitor and review risks. Once initial analysis is complete, the risk manager updates the ERM team at least quarterly with KRI data (if no other interval is defined) and change response plans as necessary.
  - Implement response plans according to schedule.
  - Track assigned budgets and schedules.
  - Acknowledge the interdependency among risks and partner with other risk owners to ensure sufficient coverage and avoid duplicating effort.
  - Periodically review risk improvement plans for their effectiveness and return on investment.
  - Identify and document ERM lessons learned and best practices.
  - Where appropriate, declare if a risk should no longer be classified as a viable threat or opportunity to LNI. This does not mean that the risk is deleted, instead it can be placed in a custodial status where no additional actions are taken to reduce exposure to that risk unless new circumstances present themselves.

Performance Metrics Reporting

The ERM team has authority to review all LNI risks. Examples include assessing response plan effectiveness, the quality and level of detail for any risk, and the maturity or effectiveness of ERM. As necessary, LNI may use external auditing services to benchmark existing ERM practices with other organizations.

Training Requirements

Some enterprise risk owners may need training in the management of risks. The ERM team should recommend and provide new enterprise risk owners with the training they need to properly manage risk. The risk community also provides consulting and facilitation of the risk management process.

Reference Documents

COSO: Enterprise Risk Management: Integrated Framework (2004) ISO 31000:2009: Risk (https://www.iso.org/standard/65694.html)

Management of Risks

Once identified, each risk typically matures through a process of identification, assessment, response planning and response execution, and risk closure. The following sections describe related tasks and provide guidance for the proper custodianship over the entire risk lifecycle.

Risk Identification

Risks may be identified by any employee, customer, or vendor. Identification may include documenting the risk statement, trigger events, consequences, and KRIs.

Risks may originate in a project risk register and escalate to the level of an enterprise risk based on its complexity, expected monetary value, severity of consequence, etc. Risk owners should consult with the enterprise risk manager to determine if their risk meets the criteria to qualify as an enterprise risk.

The enterprise risk manager decides if a risk has appropriate significance to be addressed by a subcommittee; this decision might be made using risk tolerance criteria established in LNI's risk appetite statement or otherwise. Alternatively, a subcommittee or committee member may recommend that a particular risk be addressed, typically by notifying the enterprise risk manager.

The risk organization and other LNI audit teams play a unique role in identifying enterprise risks. If an enterprise risk is identified as the result of an audit, the audit director should refer it to the enterprise risk manager for subcommittee consideration.

The enterprise risk manager may periodically survey the committee and subcommittees to identify organizational challenges that must be considered as enterprise risks.

Risk Assessment

Working with the SME or risk owner, the risk analyst performs the risk assessment is performed using the Archer tool. This tool helps identify potential trigger events and potential consequences. Trigger events are events that could lead to the occurrence of at

least one consequence. Based on qualitative analysis, the significance of trigger events and their consequences are ranked. Depending on the possibilities, trigger event responses and fallback plans for the potential consequences are evaluated. If necessary, further quantitative analysis is performed.

Risk Response Planning and Response Execution

The risk response plan reduces the likelihood of the occurrence of a risk and/or reduces the potential impact of a risk by addressing the triggers and consequences. Risk responses may also change how frequently the risk occurs and/or how quickly it escalates. Risk response plans should be periodically reviewed and scrutinized for their effectiveness; LNI determines the schedule for the reviews and who should lead the effort.

Enterprise risk owners are encouraged to consult subject matter experts and others to evaluate response plans for prioritization and potential effectiveness, where appropriate.

Risk Closure

Enterprise risks should never be deleted; rather, they should be closed and archived at LNI's HQ at Cove Locker.

Following closure, risk owners must discern the effort necessary to maintain proper custodianship by monitoring for a risk reemerging, reporting significant changes, and providing updates when necessary.

When roles and responsibilities are reassigned, all enterprise risk owners must report (1) each risk as an item that must be reassigned and (2) whether the risk's status is active or closed.

Tools and Techniques

Lagoon Navigations, Inc. leverages the capabilities of a single governance, risk, and compliance (GRC) software utility called RiskDredger. Although the office of the CIO provides and maintains this utility, the CISO owns it and is responsible for managing it. As the owner of the tool, the CISO's duties include but are not limited to the following:

- maintaining data quality
- providing reporting services
- training the organization to use the tool
- enforcing the tool's use

Enterprise risks must be documented and can be managed using one of the following risk tools: RiskManageIt, RiskNoMore, and RiskSuppressor. These tools are helpful in analyzing risks, specifically risks pertaining to modeling, simulation, and calculation.

As with most risks, the risk owner must be vigilant in accurately documenting risk and properly classifying them to avoid losing or exposing sensitive information.

Part A: Risk Committee Charter

The RC provides the organization with the consultation and leadership necessary to navigate through uncertainty.

RC meetings are held every other month, opposite those of the RSC. A chairperson may approve delays and cancellations as business conditions warrant; however, the RC must still meet at least semi-annually.

Membership must include no fewer than 5-7 members from the C-suite. The chief risk officer must chair each meeting and provide an annual update to the executive board.

Member attendance should be no less than 70% in a year for subcommittees and 100% in a year for the RC. Members may send alternates in case of unavoidable absence.

Unless otherwise approved by chair members, designated alternates must be direct reports of the subcommittee/committee member and must have the power to support the decisions the particular committee makes.

Overall meeting attendance for any RC or subcommittee member organization should be no less than 100%.

Only named members or alternates should attend RC and subcommittee meetings unless the enterprise risk manager gives prior approval.

Break-out meetings are encouraged for complex issues where a greater level of detail and analysis is needed. The risk manager or issue/risk owner should share the results of those meetings should be shared with other committee members.

One member must be appointed as the secretary to take minutes, track actions items, and schedule new meetings. This duty can be delegated to someone else in the organization who is not an official member of the RC.

A 75% quorum is required to hold an official meeting. Similarly, a simple majority of members is required to approve decisions, new policies, the organizational risk appetite statement, etc.

The RC must review and reapprove the ERM policy and risk appetite statements at least annually. Similarly, all risks found in the ERM register must be reviewed and validated at least every 18 months. The risk review may be delegated to the risk subcommittee or appointed SMEs.

Part B – Risk Subcommittee Charter

The RSC directs the use of the ERM process for prioritizing and managing risks related to these specific activities: major projects like wetland reclamation, cybersecurity-related functions, and organization-wide policy changes. The RSC has the authority to prescribe ERM strategies and evaluate the effectiveness of ERM throughout LNI.

RSC membership is a core body of five to seven non-staff members, who are appointed by the RC. Individuals nominated for the RSC should represent high-potential leaders who can effectively collaborate to govern, assess, and develop scenario plans for the most significant risks facing LNI.

The RSC chairperson or co-chairs can assign additional roles and responsibilities related to ERM, including delegating duties to other members of LNI. For example, RSC chairs or co-chairs can invite subject matter experts to partner and participate in RSC activities.

The RSC meets every other month, opposite that of the RC. The target number of meetings in a year is six, but no less than two.

The RSC has the following responsibilities:

- Report high-risk threats and opportunities to the RC when necessary.
- Counsel risk owners regarding risk assessment, response plans, and related actions.
- Evaluate the relevance of the LNI risk register in terms of meeting tactical and strategic business objectives, and update the register accordingly.
- Provide guidance to the ERM team about risks that need to be elevated to other corporate governance entities.
- Improve and implement changes to the ERM process, including proposing how to identify, assess, and manage risks across business lines and portfolios.
- Contribute to developing and the ongoing monitoring of LNI's risk tolerance.
- Review and approve ERM policy exceptions when necessary.
- Leverage LNI resources to (1) help risk owners with response planning and (2) take measures to optimize the outcomes of all risks.

One member must be appointed as the secretary to take minutes, track actions items, and schedule new meetings. This duty can be delegated to someone else in the organization who is not an official member of the RC.

A 75% quorum is required to hold an official meeting. Similarly, a simple majority of members is required to approve decisions, new policies, the organizational risk appetite statement, etc.

Part C – Risk Appetite Statement

The risk manager develops LNI's risk appetite statement by collecting information from stakeholders during facilitated interviews. The risk manager collects the following information and documents it from those interviews:

- assumptions made
- strategies considered
- individuals interviewed
- questions asked during the facilitated interviews

The risk manager then analyzes, consolidates, and documents this information in LNI's risk appetite statement.

		Level of Attention		
		Executive	**Management**	**Front Line**
Category	**Revenue**	Any more than a 10% deviation from planned revenue for a quarter	Any more than a 7% deviation from planned revenue for a quarter	Any deviations from planned revenue for a quarter
	Safety	Loss of life or permanent disability	Time away or another reportable incident	Bumps, strains, bruises
	Operations	No more than 5 days of lost operations	No more than 3 day of lost operations	No more than 2 shift of lost operations
	Reputation	Loss of market segment with multiple customers	Loss of customer	Customer complaints or negative social media buzz
	Compliance	Debarment from a particular market segment linked to regulatory violation(s)	Any fines or other penalties linked to regulatory violation	Any warnings linked to regulatory violation
	Human Capital	Any more than 7% high performer attrition from any business unit in a quarter	Any more than 5% high performer attrition from any business unity in a quarter	Any developing trend in high performer attrition

References

URLs are valid as of the publication date of this document.

[Caralli 2012]
Caralli, Richard A. *Discerning the Intent of Maturity Models from Characterizations of Security Posture.* Software Engineering Institute. Carnegie Mellon University. 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=58922

[Caralli 2011]
Caralli, Richard A.; Allen, Julia H.; & White, David W. CERT® Resilience Management Model: *A Maturity Model for Managing Operational Resilience*. Addison-Wesley. 2011.

[CIO Index 2019]
"Factor Analysis of Information Risk (FAIR)." CIO Index. December 2019. https://cio-wiki.org/wiki/Factor_Analysis_of_Information_Risk_(FAIR)

[CISA 2005]
Cybersecurity and Infrastructure Security Agency (CISA). "Build Security In: Defense in Depth." 2005. https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth

[COSO 2017]
Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management: Integrating with Strategy and Performance*. June 2017. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[DOE 2012]
U.S. Department of Energy & U.S. Department of Homeland Security. *Electricity Subsector Cybersecurity Maturity Model.* Carnegie Mellon University. 2012. http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf

[FAIR 2020]
The FAIR Institute. Factor Analysis of Information Risk. 2020. https://www.fairinstitute.org/

[FMEA-FMECA 2006]
FMEA-FMECA. "Effective FMEAs: Risk Priority Number." 2006. https://www.fmea-fmeca.com/fmea-rpn.html

[Gray 2016]
Gray, Douglas. *Applying the Goal, Question, Indicator, Metric (GQIM) Method to Perform Military Situational Analysis*. Software Engineering Institute. 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=455105

[Hulett 2006]
Hulett, D. T. "Decision tree analysis for the risk averse organization." Presented at PMI Global Congress 2006—EMEA, Madrid, Spain. Newtown Square, PA: Project Management Institute. 2006. https://www.pmi.org/learning/library/decision-tree-analysis-expected-utility-8214

[ISC 2020]
$(ISC)^2$. CSSP Glossary—Student Guide. The International Information System Security Certification Consortium $(ISC)^2$. 2020. https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary

[ISO 2018]
International Standards Organization. ISO 3100 Risk Management. International Standards Organization. 2018. https://www.iso.org/iso-31000-risk-management.html

[ISO 2011]
International Standards Organization. ISO 31000:2009 Risk Management—Principles and Guidelines. 2009-2011. https://www.iso.org/standard/43170.html

[Jones 2014]
Jones, Jack & Jack, Freund. 2014. *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann. https://www.fairinstitute.org/fair-book

[Kaplan 1992]
Kaplan, Robert S. & Norton, David P. "The Balanced Scorecard—Measures that Drive Performance." Harvard Business Review. January-February 1992. https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2

[NIST 2018]
National Institute of Standards and Technology (NIST). "Cybersecurity Framework." 2018. https://www.nist.gov/cyberframework

[NIST 2013]
Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology (NIST). NIST Special Publication 800-53, Revision 4. April 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[NIST 2012]
National Institute of Standards and Technology. *Guide for Conducting Risk Assessments.* SP 800-30 Rev. 1. 2012. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[NIST 2011]
National Institute of Standards and Technology (NIST). *Managing Information Security Risk: Organization, Mission, and Information System View.* 2011. https://csrc.nist.gov/publications/detail/sp/800-39/final

[O'Brochta 2010]
O'Brochta, Michael. "How to Accelerate Executive Support for Projects." Presented at PMI Global Congress 2010, Washington, D.C. Project Management Institute. 2010. https://www.pmi.org/learning/library/accelerate-engage-executive-support-projects-6503

[Plenert 2011]
Plenert, Gerhard J. *Lean Management Principles for Information Technology*. CRC Press. 2011. https://www.crcpress.com/Lean-Management-Principles-for-Information-Technology/Plenert/p/book/9781420078602

[PMI 2017]
Project Management Institute (PMI). *PMBOK Guide – Sixth Edition.* 2017. https://www.pmi.org/pmbok-guide-standards

[Quality-One 2020]
Quality-One International. Failure Mode and Effects Analysis (FMEA). 2020. https://quality-one.com/fmea/

[Reichel 2006]
Reichel, Chance W. "Earned Value Management Systems." Project Management Institute. 2006. https://www.pmi.org/learning/library/earned-value-management-systems-analysis-8026

[SEI 2018]
Software Engineering Institute. *Smart Grid Maturity Model Assets Collection, Version 1.2.* 2018. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=512758

[SEI 2016]
Software Engineering Institute. *CERT Resilience Management Model (CERT-RMM) Version 1.2.* Software Engineering Institute. 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

[SEI 2007]
Caralli, Richard A.; Stevens, James F.; Young, Lisa R.; & Wilson, William R. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Software Engineering Institute. 2007. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

[Shevchenko 2018]
Shevchenko, Nataliya. Threat Modeling: 12 Available Methods [blog post]. *SEI Blog.* December 2018. https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

[Theis 2019]
Theis, Michael; Trzeciak, Randall; Costa, Daniel; Moore, Andrew; Miller, Sarah; Cassidy, Tracy; & Claycomb, William. *Common Sense Guide to Mitigating Insider Threats, Sixth Edition*. CMU/SEI-2018-TR-010. Software Engineering Institute, Carnegie Mellon University. 2019. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644

[Tranchard 2015]
Tranchard, Sandrine. *The Revision of ISO 31000 On Risk Management Has Started*. May 2015. https://www.iso.org/news/2015/05/Ref1963.html

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	November 2020	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Advancing Risk Management Capability Using the OCTAVE FORTE Process	FA8702-15-D-0002

6. AUTHOR(S)
B. A. Tucker

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2020-TN-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

OCTAVE FORTE (Operationally Critical Threat, Asset, and Vulnerability Evaluation **FOR T**he **E**nterprise) is a process model that helps executives understand and prioritize the complex risks affecting their organization. It also helps organizations identify, analyze, prioritize, and mitigate risks that could impact them.

The Software Engineering Institute (SEI) developed the OCTAVE FORTE process model to help organizations evaluate their security risks and use ERM principles to bridge the gap between executives and practitioners. The process model guides organizations that are new to risk management in building an ERM program, and it helps mature organizations fortify their existing ERM program, making it more reliable, measurable, consistent, and repeatable.

Besides describing the OCTAVE FORTE process, this report recommends methods and provides a sample risk management policy that organizations can refer to or adapt when writing their own policy. Supplemental materials contain templates that organizations can use when conducting many of the OCTAVE FORTE activities.

14. SUBJECT TERMS	15. NUMBER OF PAGES
risk management, OCTAVE, OCTAVE FORTE, enterprise risk management, ERM	106

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL