



## 7-Risk Management

### Cybersecurity Assessment Tool for Transit (CATT) Welcome

The Cybersecurity Assessment Tool for Transit (CATT) is designed to provide transit agencies with an on-ramp to begin identifying and building foundational elements of a cybersecurity program. CATT incorporates the guidance of the Cyber Resilience Review (CRR) and the National Institute of Standards and Technology cybersecurity framework, but takes the additional steps of tailoring the assessment process to transit organizations that would benefit from more introductory materials and transit-aware guidance.

Each of the existing ten CRR Supplemental Resource Guides provides detailed guidance for the CRR process areas and are excellent assets for any transit organization building out the fundamentals of their cybersecurity practices. To complement CATT, each CRR Resource Guide has additional CATT- and transit-relevant resources from the American Public Transportation Association (APTA), Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), and other beginner-friendly cyber resource guides.

Risk Management CATT Resources:

- NIST in 2019 published a [report](#) on managing the cyber and privacy risks stemming from the internet of things (IoT). This report offers a helpful overview of IoT in general and how to establish risk mitigation goals inclusive of IoT devices.
  - National Institute of Standards and Technology, U.S. Department of Commerce, 2019, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, <https://doi.org/10.6028/NIST.IR.8228>. Accessed 29 Mar. 2022.
- An APTA [report](#) on risk assessment methodology provides more transit-specific guidance.



# CRR Supplemental Resource Guide



Volume 7

## **Risk Management**

Version 1.1

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT® and OCTAVE® are registered marks of Carnegie Mellon University.

DM-0003282

# Table of Contents

<b>I. Introduction .....</b>	<b>1</b>
Series Welcome.....	1
Audience.....	3
<b>II. Risk Management.....</b>	<b>4</b>
Overview.....	4
Risk Management Process .....	6
Identify Risks .....	6
Analyze Risks and Assign Disposition .....	7
Control Risks .....	7
Monitor and Improve Risk Management Processes .....	8
Plan for Risk Management.....	8
Create a Risk Management Plan .....	9
Implement the Risk Management Plan .....	9
Monitor and Improve Operational Risk Management.....	9
<b>III. Create a Risk Management Plan .....</b>	<b>10</b>
Before You Begin.....	10
Step 1. Obtain support for operational risk management planning. ....	11
Step 2. Establish the risk management strategy.....	12
Step 3. Establish a process for managing operational risk documentation.....	18
Step 4. Prepare to implement the risk management strategy. ....	19
Step 5. Establish a risk communication process.....	21
Output of Section III .....	23
<b>IV. Implement the Risk Management Plan .....</b>	<b>24</b>
Before You Begin.....	24
Step 1. Assign responsibility for implementing the plan.....	25
Step 2. Provide training on the operational risk management plan.....	25
Step 3. Establish a risk identification process.....	26
Step 4. Establish a risk analysis process.....	27
Step 5. Establish a risk disposition assignment process.....	29
Step 6. Establish a risk mitigation and control process.....	31
Step 7. Establish a risk monitoring process.....	33
Step 8. Implement risk mitigation and monitoring.....	34
Step 9. Communicate risk mitigations.....	35
Output of Section IV .....	36
<b>V. Monitor and Improve Operational Risk Management .....</b>	<b>37</b>
Before You Begin.....	37
Step 1. Oversee the risk program processes to ensure its objectives are met. ....	37
Step 2. Identify updates and improvements to the risk management plan.....	38
Step 3. Proactively monitor and report on risk mitigation activities.....	39

Step 4. Improve the risk management plan. ....	39
Output of Section VI.....	40
<b>VI. Conclusion .....</b>	<b>41</b>
<b>Appendix A. Example Operations Risk Management Policy Template .....</b>	<b>43</b>
<b>Appendix B. Simple Risk Register Template .....</b>	<b>44</b>
<b>Appendix C. Example Risk Scoring Matrix .....</b>	<b>45</b>
<b>Appendix D. Example Risk Analysis and Disposition Worksheet .....</b>	<b>46</b>
<b>Appendix E. Example Risk Parameter Template .....</b>	<b>47</b>
<b>Appendix F. Example Reporting Templates .....</b>	<b>48</b>
<b>Appendix G. Example Metrics.....</b>	<b>49</b>
<b>Appendix H. Risk Register Variables and Data to Consider .....</b>	<b>51</b>
<b>Appendix I. Risk Management Resources .....</b>	<b>52</b>
<b>Appendix J. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference .....</b>	<b>55</b>
<b>Endnotes.....</b>	<b>57</b>



## I. Introduction

### Series Welcome

Welcome to the CRR Supplemental Resource Guide series. This document is 1 of 10 resource guides developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP) to help organizations implement practices identified as considerations for improvement during a Cyber Resilience Review (CRR).<sup>1</sup> The CRR is an interview-based assessment that captures an understanding and qualitative measurement of an organization's *operational resilience*, specific to IT operations. Operational resilience is the organization's ability to adapt to risk that affects its core operational capacities.<sup>2</sup> It also highlights the organization's ability to manage operational risks to critical services and associated assets during normal operations and during times of operational stress and crisis. The guides were developed for organizations that have participated in a CRR, but any organization interested in implementing or maturing operational resilience capabilities for critical IT services will find these guides useful.

The 10 domains covered by the CRR Resource Guide series are

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
- 7. Risk Management**
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

⇌ *This guide*

The objective of the CRR is to allow organizations to measure the performance of fundamental cybersecurity practices. DHS introduced the CRR in 2011. In 2014 DHS launched the Critical Infrastructure Cyber Community or C<sup>3</sup> (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). The NIST CSF provides a common taxonomy and mechanism for organizations to

1. describe their current cybersecurity posture
2. describe their target state for cybersecurity
3. identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. assess progress toward the target state

5. communicate among internal and external stakeholders about cybersecurity risk

The CRR Self-Assessment Package includes a correlation of the practices measured in the CRR to criteria of the NIST CSF. An organization can use the output of the CRR to approximate its conformance with the NIST CSF. It is important to note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may fall short of, or exceed, corresponding practices and capabilities in the NIST CSF.

Each Resource Guide in this series has the same basic structure, but each can be used independently. Each guide focuses on the development of plans and artifacts that support the implementation and execution of operational resilience capabilities. Organizations using more than one resource guide will be able to leverage complementary materials and suggestions to optimize their adoption approach. For example, this Risk Management guide describes the creation and documentation of risk tolerance thresholds, which can be used to inform activities described in the Controls Management guide. Other examples of materials that can be leveraged between guides include the scoping of specific implementation activities and the identification of key stakeholders.

Each guide derives its information from best practices described in a number of sources, but primarily from the CERT® Resilience Management Model (CERT®-RMM).<sup>3</sup> The CERT-RMM is a maturity model for managing and improving operational resilience, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute (SEI). This model is meant to

- guide the implementation and management of operational resilience activities
- converge key operational risk management activities
- define maturity through capability levels
- enable maturity measurement against the model
- improve an organization's confidence in its response to operational stress and crisis

The CERT-RMM provides the framework from which the CRR is derived—in other words, the CRR method bases its goals and practices on the CERT-RMM process areas. See Appendix J for a cross reference between the CRR and this guide.

This guide is intended for organizations seeking help in establishing a risk management process for operations depending on information technology (IT) and for organizations seeking to improve their existing operations risk management process. More specifically this guide

- educates and informs readers about the risk management process
- promotes a common understanding of the need for a risk management process
- identifies and describes key practices for risk management
- provides examples and guidance to organizations wishing to implement these practices

Additionally, Appendix J provides a mapping between the practices that constitute the Risk Management domain in the CRR and the appropriate Function, Category, and Subcategory in the NIST CSF.

The guide is structured as follows:

- I. Introduction—Introduces the *CRR Resource Guide* series and describes the content and structure of these documents.
- II. Risk Management—Presents an overview of the risk management process for IT-dependent organizations and establishes some basic terminology.

---

<sup>3</sup> CERT® is a registered mark owned by Carnegie Mellon University.

- III. Create a Risk Management Plan—Outlines a strategy and plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization’s risk management needs.
- IV. Implement the Risk Plan—Outlines the process for ensuring that the organization’s risk management plan is implemented and meets the standards set by the organization.
- V. Monitor and Improve Operational Risk Management—Outlines the process and considerations for keeping the risk management process resilient and robust.
- VI. Conclusion—Provides a summary of risk management references for further information.

#### Appendices

- A. Example Operations Risk Management Policy Template
- B. Simple Risk Register Template
- C. Example Risk Scoring Matrix
- D. Example Risk Analysis and Disposition Worksheet
- E. Example Risk Parameter Template
- F. Example Reporting Templates
- G. Example Metrics
- H. Risk Register Variables and Data to Consider
- I. Risk Management Resources
- J. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

## Audience

The principal audience for this guide includes individuals responsible for managing risk management programs for IT operations, including executives who establish policies and priorities for risk management, managers and planners who are responsible for converting executive decisions into action plans, and operations staff who implement those operational risk management plans.

*To learn more about the source documents for this guide and for other documents of interest, see Appendix I.*



## II. Risk Management

***“Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.” DHS Risk Lexicon, 2010 Edition<sup>4</sup>***

### Overview

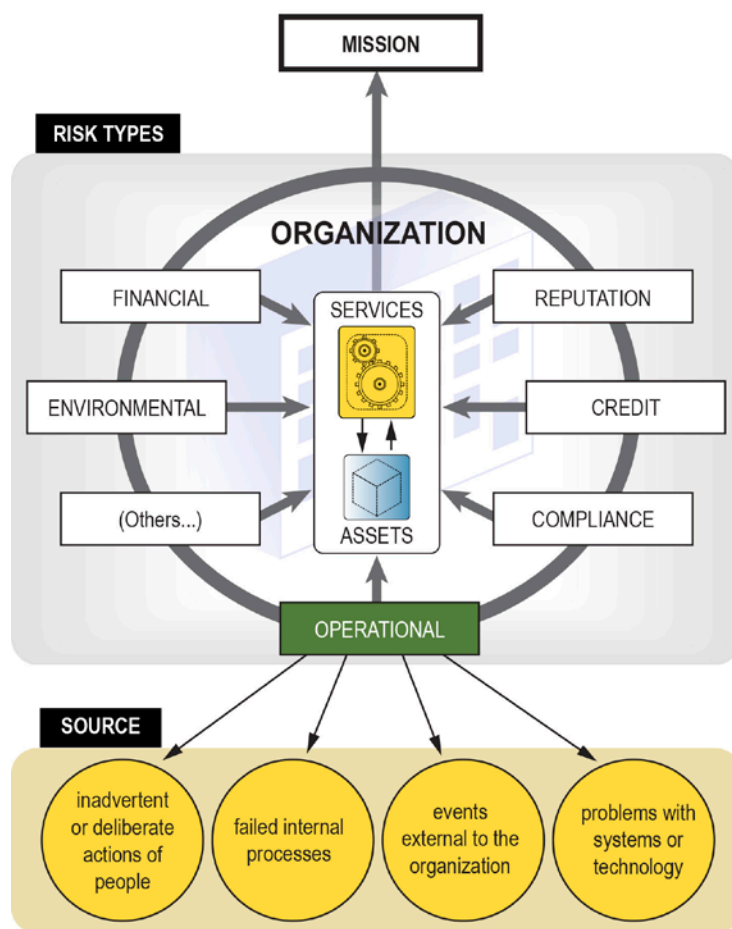


Figure 1: Types of Risks That Organizations Manage

The risk management domain focuses on the processes by which an organization identifies, analyzes, and mitigates risks in order to affect the probability of their realization and/or the impact of a disruption. It is a foundational activity for any organization and is practiced at all levels of the organization, from the executives down to individuals within business units. Organizations must manage many different types of risk (see Figure 1) to remain effective and achieve their objectives. Many organizations are moving toward more comprehensive programs, typically known as *enterprise risk management*, that address all these various

aspects of risk. This guide focuses on risks to IT-dependent operations that have the potential to interrupt delivery of a critical service. While the guide focuses on *operational risk*, it is important to note that operation risk management requires a comprehensive approach to be effective. The pervasiveness of the threats to information and the dynamics of today's global operational environment require ongoing collaboration facilitated by two-way internal and external communication.

*In this guide, risk refers to operational risk to IT-dependent assets and services.*

Operational risks emanate from a diverse and dynamic population of threats that may be natural or man-made in origin. Threats can negatively affect the organization's assets, including people, information, technology, and facilities, in a way that impacts the organization's ability to meet its objectives. The number of threats is vast, and the dynamics of those threats are increasingly complex. Identifying and prioritizing risks that may affect the organization's ability to deliver its most essential services and objectives is foundational to developing effective mitigation and disposition strategies.

**"Threat** is a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property." DHS Risk Lexicon, 2010 Edition<sup>5</sup>

An organization's capability to manage its operational risks has an impact on its operational resilience. Operational resilience is an organization's ability to adapt to risk that affects its core operational capacities, and it depends on effective operational risk management. Consider an organization that is not able to manage the risk of a disruption to one of its operational assets (people, facilities, information, and technology). Disruption of an asset's ability to support a critical service—the realization of an operational risk—may cause the service to be unable to achieve its mission, reducing operational resilience (Figure 2). Organizations that are better at managing their operational risks are more likely to achieve their operational resilience goals.<sup>6</sup>

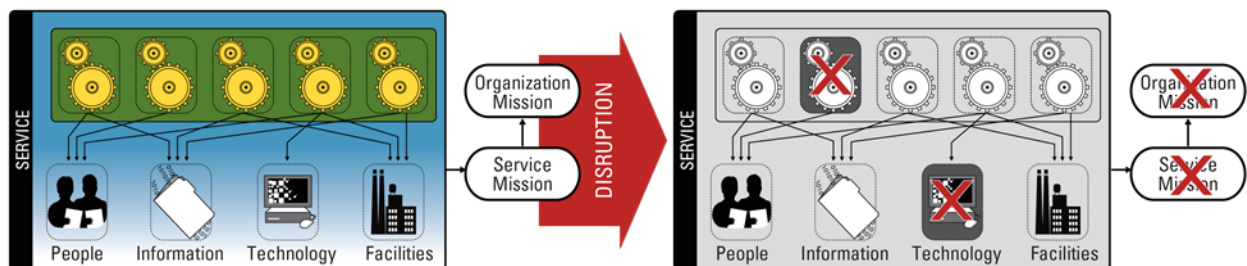


Figure 2: Disruption

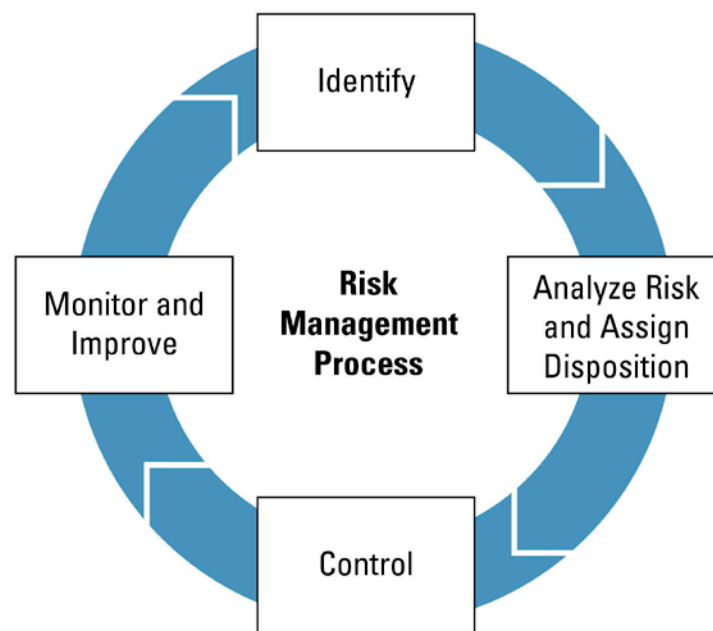
Organizations must identify the operational risks to which they are exposed and analyze them to determine the extent to which they might impact their mission. Once this is accomplished, these risks must then be dealt with (e.g., avoided, accepted, monitored, transferred, or mitigated) in a way that is commensurate with the organization's risk tolerances. This requires an approach that balances strategies for protecting assets from disruption against strategies for sustaining assets and services when a disruption occurs. For example, if the cost of preventing a certain type of disruption to an asset is significantly higher than the cost of restoring that asset once a disruption occurs, then an organization may choose to invest only in recovering the asset. The cost of the disruption must also be factored into the analysis. For example, if the cost of the disruption itself is less than the cost of implementing controls to protect or sustain the asset, then the organization might consider just accepting the risk of that particular type of disruption.

*Risk tolerance is the degree to which an organization or entity is willing to accept risk. An organization with a high risk tolerance is willing to accept more risk than an organization with a low risk tolerance. An organization's risk tolerance is derived from its business drivers, market position, competitive environment, role in critical infrastructure, and other factors.*

This guide provides suggestions regarding the management of operational risks to IT-dependent critical services and the assets that support them. To effectively manage operational risk, organizations should establish processes that

- identify risks to which the organization is exposed
- analyze risks and determine appropriate risk disposition
- control risks to reduce probability of occurrence and/or minimize impact
- monitor risks and responses to risks and improve the organization's capabilities for managing current and future risks

Figure 3 depicts the risk management process.



*Figure 3: The Risk Management Process*

The following sections detail each of the steps in the risk management process.

## **Risk Management Process**

### **Identify Risks**

The identification of risks is a foundational risk management activity; an organization will have difficulty successfully managing its risks if it does not understand what they are. Organizations need to ensure they have the ability to identify risks in a timely manner and then communicate those risks to the appropriate stakeholders.

Important activities in risk identification include the following:

- Establish categories for risk.
- Identify risk stakeholders.

- Identify sources of risk to operations dependent on technology and information assets.
- Log identified risks in a risk register or other tracking mechanism, which provides a means to organize and record information on identified operational risks.

*Key data used during the risk identification, analysis and disposition, control, and monitoring and improving processes should be organized in a common location. Typically organizations refer to this operational risk data management tool as a risk register. See Appendix B and Appendix H for more information.*

## Analyze Risks and Assign Disposition

Risk analysis allows an organization to understand a risk's potential impact on its mission and to develop appropriate strategies and responses. Risk analysis and disposition assignment focus on identifying and selecting appropriate risk response strategies. Risk analysis begins by assessing and prioritizing identified risks based on their potential impacts, likelihood of occurrence, and potentially other factors. The probability of occurrence and the areas of impact are unique to each organization. Many factors can affect risk analysis and disposition, including infrastructure sector, location, organizational structure, mission requirements, and laws and regulations. For example, a technical issue that leads to a two-day disruption of service may be an unacceptable outcome for some organizations, but for others it might be an acceptable inconvenience because the disruption's impact is minimal. A two-day outage of a web service for an online retailer might have a significant impact on its reputation and sales numbers whereas that same outage for a heavy industry organization might have almost no impact on its reputation and sales numbers.

Once an organization recognizes, analyzes, and categorizes a risk, it determines the appropriate disposition of the risk (common dispositions include avoid, accept, monitor, transfer, and mitigate) and response activities. Some organizations may have specific risk disposition assignment and response strategies they apply to certain categories of risk, and others may develop a unique strategy for each identified risk. Disposition assignment and response strategies should be developed in the context of other risks and other areas of the organization to determine whether a more comprehensive or efficient strategy can be developed. Many organizations have established enterprise risk management and operational risk management functions to facilitate the interactions and correlations of risk within an organization.

*Common dispositions of risks include avoid, accept, monitor, transfer, and mitigate.*

Important activities in the risk analysis and disposition assignment include the following:

- Establish and prioritize impact areas for risk.
- Establish risk tolerance parameters for each impact area.
- Establish risk tolerance thresholds for each risk category.
- Analyze identified risks to determine potential operational impacts.
- Categorize and prioritize identified risks based on operational impact and risk tolerance thresholds.
- Assign a disposition to all identified risks.
- Update risk register or other tracking mechanism with analysis and disposition information.

## Control Risks

Controlling risk requires that an organization design and implement a control process that reduces the likelihood of risks and their impact should they be realized. Risk management strategies should be developed that ensure that risks are reduced to an acceptable level, in other words, within established operational risk thresholds. The control process is the aggregation of the organization's activities designed to ensure its risks

are managed in a manner that allows it to meet its mission. The process includes operational activities focused on establishing risk controls as well as broader objectives that include managing fraud, unethical behavior, and compliance. Plans must be established to implement the control process, and owners of those control areas must be engaged to manage actions required to implement and monitor the control process and effectiveness.

In some cases, these actions will be simple adjustments to the current control environment. In other cases, the organization may need to design and implement new control strategies, which may be very costly. Because not all risk can be mitigated, organizations may ultimately choose to accept some risks. No matter how an organization chooses to deal with a risk, it should establish processes that track and address all operational risks, including residual risks.

Organizations design solutions for managing and controlling risks based on available resources (e.g., financial and technological) and risk tolerances; compliance with regulation sometimes also plays a role. The implementation of controls is often managed separately from the risk management function, usually by an organization's operational or technology controls management process.

*See the Controls Management Resource Guide, Volume 2 of this series, for detailed guidance on operational risk controls. Also see the External Dependencies Management process area in the CERT-RMM for additional information on managing the controls implementation process.<sup>7</sup>*

Important activities in controlling risks include the following:

- Develop plans for managing identified operational risks.
- Communicate plans and status to stakeholders.
- Validate risk management plans to ensure alignment with organizational risk tolerances and compliance requirements.
- Develop mitigation plans for risks that the organization designates.
- Track identified risks to closure.

### **Monitor and Improve Risk Management Processes**

Maintaining an effective operational risk program requires more than identifying risks, putting controls in place, and adding new controls over time. There must be a variety of supporting activities to monitor and improve the program. These activities include ensuring that the operational risk management processes are communicated and monitored for quality and effectiveness, and that coordination and collaboration with both internal and external stakeholders occur. Effective operational risk management can be seen as an iterative process improvement activity that requires frequent tuning and proactive collaboration to be successful.

Important activities in monitoring and improving risk management include the following:

- Track the status of existing, new, and potential future risks.
- Measure and report on risk mitigation efforts to determine if they are achieving the intended results.
- Establish linkages to the organization's other risk management activities (e.g., enterprise, credit, market, reputational).
- Coordinate and collaborate with external entities (e.g., regulators, service providers, business partners).

### **Plan for Risk Management**

Having a defined process for identifying, analyzing, responding to, and learning from events that may interrupt an organization's IT-dependent operations provides the basis for effective operations risk management.

Without a defined process, an organization's risk management efforts might fail to sufficiently address risks that can materially affect the organization's ability to efficiently deliver services. A risk management plan describes the organization's strategy for identifying, analyzing, controlling, and monitoring risk. The objective of the plan should be translated into specific actions assigned to individuals or groups to perform and manage. The risk management plan should be a collaborative program that addresses, at a minimum,

- the organization's approach to risk management
- the provision of adequate financial and organizational resources
- the structure of the risk management process
- the requirements and objectives of the risk management process
- a description of how the organization will identify risk, analyze risk, develop plans to mitigate risks, and monitor and improve its risk management capabilities over time
- the roles and responsibilities necessary to carry out the plan
- applicable training needs and requirements

The following sections of this guide lay out discrete steps for developing a plan to implement the risk management process for IT-dependent operations as described above.

### **Create a Risk Management Plan**

1. Obtain support for operational risk management planning.
2. Establish the risk management strategy.
3. Establish a process for managing operational risk documentation.
4. Prepare to implement the risk management strategy.
5. Establish a risk communication process.

### **Implement the Risk Management Plan**

1. Assign responsibility for implementing the plan.
2. Provide training on the operational risk management plan.
3. Establish a risk identification process.
4. Establish a risk analysis process.
5. Establish a risk disposition assignment process.
6. Establish a risk mitigation and control process.
7. Establish a risk monitoring process.
8. Implement risk mitigation and monitoring.
9. Communicate risk mitigations.

### **Monitor and Improve Operational Risk Management**

1. Oversee the risk program processes to ensure their objectives are met.
2. Identify updates and improvements to the risk management plan.
3. Proactively monitor and report on risk mitigation activities.
4. Improve the risk management plan.

Organizations that already have an operational risk management plan can use the guidance in this Resource Guide to assess and make improvements to their existing processes.

### III. Create a Risk Management Plan

#### Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin developing a risk management plan.

*In this guide, risk refers to operational risk to IT-dependent assets and services.*

	Input	Guidance
✓	Scoping statement	This statement defines what the risk management plans intend to address. The risk management plan could be scoped to cover a single service and the assets (e.g., the people, information, technology, and facilities) that support it, or it could cover all mission-essential organizational services. It is recommended that organizations that are not sure where to start begin with one of their essential services and the assets that directly affect its performance. This approach can allow an organization to begin addressing risk in areas most important to achieving the organizational mission and begin mitigating their impact while risk management practices are being more fully developed. If your organization has participated in a CRR, it may be beneficial to begin with the essential service addressed during the CRR.
✓	Lists of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include <ul style="list-style-type: none"><li>• service/business owners within the organization</li><li>• business partners and vendors</li><li>• technology and infrastructure owners in the organization</li><li>• law enforcement and other first responder organizations</li><li>• technology vendors</li><li>• regulators and auditors</li><li>• customers and providers who may be impacted in the event of service interruption</li></ul>
✓	Management support	<ul style="list-style-type: none"><li>• An endorsement by senior management for establishing a risk management plan, risk management program, and the implementation of the processes. This often appears in the form of a policy statement.</li></ul>
✓	Guidance from senior leadership and stakeholders on risk tolerance and resource commitments	<ul style="list-style-type: none"><li>• Preliminary/basic assessment of perceived key risks</li><li>• Initial prioritization of key risks and suggested timelines for resolution</li><li>• Outline of financial and human resources that could be used for risk management</li><li>• Key business objectives where risk management activities should focus</li></ul>
✓	Externally imposed requirements for risk management	<ul style="list-style-type: none"><li>• Regulatory requirements defining mandatory risk management requirements and other needs. Sources for that guidance could include<ul style="list-style-type: none"><li>○ Legal</li><li>○ Audit</li><li>○ Compliance</li><li>○ Regulatory documents (e.g., NERC, FERC, FFIEC, FTC, HIPPA)</li></ul></li><li>• Service-level agreement (SLA) requirements with other organizations where risk management planning and collaborative interaction is required</li></ul>



	Input	Guidance
✓	Assignment of responsibility for developing the risk management plan	<ul style="list-style-type: none"> <li>• Explicit mapping between roles and responsibilities in the organization and the risk management process</li> <li>• Explicit acknowledgement of risk ownership and sign-off responsibilities</li> </ul>
✓	Budget for risk management planning	<ul style="list-style-type: none"> <li>• Identification of available funds and resources to perform risk management planning <ul style="list-style-type: none"> <li>○ staffing resources</li> <li>○ tools (applications and associated hardware)</li> <li>○ third-party support</li> <li>○ technology to support resilience requirements</li> </ul> </li> </ul>
✓	Linkage to other organizational risk management activities and plans	<ul style="list-style-type: none"> <li>• Coordination of broader enterprise risk management processes with operational risk management planning, execution, and monitoring</li> <li>• Communication to risk stakeholders (i.e., audit, compliance, business partners, regulators) to gather support, expertise, and engagement</li> </ul>

### Step 1. Obtain support for operational risk management planning.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A strategy for identifying, analyzing, and mitigating risks is developed.</b>	
3. Has a plan for managing operational risk been established? [RISK: SG1.SP2]	ID.GV-4: Governance and risk management processes address cybersecurity risks. ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

Management support and participation is an essential requirement for an operational risk management strategy to be effective. A strategy lacking appropriate support is unlikely to be successfully implemented. The level of management support required depends on the scope of the strategy being developed. Smaller implementations, such as a strategy focused on a single critical service, may require sponsorship from only the senior management responsible for that particular service. A strategy being developed to cover an entire enterprise is likely to require much broader support and a more extensive resource commitment. Ensuring that the scope of the risk plan is clearly defined and communicated to key stakeholders can be a valuable step in managing the process and gaining traction for longer term support of the risk program.

*It is highly recommended that organizations that have not previously developed operational risk management strategies and plans should start by developing a plan for a single critical service. Lessons learned from that effort could inform the development of additional plans and the development of an organization-wide operational risk management program.*

When considering organization-wide risk management strategy, it may be useful to look to very high-level areas of risk where the impacts could be large and the probability of occurrence is also high. For example, an organization that is extremely dependent on access to its customer data may want to initially focus its risk program on protecting the systems that house that data. It may want to raise the priority of the controls and mitigations currently in place to prevent a data breach or the lack of availability of that data due to a data center outage or failure of the networks used to access that customer data. It may also want to increase the capability and depth of those controls.

For a plan that covers an entire organization, support and commitment from executives and leaders from across the organization are essential. This might include

- executives and senior leaders who provide oversight, define the risk management strategy, and set program objectives



- managers and leaders who can translate the program strategy and objectives into detailed plans
- operations managers who can actively oversee the day-to-day implementation and ongoing operational processes, which are essentially the front-line defense against disruptions and risk
- other organizational risk management programs

A common way for organizations to demonstrate support is to create policy that requires and/or defines risk management activities and assigns responsibility for their completion. See Appendix A for an example risk management policy template.

*Ensuring that there is support and engagement from across the organization is a foundational element of effective operational risk management activities, making support and commitment essential to establishing a strong program.*

## Step 2. Establish the risk management strategy.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A strategy for identifying, analyzing, and mitigating risks is developed.</b>	
1. Have sources of risk that can affect operations been identified? [RISK: SG1.SP1]	ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
2. Have categories been established for risks? [RISK: SG1.SP1]	ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
3. Has a plan for managing operational risk been established? [RISK: SG1.SP2]	ID.GV-4: Governance and risk management processes address cybersecurity risks. ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.
<b>Goal 2: Risk tolerances are identified, and the focus of risk management activities is established.</b>	
1. Have impact areas been identified, such as reputation, financial health, and regulatory compliance? [RISK: SG2.SP2]	ID.RA-4: Potential business impacts and likelihoods are identified. RC.CO-2: Reputation after an event is repaired.
2. Have impact areas been prioritized to determine their relative importance? [RISK: SG2.SP2]	ID.RA-4: Potential business impacts and likelihoods are identified. ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
3. Have risk tolerance parameters been established for each impact area? [RISK: SG2.SP2]	ID.RM-2: Organizational risk tolerance is determined and clearly expressed. ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.
4. Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK: SG2.SP1]	ID.RM-2: Organizational risk tolerance is determined and clearly expressed. ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis. RC.CO-2: Reputation after an event is repaired.

The risk management strategy defines a common approach for the performance of operational risk management activities. An effective risk management strategy supports an organization's ability to make business decisions within the context of the potential for the realization of risk and the negative impacts that may result. For example, a new business opportunity that relies on cutting-edge software may favor early entry with the potential to generate significant new business and revenue. Should the organization enter the market quickly and risk the potential for cybersecurity issues due to oversights in the software's security controls

design? Will delays in entering the market and the cost of strong cybersecurity controls eliminate or reduce the benefit of the new business opportunity? An organization's risk management strategy should establish a risk management process that can respond to change and avoid making ad hoc decisions on operational risk that can lead to unforeseen impacts or ineffective or inefficient responses.

A well-designed risk management strategy draws on informed decision makers who proactively consider the risks and define the path forward based on a clearly documented risk management process. The risk program can be extensive, or it may be simply a few leaders coordinating a defined strategy. Regardless of size, successful risk programs set clear objectives, employ a collaborative communications process, and use systematic decision making that reflects an established organizational strategy.

The development and maintenance of a risk management strategy is an iterative effort. Establishing a risk management strategy begins with scoping, training, identifying potential risk sources, and establishing risk impact thresholds. The strategy should also include assignment of responsibilities and define approaches for activities such as risk identification. The strategy will typically evolve as the plans for risk identification, risk analysis, and other activities are developed. Organizations that have other risk management programs (e.g., enterprise risk, credit risk, market risk, privacy risk, or reputation risk) should seek to leverage their experience, vocabulary, and outputs.

An operational risk management strategy should define the following:

- the scope of the risk management activities
- how operational risks sources and categories are defined
- how risk parameters (e.g., impact areas and thresholds) are determined
- the responsibilities and training requirements for risk management
- how risk information will be recorded and tracked
- time intervals for strategy reviews and updates

*Using a consistent risk vocabulary throughout the organization is important to the success of risk management activities. An operational risk management process whose outputs do not align with the outputs of other enterprise risk management activities will create boundaries to understanding and acceptance throughout the organization, often with senior management. The DHS Risk Lexicon<sup>8</sup> is a resource for organizations seeking to establish a common risk vocabulary.*

**A. Establish the scope of operational risk management activities.** The scope of the operational risk management activities is defined by the critical assets and services that the strategy will address. To ensure that the strategy is properly scoped, it is important to understand the linkage between asset types (e.g., people, information, technology, and facilities) and the critical service(s). If the scope of a strategy being developed is for a single critical service, the scope should include that service and all the assets that support its delivery. If a strategy covers multiple services or the entire organization, then the scope should include all of the critical assets that support the services that are in scope.

For example, an electric utility may identify electricity generation as a critical service and decide to develop an operational risk management strategy for that particular service. The company needs to consider the assets that support this critical service, such as the engineers and operators who maintain the supervisory control and data acquisition (SCADA) system, the SCADA system set points, the SCADA hardware and software, and the plant housing the control system. Figure 4 illustrates this relationship between a critical service and its underlying assets.

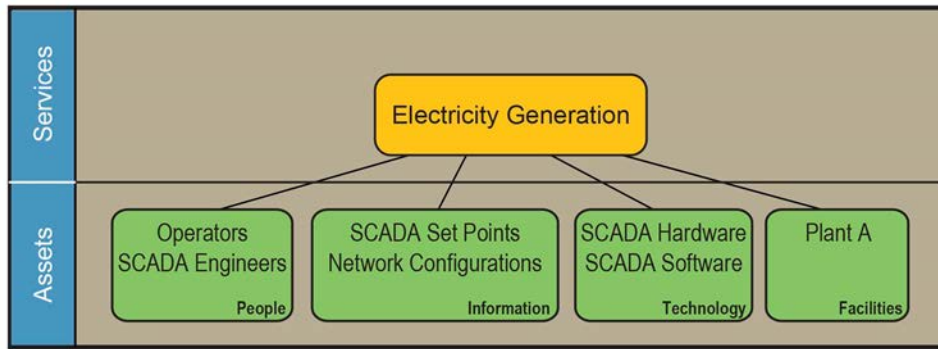


Figure 4: Service and Asset Relationships

- i. **Identify and document services and assets that are in scope.** This information should be regularly revisited as the assets supporting the service evolve.
- ii. **Validate scope of operational risk management strategy with relevant stakeholders.**

*The Asset Management Resource Guide, Volume 1 of this series, has more information on identifying assets and their resilience requirements and establishing mappings between assets and services.*

**B. Define risks sources and categories.**<sup>9</sup> A common way of considering the threat landscape is to identify sources of risks/threats. This approach facilitates the grouping of risks into categories that may share common traits, tactics, and trends. For example, the analysis of various risks can be categorized as natural or manmade. Those categories can then be more efficiently analyzed to identify common trends, characteristics, likelihood, and impact. Natural risks in particular lend themselves to valuable analytics based on historical trends or the use of related predictive indicators (e.g., temperature changes, ocean current variations, seismic trends). Man-made risks are often analyzed from a “threat actor” perspective to understand the reason or motivation for the action (i.e., financial, competitive, human error, malicious).

Identifying a common set of risk sources helps to ensure that risk identification activities comprehensively consider the risk landscape and that the development of risk categories supports the analysis and mitigation process. Grouping similar types of risk together into categories facilitates the development of mitigation strategies and control design.

- i. **Identify and document the sources of operational risk.** Stakeholders in the operational risk management process should be included in the development of this list and should review final outputs.

Risks should be bounded by the scope of the risk management plan. Including sources of risk outside the scope can lead to unnecessary resource expenditures.

Reviewing the organization’s historical experience with negative operational events can be a good first step toward the identification of risk sources. Useful data on sources of operational risk can often be found in incident and service continuity data.

Some common sources of internal and external operational risks can be found in Table 1. An organization could start with this list and then customize it based on the scope of its risk management activities and unique operating environment.

Table 1: Common Sources of Internal and External Operational Risks

Common Risk Sources	
Source	Example
Poorly designed business processes and services	Individual assigned for monitoring account permissions is the same person who assigns them.
Incorrectly implemented/executed business processes and services	There is a policy establishing password complexity and length rules, but not controls to enforce it.
Intentional actions of people	A disgruntled employee deletes customer files.
Inadvertent/accidental actions of people	An employee fails to close the door to the computer room.
System failures	Web service fails because of unexpected loading.
Hardware failures	Router stops functioning because power supply fails.
Software failures	Software crashes because of design fault.
External dependency failures	Electricity is out for an extended period.
Natural disasters	A hurricane halts business.

- ii. **Identify and document operational risk categories.** Risk categories are created by organizing the identified risk sources into related groupings and are used to support the identification of control strategies and risk mitigations. A common way to categorize risks is by their source. Alternatively, risks could be categorized by the assets they are most likely to affect, for example, risks to availability of people, confidentiality of information, or availability of a facility. They could also be aligned by the services they affect or some other common characteristic. The right choice of categories and their associated granularity are highly dependent on the organization's unique environment. Table 2 provides an example of operational risks grouped by sources. If there are too many categories, make the categories more generic. If the risk categories do not help differentiate the control strategies that will be used to address them, then it is likely that the number of risk categories can be reduced.

Stakeholders in the operational risk management process should be included in the development and refinement of the risk category lists.

Table 2: Risk Categories Example

Actions of People	Systems and Technology Failures	Failed Internal Processes	External Events
<b>1. Inadvertent</b> 1.1 Mistakes 1.2 Errors 1.3 Omissions  <b>2. Deliberate</b> 2.1 Fraud 2.2 Sabotage 2.3 Theft 2.4 Vandalism  <b>3. Inaction</b> 3.1 Skills 3.2 Knowledge 3.3 Guidance 3.4 Availability	<b>1. Hardware</b> 1.1 Capacity 1.2 Performance 1.3 Maintenance 1.4 Obsolescence  <b>2. Software</b> 2.1 Compatibility 2.2 Configuration management 2.3 Change control 2.4 Security settings 2.5 Coding practices 2.6 Testing  <b>3. Systems</b> 3.1 Design 3.2 Specifications 3.3 Integration 3.4 Complexity	<b>1. Hardware</b> 1.1 Process flow 1.2 Process documentation 1.3 Roles and responsibilities 1.4 Notifications and alerts 1.5 Information flow 1.6 Escalation of issues 1.7 Service-level agreements 1.8 Task hand-off  <b>2. Process controls</b> 2.1 Status monitoring 2.2 Metrics 2.3 Periodic review 2.4 Process ownership  <b>3. Supporting processes</b> 3.1 Staffing 3.2 Funding 3.3 Training and development 3.4 Procurement complexity	<b>1. Disasters</b> 1.1 Weather event 1.2 Fire 1.3 Flood 1.4 Earthquake 1.5 Unrest 1.6 Pandemic  <b>2. Legal issues</b> 2.1 Regulatory compliance 2.2 Legislation 2.3 Litigation  <b>3. Business issues</b> 3.1 Supplier failure 3.2 Market conditions 3.3 Economic conditions  <b>4. Service dependencies</b> 4.1 Utilities 4.2 Emergency services 4.3 Fuel 4.4 Transportation

**C. Identify and document operational risk parameters.** The organization's risk management strategy must provide a means of prioritizing operational activities and processes into those that are managed and those that are of less importance and require lower levels of focus. Risk parameters define measurement criteria and tolerance thresholds that provide a means of identifying which risks should get the most attention and trigger more extensive operational risk analysis and disposition assignment activities. By documenting these parameters in the risk management strategy, the organization has greater assurance that common and consistent criteria will be used for evaluating risk. Appendix E contains a template for capturing the risk parameters.

- i. **Identify and document organizational impact areas.** An impact area describes a realized risk that is meaningful to the organization. Business impact assessments (BIA) often contain useful information for identifying these areas. (See the *Service Continuity Resource Guide*, Volume 6 of this series, for more information on BIAs.) These should be aligned to the scope of the risk management strategy. For example, if the strategy covers a single service, the areas of impact should be related to that service. Some examples of organizational impact areas include
  - o reputation and customer confidence
  - o financial health and stability
  - o safety and health of staff and customers
  - o fines and legal penalties
  - o regulatory noncompliance
- ii. **Prioritize organizational impact areas.** This establishes the relative importance of each impact area to the organization and can be used to support the risk analysis and disposition assignment

activities. For some critical services, the issue of regulatory noncompliance may be more important than reputation and customer confidence.

- iii. **Identify and document operational risk impact thresholds.** Risk thresholds define the levels or points at which an organization will take different actions because of the realization of a risk. For example, the organizational impact of one realized risk might be a single noncompliance event that the organization can quickly identify and resolve, but the impact of another risk might be a noncompliance event that results in a fine and additional reporting requirements. The organization is unlikely to deal with those risks in the same way. They may simply accept the risks that cause an impact they can easily deal with, and they may put controls in place to prevent the realization of risks that result in fines and increased reporting requirements.

Many organizations simply create high, medium, and low thresholds for impact areas at first. There does seem to be a diminishing return with respect to effort when organizations go beyond establishing more than four or five threshold levels.

Thresholds should be captured for each identified impact area and establish a means for measuring risk. Thresholds should be as specific to the scope of the risk analysis as possible. See Table 3 for an example.

- iv. **Review risk parameters and prioritization with senior management.** Thresholds and priorities should align with the organization's strategic objectives, critical success factors, and risk appetite.

*Table 3: Example Impact Area with Defined Thresholds*

Impact Area: Regulatory Compliance			
<i>Critical</i>	<i>High</i>	<i>Medium</i>	<i>Low</i>
The organization remains out of compliance for more than five days. While the event is underway, the organization must report its inability to meet compliance requirements to the regulatory board, and the organization will incur fines and penalties.	The organization remains out of compliance for more than one day and less than five days. It must report its inability to meet compliance requirements to the regulatory board at the conclusion of the event.	The noncompliance event and outage lasts less than 24 hours. The noncompliance event must be included in the annual summary report to the regulatory board.	The noncompliance event occurs, but the issue is resolved before the reporting threshold of more than one hour is met.

- D. **Identify and document responsibilities for risk management.** Each risk management activity in the strategy needs to have an individual or role assigned to ensure that the activity is performed. Typically owners will be closely engaged in determining responsibilities and accountability.
- E. **Identify training requirements for strategy execution.** The organization must identify the training needs for implementing the risk management strategy. Implementation of the strategy should account for the time it will require to develop or obtain the appropriate expertise. Some organizations may need to obtain external support until internal resources can be hired and developed.
- F. **Define interval for strategy review and update.** Establish the frequency for monitoring and for broader revisits to key operational risk criteria and information, for example, identified risks, disposition assignment, controls, residual risk, and stakeholders.

### Step 3. Establish a process for managing operational risk documentation.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A strategy for identifying, analyzing, and mitigating risks is developed.</b>	
3. Has a plan for managing operational risk been established? [RISK: SG1.SP2]	ID.GV-4: Governance and risk management processes address cybersecurity risks. ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

**A. Establish a repository for risk plans, documentation, tracking, and reporting.** Effective risk management requires the ability to systematically document processes and track historical and expected risks. Establishing a common location, typically called a *risk register*, for risk tracking and documentation simplifies the implementation and management of the risk plan. This can be done by setting up a directory on a server where risk information is stored, developing a spreadsheet that has links to various risk documentation, or using a risk software tool. The risk document repository and/or software tool set should consider

- security of sensitive information
  - strategies and objectives
  - risks, controls, and threats, historical and anticipated
  - action plans
  - risk triggers and escalation plans
- integrity of information
  - policy, standards, and guidelines
  - process documentation
  - process management and improvement plans
  - compliance
  - role-based access
- access
  - real-time access to risk documentation
  - procedures for offsite or remote access if the primary location is not available
- availability and backup of the repository
  - required backup frequency<sup>10</sup>
  - alternate location if the repository is affected by a service interruption<sup>11</sup>

**B. Define a strategy for recording and tracking risk information.** Having a repository or risk register for collecting information can significantly facilitate the execution of the risk management strategy. Simply recording information in the risk register is not sufficient for managing risks.

For organizations starting to develop a risk management process for their IT operations, a simple spreadsheet can be used for a risk register. For organizations needing more sophisticated support, there are a number of commercial risk management tools that include a risk register. Organizations that have other risk management programs should consider leveraging the tools being used within those programs.

Information recorded in the risk register often includes the following:

- risk category
- risk description

- risk identifier (a unique identifier for the risk)
- risk impacts
- risk valuations
- risk analysis results
- risk mitigation decisions and plans
- internal and external stakeholders
- risk ownership

#### Step 4. Prepare to implement the risk management strategy.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A strategy for identifying, analyzing, and mitigating risks is developed.</b>	
3. Has a plan for managing operational risk been established? [RISK: SG1.SP2]	ID.GV-4: Governance and risk management processes address cybersecurity risks. ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

Compelling needs for change may drive organizations to take an aggressive approach to implementing a new risk program, but an overly aggressive approach can be problematic or too costly. There is often a steep learning curve for an organization as it matures its risk management capabilities. Organizations that are implementing a new risk management program can benefit by focusing on a few key tasks and establishing a goal of iteratively refining the program over time as staff gain experience and the organization deepens its resource investment in risk management.

Initializing implementation requires the development of detailed plans that are informed by knowledge provided by those most familiar with the day-to-day activities of the organization and operations. Gathering that information requires engaging key stakeholders and operations managers. Those stakeholders and managers may be the best owners of risk action plans that support the objectives of the overall program. While for smaller organizations this may be just a few individuals, the core concept remains the same: risk management must be understood and managed at all levels to be effective.

##### A. Manage and coordinate the implementation.

- i. **Broadly communicate the risk implementation plan and objectives.**
- ii. **Establish a process to plan, manage, and coordinate the implementation.**
- iii. **Engage business, operations, and external stakeholders and gain buy-in.**
- iv. **Track the implementation using metrics designed to measure progress, and identify improvements to the plan that may be needed.**

**B. Leverage existing processes.** Building risk identification, analysis, disposition assignment, control, and monitoring processes in the organization can be challenging when there are many new procedures or changes. An approach that can ease these challenges is to build on existing organizational processes and refine them over time to meet the evolving needs of the risk program. The headwinds that often delay progress on new initiatives result from a natural aversion to change, as well as cultures that are less risk-management oriented. Leveraging existing processes and practices can provide a starting point for overcoming those headwinds, establishing a path to building an effective risk management culture. Use of existing process can jump-start the implementation while engaging key stakeholders and building on



existing communication channels. For example, if an organization already has a reporting process for other risks that it manages, then reporting of operational risks to IT-dependent services can build on the same process. If all risks are already scored on a 1-to-5 scale, the operational risk management process could leverage that same scale to report on individual risks.

*Leveraging and building on existing organizational processes can ease the challenges of implementing new or expanded risk management plans. Use of existing processes can jump-start the implementation while engaging key stakeholders and the existing communication channels to facilitate coordination and collaboration.*

Table 4 outlines key risk program areas and examples of existing processes, activities, and expertise that may be leveraged to support their implementation.

*Table 4: Existing Resources for Use in the Risk Management Strategy*

Key Risk Program Area	Relevant Existing Resources	Example Contribution to Risk Program
Risk identification and prioritization	Insurance-based assessments	Information gathered to support insurance requirements
	Audit reports	Identified operational and IT issues to identify and prioritize risks
	IT controls	Documentation of existing controls and the risks they were designed to manage
	Budget planning process and related artifacts	Financial planning processes and activities that manage cost and risk
Risk analysis and disposition assignment	Existing credit or market risk tools and committees	Guideposts for operational risk management
	Senior leaders	Those who have experience with risk decision making, such as the Chief Financial Officer, Audit, Compliance
	BIA	Information gathered to support disaster and continuity planning
	External industry	Information on the practices of similar organizations and industry groups
	Project management	Skills for managing risk activities
Controls and monitoring	Audit teams	Skills and experience in developing control design, testing, and monitoring processes
	External audits	Information produced by external audits
	IT teams	Controls for IT failures commonly established in most organizations; for example, anti-virus tools, backup, intrusion tools and devices, and data backup and recovery can serve as the foundation of a control strategy
	Physical security	Some of the most well-established controls and risk processes form the basis of security and can be leveraged for overall risk management, for example, site security requirements, site assessments, and background checks
	Compliance teams	Processes and skills that are employed for credit, safety, security, and so on
	Reporting and governance	Process used to provide board oversight, financial reporting, audit, and compliance management

**C. Establish a risk management culture.** A longer term objective of the implementation of the risk management program should be to establish resilience and a risk management culture—a pervasive

recognition of the importance of effective risk management that positively rewards appropriate risk taking, establishes accountability, ensures employee engagement, values risk skills, and ensures ongoing refinements to continuously improve risk processes. The benefits of such a risk management culture must be balanced with the costs of the program. The challenge is finding a balance between risk and cost, which essentially defines a state of risk management efficiency (i.e., resilience).

*"An effective risk culture is one that enables and rewards individuals and groups for taking the right risks in an informed manner." Institute of Risk Management, October 2012<sup>12</sup>*

## Step 5. Establish a risk communication process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A strategy for identifying, analyzing, and mitigating risks is developed.</b>	
4. Is the plan for managing operational risk communicated to stakeholders? [RISK: SG1.SP2]	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

Effective risk management relies heavily on knowledgeable organizational resources to support the development and execution of risk strategies and plans. Moreover, the identification of realized and potential risks can be most effectively accomplished by stakeholders who are directly engaged with the delivery of services and the assets that support them. Not only do stakeholders have valuable knowledge about key services and assets, they also typically have control or influence over resources that must be provided to risk management activities. Ensuring ongoing, two-way communications between individuals responsible for making risk management decisions and stakeholders engaged in the delivery of services helps ensure that the right risks are being addressed and that the appropriate level of resources are being invested to manage those risks.

Communication is also essential to ensuring that processes are well designed and integrated into day-to-day processes in a manner that meets the objectives of the organization. Operational risk management can easily be overlooked as stakeholders focus on profits and growth. Ensuring that all members of an organization understand their roles in risk management, the objectives of the program, and their ongoing risk management responsibilities is foundational to the success of risk management programs. Establishing a risk management culture that recognizes the importance of risk management, rewards positive actions to manage risk, and facilitates accountability for results should be a primary goal of risk communications. Risk management must be recognized as vital to individual and organizational success.

*Ongoing, two-way communications between individuals responsible for making risk management decisions and stakeholders engaged in the delivery of services help ensure that the right risks are being addressed and that the appropriate level of resources is being invested to manage those risks. To remain effective, risk communications should focus on ensuring that members of an organization understand their roles in risk management, the objectives of the program, and their ongoing risk management responsibilities.*

The following steps outline a recommended approach to risk management communications.

### A. Identify stakeholders to be targeted for communications. Considerations should include

- the rationale for stakeholder involvement
- roles and responsibility of stakeholders
- relationship between stakeholders
- the importance of stakeholders in managing the risk program

**B. Develop a communication plan.** It should include

- objectives of the communications
- key risk management messages
- the extent and frequency of communications
- resources required to accomplish the objectives of risk communications
- approval process for establishing communication content
- guidelines for communications with external originations, business partners, and regulators

**C. Define communications delivery methods and channels.**

- types of communication (e.g., presentations, newsletters)
- channels to be used (e.g., email, meetings, risk forums, training)
- communication design considerations and infrastructure

**D. Develop a process to assess and improve the effectiveness of communications.**

- i. **Determine how communications results will be assessed.** Options to consider include
  - questionnaires and surveys
  - risk behavior changes that resulted from communications
  - third-party reviews and benchmarking
  - interviews with stakeholders, staff, and external entities who may have been communicated with (e.g., vendors, business partners, regulators)
- ii. **Determine if the communications were received by those targeted to receive it.**
- iii. **Assess whether the communications helped the risk program meet its objectives.**

***"Risk communication** is the exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to take appropriate actions in response to an identified risk." DHS Risk Lexicon, 2010 Edition<sup>13</sup>*

## Output of Section III

	Output	Guidance
✓	Enterprise guidance for risk management	<ul style="list-style-type: none"> <li>Organization-wide program, strategy, standards, and documentation for performing risk management activities</li> </ul>
✓	Executive endorsement and oversight of risk management planning	<ul style="list-style-type: none"> <li>Risk management policy, standards, and a program oversight or steering group</li> </ul>
✓	Identified stakeholders for risk management	<ul style="list-style-type: none"> <li>All participants in the risk management process, including owners of enterprise risk and organizational services, will be aware of their roles and responsibilities</li> </ul>
✓	Key foundational processes and plans documented	<ul style="list-style-type: none"> <li>Process to define and monitor risk tolerance and appetite</li> <li>Risk analysis processes defined to provide resilience requirements to the identification, disposition assignment, and monitoring processes</li> <li>Risk communications and training and awareness activities incorporated into job functions and employment processes</li> <li>Risk management strategy defined with clear objectives documented and communicated across the organization and to external stakeholders</li> <li>Risk identification, disposition assignment, and monitoring processes documented and implemented</li> </ul>
✓	Linkage to other risk management processes established	<ul style="list-style-type: none"> <li>Operational and enterprise risk management are complementary processes that must work closely together to ensure resilience and the effective management of the overall risk posture of an organization</li> </ul>
✓	Identified laws, regulations, and rules	<ul style="list-style-type: none"> <li>List of requirements affecting the organization's service continuity</li> </ul>
✓	Risk management procedures	<ul style="list-style-type: none"> <li>A written description of how risk management activities will be communicated, executed, and coordinated throughout the organization</li> </ul>
✓	Detailed processes for risk management	<ul style="list-style-type: none"> <li>Predefined processes for risk management strategy, plan development, execution, monitoring, and improvement</li> </ul>

## IV. Implement the Risk Management Plan

### Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin implementing a risk management plan.

*In this guide, risk refers to operational risk to IT-dependent assets and services.*

	Input	Guidance
✓	Risk objectives and plan	The objectives and plan provide direction for the implementation and management of the risk program. For example, the risk program may limit its scope to cyber threats that could cause large financial and customer impacts. If your organization has participated in a CRR, it may be beneficial to begin with the risks that appear to be the most significant for the critical service addressed during the CRR.
✓	Risk objective and strategy	<ul style="list-style-type: none"><li>• Objectives of the operational risk program that are easy to articulate and understand</li><li>• Strategy reflecting risk tolerance</li><li>• Policy and standards defining how risks should be measured and addressed</li><li>• Communications processes that engage stakeholders and facilitate the program</li></ul>
✓	Risk documentation approach defined	<ul style="list-style-type: none"><li>• A defined process for tracking risk information in a central risk register</li></ul>
✓	Risk communications	<ul style="list-style-type: none"><li>• Documented process that facilitates two-way risk communications and collaboration</li></ul>
✓	Lists of stakeholders	The list of stakeholders should be aligned to the program objectives and include all appropriate internal and external entities. Potential candidates include <ul style="list-style-type: none"><li>• customers</li><li>• service owners</li><li>• executives, senior managers, and board members</li><li>• information technology service owners</li><li>• insurance providers and lenders</li><li>• vendors</li><li>• regulators</li><li>• infrastructure providers, such as data, telephony, and regulatory agencies</li></ul>
✓	Management support	<ul style="list-style-type: none"><li>• An endorsement by senior management supporting the establishment and implementation of an operational risk management program</li></ul>
✓	Risk tolerance dialogue and authoritative sources for validation of strategies	<ul style="list-style-type: none"><li>• Organization's aversion to risk</li><li>• Levels of acceptance of risk</li><li>• General perspective on how to address risk, for example, accept, avoid, mitigate, transfer</li></ul>
✓	Externally imposed risk requirements	<ul style="list-style-type: none"><li>• Regulatory requirements defining mandatory risk management activities</li><li>• Partner requirements</li></ul>
✓	Budget for risk management	<ul style="list-style-type: none"><li>• Identification of available funds to perform risk management and execution, including funds for<ul style="list-style-type: none"><li>○ staffing resources</li><li>○ tools (applications and associated hardware)</li><li>○ third-party support</li></ul></li></ul>

## Step 1. Assign responsibility for implementing the plan.

As noted earlier in this guide, organizational ownership of the overall and operational risk management functions can be established in a variety of ways. For example, the functions can be assigned to a single executive, managed by a committee, or coordinated by a steering group. Ensuring that the implementation goes smoothly requires that responsibility be established across virtually all levels of the organization. Leveraging existing management processes, such as existing management hierarchies and project management processes and reporting, is typically the most efficient way to establish those risk responsibilities and accountabilities.

A crucial first step is to establish an implementation management process that ensures that core objectives are communicated, accountability for achieving those objectives is assigned, and the overall process is managed. Strategies for establishing accountability for results vary widely, but ensuring oversight and coordination of the risk implementation will help ensure success.

Suggested risk implementation management practices include the following:

- Establish executive or leadership team ownership of the implementation and program.
- Executives communicate risk management plan objectives, strategies, and accountabilities.
- Require risk training and provide regular risk awareness communications.
- Establish a central repository for policy, standards, procedures, plans, and supporting documentation.
- Engage stakeholders and define ownership of risk areas and mitigations.
- Document implementation action/project plans with timelines.
- Develop management reporting and metrics for implementation performance.
- Provide a forum for project updates, issues identification, and resolution tracking.
- Conduct regular reviews of the risk implementation plan and modify it as necessary.
- Establish a process to communicate and/or escalate significant issues.

*The implementation of the risk plan can be one of the most challenging activities to manage. Establishing responsibilities across the organization for meeting clearly delineated objectives and timelines is a foundational activity. Reporting on the progress and issues associated with the implementation facilitates the visibility and stakeholder engagement needed for success.*

## Step 2. Provide training on the operational risk management plan.

Ensuring that those people responsible for implementing and managing operational risk understand risk plans and their responsibilities is essential. The focus of the training should be on the specifics of the operational risk management implementation: its timeline, reporting, accountabilities, and approach. The training to support the risk implementation recommended here should complement more generalized training that is provided across the organization and that supports establishing baseline risk skills and a risk culture. Training and risk awareness are essential to the success of operational risk management and should be an ongoing, foundational aspect of both the overall program and implementation activities.

The training may need to be targeted to different types of audiences, depending on the scope or the implementation (e.g., single service, enterprise, or region) and the size of the organization. For example, training meant for managers and executives should focus on overall objectives, budgets, and timelines; another version oriented toward operations staff should provide more detailed definitions of controls implementations and monitoring.

### Step 3. Establish a risk identification process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 3: Risks are identified.</b>	
1. Are operational risks that could affect delivery of the critical service identified? [RISK: SG3.SP2]	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

**A. Define and document risk identification process.** The risk identification process should not be viewed as an effort to identify every conceivable operational risk. Instead the effort should focus on the risks that are the most important to the organization's business needs and its role in the critical infrastructure. There are many techniques for identifying operational risks to be managed. These include everything from a simple questionnaire based on the operational risk categories identified in Section III, Step 2, to more complex combinations of activities involving synthesis of data from vulnerability scans, penetration testing, and environmental studies. Some potential techniques for consideration include

- distributing questionnaires and surveys
- interviewing vital managers and subject-matter experts
- brainstorming with asset and service stakeholders
- mining historical data (both internal and external)
- acquiring external expertise (e.g., consultants)
- developing scenarios

Organizations that have existing enterprise risk management programs should leverage those programs' tools and techniques.

The risk identification process should include the following activities:

- i. **Identify tools, techniques, and methods that will be used to identify operational risks to the assets that support a critical service.** Staff may need training or external support to effectively execute the risk identification process.
- ii. **Describe which techniques should be applied for which assets and asset classes.**
- iii. **Consider the risk sources identified in the risk management strategy to ensure adequate risk coverage.**
- iv. **Develop risk statements for each identified risk.**
  - Risk statements should include information about
    - the assets affected
    - the weakness or vulnerability to the asset that could be exploited
    - actors who would exploit the weakness
    - impact on the asset
    - resilience requirement of that asset
    - impact on the critical service the asset supports
    - resilience requirements of that service
  - Risk statements may include information about
    - the likelihood of the risk being realized
    - the motive of the actor
    - controls currently in place to mitigate that risk
- v. **Identify relevant stakeholders associated with the risk.**
- vi. **Communicate identified risks to appropriate stakeholders.**

- vii. **Collect and track identified risks and associated risk statements.** This is often done in a risk register.

**B. Identify and document responsibilities for operational risk identification.** The responsibility for identifying operational risks to IT-dependent services is often assigned to the organization's IT department, but this task may also be effectively performed by other organizational units. The optimal implementation of risk identification activities depends heavily on the organization's structure and risk management approach. For example, an organization with many business units that operate in distinct risk environments may assign responsibility for risk identification activities to each business unit, which best understands its own environment. Another organization with many business units that share common technology infrastructure resources and business risks may choose to centralize all risk identification activities, for efficiency and to ensure a consistent approach.

- i. **Assign responsibility for identifying risks to assets and the services they support to specific roles or groups in the organization.**
- ii. **Require specific roles or groups to sign off on their assigned responsibility for implementing risk identification processes.**

**C. Execute the risk identification process.**

#### Step 4. Establish a risk analysis process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 4: Risks are analyzed and assigned a disposition.</b>	
1. Are risks analyzed to determine potential impact to the critical service? [RISK: SG4.SP1]	ID.RA-4: Potential business impacts and likelihoods are identified.

The purpose of the risk analysis process is to ensure that all identified risks are consistently evaluated in the context of the organization's risk drivers (tolerance, appetite, and measurement criteria) to inform risk disposition decisions. The risk analysis process may use formalized quantitative measures that consider impact and probabilities, or it may use more qualitative measures related to other strategic or tactical considerations. The approach used to conduct the analysis should be documented and the results reviewed with stakeholders and those who participated in the earlier phases of the risk management process.

Variables often considered in the analysis of risk include

- impact (e.g., high, medium, low; dollars; number of customers; regulatory fines and costs)
- probability (e.g., high, medium, low; discrete percentages; other more sophisticated techniques)
- strategic value of the service to the organization's objectives
- correlation with other risks (e.g., multiple assets facing the same threat or related threat)
- anticipated or emerging man-made threat dynamics (e.g., new malware, distributed denial-of-service attack, or phishing technique)
- expected changes in threat, such as weather (e.g., flooding, fires, snowstorms)

**A. Define and document risk analysis process.** Regardless of the methodology used to conduct the risk analysis, it is important to document the process to help ensure consistency and provide context for future improvements to the process. Moreover, clearly documented processes can be more effectively managed and iteratively improved. The risk identification process should include the following activities:

- i. **Evaluate all identified operational risks against the organizationally defined risk parameters (i.e., criteria and thresholds).**



- ii. **Assign a value to each risk statement.** Risk valuations can be quantitative, qualitative, or combinations of both. Risk valuations should be consistent with those for other risk management functions where possible. Organizations developing their first risk analysis process should begin with a simple evaluation approach and then consider adding additional complexity as resources, expertise, and organizational needs require.
  - iii. **Update the risk register with risk values.**
  - iv. **Categorize and group risks according to the defined risk categories.** This may allow for consolidation, elimination, or merging of risk statements, and it supports the development of more efficient and effective mitigation and control decisions.
  - v. **Prioritize risks.** This enables organizations to make decisions about which risks to address first.
  - vi. **Communicate and validate risk assessment results with the appropriate stakeholders.**
- B. Identify and document responsibilities for operational risk analysis.** The responsibility for analyzing risks to IT-dependent services is often assigned to the organization's IT department, but this task may also be effectively performed by other organizational units. The optimal implementation of risk analysis activities depends heavily on the organization's structure and risk management approach. For example, an organization with many business units that operate in distinct risk environments may assign responsibility for risk analysis to each business unit, which best understands its own environment. Another organization with many business units that share common technology infrastructure resources and business risks may choose to centralize all risk analysis activities, for efficiency and to ensure a consistent approach.
- i. **Assign responsibility for analyzing risks to assets and the services they support to specific roles or groups in the organization.**
  - ii. **Require specific roles or groups to sign off on their assigned responsibility for implementing risk analysis processes.**
- C. Execute risk analysis process.** See Figure 5 for an example analysis data matrix.

Risk Categories	Impact Area Description	Tolerance Parameters		
		High Risk	Medium Risk	Low Risk
Technology	System availability - server offline	20 minutes/day	10 minutes/day	5 minutes/day
	Problem resolution - sev -1 issue	4 hours	3 hours	2 Hours
	Security patching - % of servers	10%	8%	4%
	Viruses found - % of servers	2%	1%	0.5%
Process	Security training - % not trained	25%	15%	10%
	Process documentation current	50%	25%	10%
	Policy exception resolution	90 days	75 days	60 days
	Controls not tested annually	80%	75%	70%
External	Late regulatory finding responses	3	2	1
	Suppliers - % late security reviews	20%	15%	10%
	Power failures - minutes/month	30	20	10
People	Financial errors - \$	20,000	15,000	10,000
	Customer order errors - %	3%	2.5%	2.0%
	Fraud, external actors - \$	20,000	15,000	10,000
	Fraud, insider - \$	20,000	15,000	10,000

Figure 5: Risk Analysis Data Example

## Step 5. Establish a risk disposition assignment process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 4: Risks are analyzed and assigned a disposition.</b>	
2. Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK: SG4.SP3]	ID.RA-6: Risk responses are identified and prioritized.

Assigning a risk disposition defines the approach the organization will use to manage the risk. Common risk dispositions include accept, avoid, monitor, mitigate, and transfer (see Figure 6). Risk disposition assignment is a key risk management step that should be carefully undertaken with input from key internal and external stakeholders. The frequency (i.e., probability) of the realization of risk and the likely impact on the organization are key variables driving disposition decisions. Risk frequency and impact considerations are often combined with other strategic factors to inform disposition assignment. Because of the dynamic nature of today's risk-threat landscape, many organizations also utilize information provided by industry groups, governments, and vendors to support their disposition assignment and mitigation activities.

*Common risk dispositions include accept, avoid, monitor, mitigate, and transfer.*

## RISK DISPOSITION PROCESS

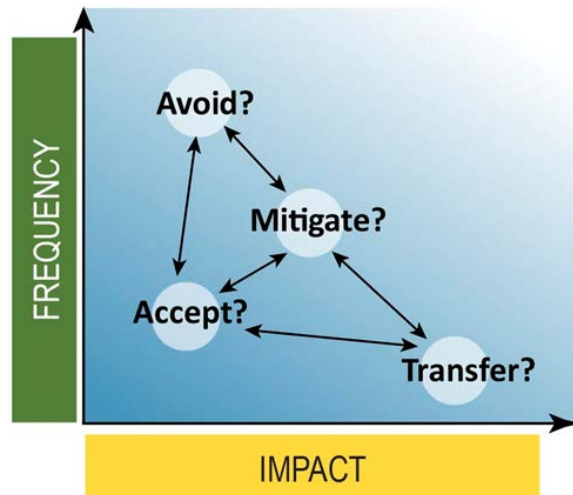


Figure 6: Risk Disposition, Conceptual Diagram

Regardless of the disposition, this aspect of risk management requires careful design, monitoring, and oversight. It is strongly recommended that stakeholders, executives, and risk management teams be involved in reviewing and acknowledging the disposition and mitigation decisions and implementations to ensure transparency and ongoing support for the process. Where significant financial investments on controls come into play, the disposition process often becomes highly visible due to its importance in the effective allocation of resources. For example, building a second data center to help ensure availability can cost many millions of dollars, making the disposition-related business case critical to the decision on the value of that investment. For less significant investments, disposition and mitigation can be equally important to ensure that key risks are not overlooked or incorrectly specified. More so than for any other area of risk management, risk disposition assignment requires effective and ongoing communication to drive stakeholder interaction and engagement in the process.

A core risk management principle is that not all risk can be eliminated. Regardless of the disposition method, some level of residual risk will remain. The status of the residual risk should be carefully tracked and monitored as objectives, risk tolerance, threats, and operations evolve. If not adequately monitored, today's low-priority residual risk can evolve into tomorrow's risk management oversight and failure. The dynamics of the threat and risk environment require careful, ongoing monitoring. Use of risk-tracking tools can be essential to this process and is discussed in further detail in Section III, Step 3.

Common risk disposition strategies include the following:<sup>14</sup>

- avoidance—a strategy or measure that effectively removes the exposure of an organization to a risk
- acceptance—an explicit or implicit decision not to take an action that would affect a particular risk
- control or mitigation—deliberate actions taken to reduce a risk's potential for harm or to maintain the risk at an acceptable level
- transfer—shifting some or all of the risk to another entity, asset, system, network, or geographic area
- monitoring—an explicit decision to further research and defer action on a risk until the need to address it is apparent and the risk is better understood

**A. Define and document the risk disposition process.** The risk disposition process should include the following activities:

- i. **Assign a disposition to all identified operational risks based on risk valuation and prioritization.**
- ii. **Update the risk register with disposition decisions.**
- iii. **Develop disposition strategies.**
- iv. **Assign the implementation of disposition strategies to individuals or roles.**
- v. **Communicate and validate risk disposition decisions and strategies to appropriate stakeholders (typically senior management).**

*More so than for any other area of risk management, risk disposition assignment requires effective and ongoing communication to drive stakeholder interaction and engagement in the process.*

## Step 6. Establish a risk mitigation and control process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 5: Risks to assets and services are mitigated and controlled.</b>	
1. Are plans developed for risks that the organization decides to mitigate? [RISK: SG5.SP1]	ID.RA-6: Risk responses are identified and prioritized. ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Operational risks that exceed the organization's risk tolerance thresholds, as determined by the risk analysis process, require the development of mitigation and control plans to reduce the risk to a level acceptable to the organization. Figure 7 shows an example mapping of risks to controls. The possible approaches to mitigating risk include actions to

- prevent or minimize the exposure to the vulnerability or threat
- establish response and restoration processes to reduce the impact of a realized risk

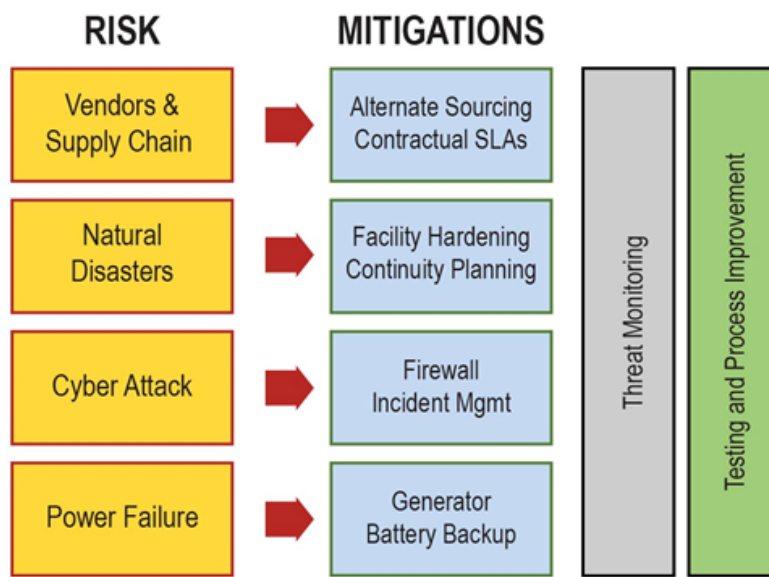


Figure 7: Risk and Controls Mapping Example

The control process should be designed to reduce, mitigate, or respond to risks faced by the organization. The control process is the aggregation of the organization's activities designed to ensure that its risks are managed in a manner that allows it to meet its mission. The process includes operational activities focused on establishing risk controls and broader objectives that include managing fraud, unethical behavior, and compliance. Controls design should be driven by the requirements and objectives established for the service at risk. Control requirements generally support maintaining the confidentiality, integrity, and availability of the assets used to support the service. Some common requirements include

- the criticality and confidentiality of data associated with the service
- how quickly the service must be recovered in the event of a disruption
- the desired currency or age of the last data backup should a disruption occur (e.g., 1 hour old or 24 hours old)

*The control process is the aggregation of the organization's activities designed to ensure that its risks are managed in a manner that allows it to meet its mission. The process can include both operational implementation of risk controls and broader activities that target the management of issues such as fraud, unethical behavior, and compliance.*

A crucial aspect of the control design process is the determination of whether it is more appropriate to focus on controls to protect against realized risk or to focus on managing the consequence of the risk. Typically, proactive controls to protect against risks are more effective, but they are often more costly and difficult to manage. Organizations frequently develop a combination of protective and reactive controls. For example, organizations may implement backup solutions for lower risk applications, along with business continuity plans to manage alternate manual service delivery during times when systems are rebuilt and restorations occur.

The design of the control process can be affected by the organization's

- risk tolerance and appetite
- the probability of the occurrence of the risk
- the potential impact of a realized risk
- willingness to invest in and expend resources to manage controls

The process of designing and implementing controls should be well documented and monitored for effectiveness and efficiency. Not only should risk controls address the requirements established, but also they must not create unintended risks or issues. For example, if it is determined that more complex passwords are necessary, technical and procedural actions should be taken to implement the risk control approach within acceptable time frames and on budget.

The risk mitigation and control process should include the following activities:

- i. Ensure there are risk mitigation plans for all operational risks that the risk analysis process has assigned a mitigation or control disposition to.**
  - Mitigation planning can be a resource-intensive activity, and the effort required will vary from organization to organization.
  - Some common elements that should appear in all plans include
    - explanation of how threat or vulnerability will be reduced or explanation of how the impact of a realized risk will be reduced
    - controls that will need to be implemented or service continuity plans that will need to be developed
    - staff responsible for implementing plan

- costs associated with the plan
  - implementation requirements of the plan
  - residual risks that the plan does not address
- ii. **Validate the risk mitigation plan with appropriate stakeholders.**
  - iii. **Establish monitoring of implementation of risk mitigation and control plans.**
  - iv. **Assign implementation of disposition strategies to individuals or roles.**

*This Resource Guide does not specifically address the development of protection and sustainment strategies through the development and implementation of control strategies and service continuity strategies. See the Controls Management Resource Guide, Volume 2 of this series, for more detailed guidance on the controls process. See the Service Continuity Management Guide, Volume 5 of this series, for more detailed guidance on the service continuity process.*

## **Step 7. Establish a risk monitoring process.**

To understand whether its risk management program is effective, an organization must monitor the program's processes to ensure that each step is performed and that all identified risks are adequately addressed. A risk monitoring process should be designed to provide the information necessary to keep the operational risk program robust and efficient. The key processes to consider for an effective monitoring program include the following.

- A. **Track existing, new, and potential risks.** Tracking risk status and identifying new risks are core practices that a monitoring program should establish. The following activities should be undertaken in support of risk tracking:
  - i. **Maintain a prioritized list of existing operational risks and their dispositions.**
  - ii. **List any new risks that have been identified, and document threats being monitored as potential new risks to the organization.**
  - iii. **Document existing mitigation and control strategies, implementation timelines, status, and those responsible for executing the process.**
- B. **Conduct assessments of protection/sustainment controls and mitigations.** Ensuring that protection and sustainment strategies are properly designed requires ongoing review of their objectives and assessment to measure the effectiveness of strategies used to meet those objectives. Control assessments provide valuable insights into how controls are functioning and whether there are weaknesses, unforeseen consequences, or gaps. For example, did increasing the complexity of passwords lead to improved security by reducing the chance of unauthorized access, or did it lead to users writing their passwords down and leaving those written passwords in locations near their computer? Did service continuity plans adequately provide for the smooth recovery of operations as validated by thorough, integrated testing of both process and technology recovery procedures? The following activities should be put in place to monitor protection/sustainment mitigations and controls:
  - i. **Establish protection and sustainment assessments of mitigations and controls.**
  - ii. **Document the schedule for assessments.**
  - iii. **Develop assessment objectives.**
  - iv. **Execute assessments and document the results.**

- v. **Track the resolution of any gaps or weakness identified.**

*See the Controls Management Resource Guide, Volume 2 of this series, for more information on assessing risk controls.*

**C. Develop reporting and risk metrics designed to measure the effectiveness of strategies and level of risk.** Reporting on risks and related metrics should be provided on a regular basis to stakeholders, including leaders and operational managers. Having a clear understanding of the most important risks the organization is facing and the strategies that are being deployed to manage those risks helps ensure that the right risks are being addressed in an appropriate manner. The following recommended actions should be considered for risk reporting on risk monitoring:

- i. **Establish a common location for the collection of operational risk information, strategy tracking, and monitoring, for example, in a risk register.** See Section III, Step 3, for a more detailed description of the design considerations of a risk register.
- ii. **Establish a schedule and format for risk reporting.** See Appendix F for example formats.
- iii. **Develop and refine reporting metrics to support the objectives of the risk strategies and program.** See Appendix G for examples metrics.
- iv. **Provide reporting and gather regular feedback to improve and refine that reporting.**

## Step 8. Implement risk mitigation and monitoring.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 5: Risks to assets and services are mitigated and controlled.</b>	
2. Are identified risks tracked to closure? [RISK: SG5.SP2]	ID.RA-6: Risk responses are identified and prioritized. ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Mitigation of risk generally includes the use of protective controls as well as consequence management and response plans that protect and sustain the organization from threats that have been identified as posing significant risk to the organization. Mitigations generally take the form of a combination of controls designed to reduce the probability of and exposure to risks and service continuity plans that limit the impact of a realized risk.

Organizations must ensure that mitigations are effective over time as changes occur to the organization, its external environment (e.g., vendors, governments, society), and the threat landscape (e.g., new malware, viruses, denial of service exploits, natural environment). In addition to reviewing mitigations, the organization must also monitor the overall risk–threat landscape to determine if the organization must change how it addresses risks (e.g., accept, avoid, monitor, control, or transfer). A process of ongoing monitoring and process improvement is essential and is the essence of what makes a risk program highly effective and mature.

- A. Implement mitigations.** The implementation of mitigations should include the following activities:<sup>15</sup>
- Review and validate existing mitigations to determine if they are meeting risk objectives.
  - Identify new mitigations that may be needed to address risks.
  - Determine the person or group responsible for each risk mitigation.
  - Manage and monitor residual risk, such as a change in the risk level, for further disposition/mitigation.

**B. Monitor mitigations.** Monitoring of risk mitigation strategies to determine if they are achieving their objectives should include the following activities:

- Continually review residual risks and any other active or potentially active risks.
- Monitor the effectiveness of risk mitigations.
- Measure and report on the performance of risk mitigations.
- Monitor the threat landscape to identify new or emerging risks.

## **Step 9. Communicate risk mitigations.**

Risk mitigation is an expansive and difficult process requiring regular, two-way communication between risk owners and stakeholders. Challenges to managing both risks and costs are common, and they require adjustments to risk plans, strategies, and budgets. Risk owners and stakeholders must work together to find appropriate solutions that keep the risk program on track. Transparency is essential for an effective risk program to manage risk outcomes and issues.

Mitigation issues to monitor and report on include

- realized risk events (e.g., breaches, increased virus activity, availability declines)
- identified gaps or weaknesses in controls
- delays in mitigation implementations
- new controls requiring unplanned resourcing (e.g., funding and people)
- newly identified threats that require disposition

Reporting on mitigations is often most effective when there are a variety of venues and approaches used at various levels in the organization. Smaller organizations might require only reporting to technical managers and senior executives, but larger organizations might require reporting to a broader collection of stakeholders at multiple levels within the organization. Regardless, the reporting should be documented and, as appropriate, provided in the form of a briefing or presentation that is targeted to the audience, for example, technically detailed for operational teams versus higher levels of risk issue reporting for managers and executives.

Suggested reporting tools and techniques include

- heat map dashboards (e.g., red-yellow-green status summaries)
- key risk indicators (e.g., metrics that the organization is subject to a risk that exceeds a defined risk threshold)
- key performance indicators
- graphical depictions of key risk variables (e.g., availability, failed technical change events, problem reports)



## Output of Section IV

	Output	Guidance
✓	Responsibilities for the implementation documented	<ul style="list-style-type: none"> <li>Responsibilities assigned and accountabilities established</li> <li>Plan implementation managed to ensure it remains on track to meet its objectives</li> <li>Metrics and reporting that provide visibility into plan implementation progress and issues</li> </ul>
✓	Operational risk activities implemented	<ul style="list-style-type: none"> <li>Key operational activities that provide day-to-day risk management capabilities</li> <li>Operational activities that are reviewed against the risk plan objectives</li> <li>Risk plan and strategy refinements that are reviewed and managed</li> </ul>
✓	Stakeholder engagement and communication	<ul style="list-style-type: none"> <li>Stakeholders identified and engaged in the design and management of the program</li> <li>Two-way communication underway to facilitate the integration of the risk program into the organization</li> </ul>
✓	Risk identification, analysis, and disposition assignment process	<ul style="list-style-type: none"> <li>Process to identify and prioritize risks</li> <li>Process to analyze the risks to inform how the organization should address them</li> <li>Process for assigning risk disposition (e.g., accept, avoid, monitor, control, or transfer)</li> </ul>
✓	Mitigation and monitoring	<ul style="list-style-type: none"> <li>Design of a process to develop and implement mitigations</li> <li>Monitoring and oversight process to ensure mitigations are effective and appropriate</li> </ul>
✓	Risk repository and tracking	<ul style="list-style-type: none"> <li>A secure location for storing and maintaining continuity plans that provides access and availability when plans are needed</li> </ul>
✓	Training and awareness	<ul style="list-style-type: none"> <li>Processes established to provide risk training in support of the objectives of the program</li> <li>Awareness activities designed to build a risk culture and recognition of the importance of the risk program to achieving the organization's mission</li> </ul>



## V. Monitor and Improve Operational Risk Management

### Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin monitoring and improving operational risk management.

*In this guide, risk refers to operational risk to IT-dependent assets and services.*

	Input	Guidance
✓	Program objectives, policies, and standards	<ul style="list-style-type: none"><li>• Determine if the program is functioning as documented</li><li>• Measure program outcomes against stated objectives</li><li>• Determine if the level of risk is within the organization's tolerance parameters</li><li>• Identify needed changes in strategy, oversight, governance, and reporting</li></ul>
✓	Change criteria for the risk program objectives and strategies	<ul style="list-style-type: none"><li>• Program assessment and risk review; risk strategies reviewed during any major change to the organization</li><li>• Risk measurement and stakeholder perspectives on risk assurance and approach</li><li>• Risk event/incident analysis and trending; an internal and external perspective</li></ul>

### Step 1. Oversee the risk program processes to ensure its objectives are met.

Ensuring that the risk program remains effective requires ongoing monitoring of risks, threats, strategies, the organization's objectives, and the performance of the program as designed. The risk objective communications approach can vary depending on the organization; it can be as simple as a few key goals outlined in an email to stakeholders or as complex as a comprehensive plan that is managed in a sophisticated risk management tool. The key is having clearly communicated objectives that facilitate management of a risk program, which is iteratively improved over time in support of the organization's mission.

*Risk management activities are most effective when they are established as a core aspect of the organization's processes and continually improved. Stakeholder engagement and participation are key aspects of successful programs, regardless of the size or complexity of the organization.*

For most organizations, a risk management program takes time to fully implement, and the process is a journey requiring regular tuning. Adjustments to the program will be required when gaps are identified, as risks evolve, and as normal internal and external changes occur. Some organizations faced with large, immediate risks may need to invest heavily in the implementation of a new risk program to limit impacts to their mission, and others without pressing risk issues and limited budgets may choose a slow and systematic approach over a longer period of time. Whatever pace an organization chooses, getting started is what is most important.

The operations risk executive, committee, or steering group, described in Section III, Step 1, is typically best suited to take an active role in managing the program, monitoring the need to make adjustments, and coordinating improvement activities. The oversight role and responsibilities may include

- establishing refined or updated program strategies and objectives; many do this annually
- updating risk tolerance parameters and priorities
- refining program objectives
- providing new or refined risk standards
- providing guidance on how risks should be managed
- identifying program gaps or weaknesses that must be addressed
- coordinating communications with stakeholders
- modifying or strengthening training and awareness requirements
- establishing budgets
- identifying and implementing new program methodologies

*Leadership from across the organization is required for the risk management program to be effective. While there is no substitute for executive support, commitment from all levels is essential to address the range of risks faced by the operational areas of organizations.*

## **Step 2. Identify updates and improvements to the risk management plan.**

To help identify when the risk management plan needs to be updated or improved, the organization should assess the plan against its objectives. Broadly, when risks appear to be exceeding the organization's tolerances, then action needs to be taken. Determining when risks should be addressed is often complex and hard to measure. Organizations may find that the best approach is to use a combination of metrics that are collaboratively reviewed to arrive at actionable decisions. Below are suggested approaches to risk measurement.

- qualitative measurements
  - internal or external audit ratings on overall results (e.g., good, fair, poor)
  - management assessment
  - risk analysis by service and process owners
  - self-assessments by control owners
  - regulatory reviews
  - assessment of contribution to service objectives (i.e., growth, accessibility, information protection)
- quantitative measure examples
  - technical measures (e.g., availability, virus infection rates, problem reports, change management events, access violations)
  - incident and service continuity plan tested as scheduled
  - risk policy/standards exception and violation rates
  - realized risk impacts in dollars, customers, reputation, stock price, etc.
  - percentage of risk objectives met
  - percentage of risk action plans on schedule

### Step 3. Proactively monitor and report on risk mitigation activities.

#### A. Monitor protective controls.

- Document existing controls and risks they are designed to address.
- Prioritize the controls based on risks addressed.
- Identify emerging risks and planned actions.
- Track testing of risk controls.

#### B. Monitor consequence management.

- Maintain and test incident management plan.
- Maintain and test business continuity and technology recovery plan.
- Monitor trends and issues in problem management.

#### C. Proactively review threat intelligence to identify new or emerging threats.

- Track and monitor threats (e.g., type, frequency, exploit type, motivation).
- Monitor trends (e.g., sector/industry, new exploits, new threat actors, nation-state activities).
- Monitor organization-specific threats (e.g., targeted activities, products, companies).
- Coordinate with external groups (e.g., US-CERT, Information Sharing and Analysis Centers (ISACs), DHS, industry consortiums) .

*See the Situational Awareness Resource Guide, Volume 10 of this series, for more information on tracking and monitoring threats and coordinating with external groups.*

### Step 4. Improve the risk management plan.

#### A. Schedule and assign responsibility for improvements.

**B. Update the risk management program processes and plans.**<sup>16</sup> Risk management plans should be treated as living documents that must be refined and modified as changes occur and as weaknesses in the plan are identified. Changes to the threat landscape, organization, and technologies are common drivers for needed updates to the risk plans. Organizations should make ongoing refinements to their risk plans and conduct a major revisit to the risk plan and its key components at least annually, including

- objectives
- strategy
- risk tolerances
- budget
- stakeholders
- policies and standards
- training
- communications

#### C. Track open items to closure.

## Output of Section VI

	Output	Guidance
✓	Updated program processes	<ul style="list-style-type: none"> <li>Updated program strategy, objectives, documentation, and procedures</li> <li>Documented process change objectives, timelines, and responsibilities</li> </ul>
✓	Updated program strategies and objectives	<ul style="list-style-type: none"> <li>Approved changes</li> </ul>
✓	Updated risk documentation, tracking, and action plans	<ul style="list-style-type: none"> <li>A database, spreadsheet, or list showing the current documentation update status</li> <li>Updated tracking database</li> <li>Updated risk action plans for all affected areas, showing tasks and timelines in support of the risk program objectives</li> </ul>



## VI. Conclusion

Operational risk must be identified, analyzed, and managed to ensure that an organization can deliver its services and accomplish its mission. Effective operational risk management arises from the development of impact evaluation criteria that align with the services an organization delivers and the construction of stable, repeatable processes to identify and manage risks that may yield undesired impact. This guide has provided a step-by-step overview of how to establish and manage an operational risk program that reflects the unique needs and risk tolerance of an organization.

The NIST CSF function Identify contains most aspects of the practices described in the Risk Management domain. The most direct mappings of Risk Management domain practices to the NIST CSF can be found in the category of Risk Management Strategy Processes and Procedures within the Identify function (ID.RM). See Appendix J for a complete mapping of Risk Management practices to NIST CSF Categories and Subcategories.

Methodologies that have been outlined throughout this document are designed to provide a pragmatic approach that focuses on three primary concepts:

- Efficient risk programs are built on a deliberate strategy, a defined plan, and clear objectives that are informed by two-way communication among internal and external stakeholders.
- Effective risk programs are built and maintained by systematically ensuring risk processes are managed and improved across all aspects and areas of the organization.
- Leveraging current processes within the organization builds upon existing collaboration and communication channels and simplifies the implementation of new or refined risk processes.

The body of documentation, standards, guidelines, and regulations developed to address risk is extensive, but there are a few straightforward foundational activities that they all share, such as knowing those activities (i.e., services) that are most important, identifying and prioritizing risks, managing those risks that are deemed of greatest concern, monitoring existing and emerging risks, and modifying and improving the risk program to keep pace with the dynamics of today's risk environment. Risk cannot be eliminated, only managed. By taking a systematic and informed approach to managing risks, organizations can determine those risk management activities that make sense for them. Operational resilience, a goal many organizations pursue, is about finding that point where an organization has just the right of amount of risk management.

This document is organized around those common foundational activities to provide a standard- and guideline-agnostic approach to managing risk. While standards can be useful in identifying more detailed activities, the approach taken by this guide is to provide a clear outline of what should be done to effectively manage risk.

The following documents provide standards and methodologies for preparing for and managing cybersecurity risk:

- Risk Management Fundamentals: Homeland Security Risk Management Doctrine  
<http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf>

- NIST Special Publication 800-39, Managing Information Security Risk  
<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>
- OCTAVE® Allegro  
<http://www.cert.org/octave/allegro.html>
- The CERT Resilience Management Model (*CERT-RMM*) [Caralli 2010] is the basis for the CRR and contains more in-depth guidance for establishing cybersecurity practices. The Risk process area provides detailed description of practices and goals associated with risk management.

For more information about the Cyber Resilience Review, please email the Cyber Security Evaluation Program at [CSE@hq.dhs.gov](mailto:CSE@hq.dhs.gov) or visit the website of the Office of Cybersecurity and Communications at <http://www.dhs.gov/office-cybersecurity-and-communications>.

## Appendix A. Example Operations Risk Management Policy Template

### ***[Organization Name]*** **POLICY [XX-X]: Operations Risk Management**

Risk management is the ongoing process of identifying, analyzing, and mitigating risks in order to control the probability of occurrence and/or impact of a disruption to *[Organization Name]*'s mission. This policy lays the framework for a formal risk management program by establishing responsibility for risk identification and analysis, planning for risk mitigation, and program management and oversight.

#### **POLICY STATEMENT:**

All employees, contractors, and business partners will take all appropriate actions to control the probability of occurrence and/or impact of a disruption to *[Organization Name]*'s business objectives and mission.

#### **OBJECTIVE:**

The objective of this policy is to ensure that operational risks to *[Organization Name]* that arise from the deployment of information management and technology processes are identified, analyzed, and managed so that the risks are maintained at acceptable levels.

#### **SCOPE:**

This policy applies to all individuals and functions that utilize information and technology resources to perform tasks in support of the organization's mission.

#### **RESPONSIBILITIES:**

##### **Employees, Contractors, and Business Partners**

All employees, contractors, and business partners of *[Organization Name]* shall

- comply with all operational risk policies, standards, and guidelines
- be familiar with and support operational risk objectives
- report any actual or suspected operational risks
- take all appropriate actions to support the confidentiality, availability, and integrity of the information, technology, facility, and people assets of the organization

##### **Executive and Senior Management**

Executive and senior management shall

- support the development and maintenance of the operational risk management plan
- implement the operational risk management plan
- provide support for adequately resourcing the operational risk management plan
- ensure all employees, contractors, and business partners understand their operational risk management responsibilities

#### **Document History**

Version	Release Date	Comments



## Appendix B. Simple Risk Register Template

Risk ID	Date Identified	Risk Description	Impact	Likelihood	Risk Rating	Disposition	Mitigating Controls	Risk Owner

## Appendix C. Example Risk Scoring Matrix

IMPACT	Critical	High	High	Critical
	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Moderate	High
		LIKELIHOOD		

## Appendix D. Example Risk Analysis and Disposition Worksheet

Risk Analysis and Disposition Worksheet					
Risk ID:		Risk Owner:		Date:	
Risk Summary					
		<b>Actor</b> <i>Who would exploit the area of concern or threat?</i>			
		<b>Means</b> <i>How would the actor do it? What would he or she do?</i>			
		<b>Motive</b> <i>What is the actor's reason for doing it?</i>			
		<b>Outcome</b> <i>What would be the resulting effect on the asset?</i>	<input type="checkbox"/> <b>Disclosure</b>	<input type="checkbox"/> <b>Destruction</b>	
		<b>Security Requirements</b> <i>How would the asset's security requirements be breached?</i>	<input type="checkbox"/> <b>Modification</b>	<input type="checkbox"/> <b>Interruption</b>	
	<b>Impact Evaluation</b>				
	<b>Consequences</b> <i>What are the consequences to the organization or the asset owner as a result of a disruption or security breach?</i>		<b>Severity</b> <i>How severe are these consequences to the organization or asset owner by impact area?</i>		
			<b>Impact</b> Hi/Med/Low 1/2/3	<b>Likelihood</b> Hi/Med/Low 1/2/3	<b>Score</b>
	Reputation & Customer Confidence				
	Financial				
Productivity					
Safety & Health					
Fines & Legal Penalties					
<b>Risk Disposition Decision</b> <i>Based on the above assessment of this risk, what action will be taken?</i>					
<input type="checkbox"/> <b>Accept</b>		<input type="checkbox"/> <b>Avoid</b>		<input type="checkbox"/> <b>Defer/Monitor</b>	
		<input type="checkbox"/> <b>Mitigate</b>		<input type="checkbox"/> <b>Transfer</b>	

## Appendix E. Example Risk Parameter Template

Risk Categories	Impact Area Description	Tolerance Parameters		
		High Risk	Medium Risk	Low Risk
Technology	System availability - server offline	20 minutes/day	10 minutes/day	5 minutes/day
	Problem resolution - sev -1 issue	4 hours	3 hours	2 Hours
	Security patching - % of servers	10%	8%	4%
	Viruses found - % of servers	2%	1%	0.5%
Process	Security training - % not trained	25%	15%	10%
	Process documentation current	50%	25%	10%
	Policy exception resolution	90 days	75 days	60 days
	Controls not tested annually	80%	75%	70%
External	Late regulatory finding responses	3	2	1
	Suppliers - % late security reviews	20%	15%	10%
	Power failures - minutes/month	30	20	10
People	Financial errors - \$	20,000	15,000	10,000
	Customer order errors - %	3%	2.5%	2.0%
	Fraud, external actors - \$	20,000	15,000	10,000
	Fraud, insider - \$	20,000	15,000	10,000

## Appendix F. Example Reporting Templates

Operational Dashboard - January 2014							
Business Group	Office	Server Availability	Network Availability	Problem Resolution	Risk Training	Continuity Planning	Logical Security
Manufacturing	DET	95%	100%	100%	91%	95%	100%
Sales	LA	100%	100%	100%	67%	0%	100%
Marketing	KC	100%	84%	100%	95%	93%	92%
Network Mgmt	ALL	97%	100%	100%	98%	95%	98%
Data Center Tm	KC	100%	100%	100%	95%	93%	100%
Facilities	ALL	100%	100%	100%	96%	88%	100%
Info Security	ALL	100%	100%	100%	100%	100%	100%
Phys Security	ALL	100%	100%	100%	100%	100%	33%
Training	NY	100%	100%	100%	100%	42%	100%
Finance	NY	100%	91%	100%	85%	90%	97%
Audit	DFW	100%	100%	100%	100%	100%	100%
Legal	DFW	100%	100%	100%	100%	91%	100%
Contracts	DFW	98%	99%	99%	97%	83%	98%

## Appendix G. Example Metrics

This table appears in the SEI technical report *Measures for Managing Operational Resilience*.<sup>17</sup>

ID	Measure	Type of Information	Applicable CERT-RMM SG.SP
RISK-M1	number of internal operational risk sources identified	risk planning	RISK:SG1.SP1
RISK-M2	number of external operational risk sources identified	risk planning	RISK:SG1.SP1
RISK-M3	number of operational risk sources that are not addressed by process policies or other mitigating activities	risk sources	RISK:SG1.SP1
RISK-M4	number of risk categories defined	risk planning	RISK:SG1.SP1
RISK-M5	elapsed time since validation of risk categories performed	risk planning	RISK:SG1.SP1
RISK-M6	percentage of repeat audit findings related to operational risk management	risk strategy	RISK:SG1.SP2
RISK-M7	number of operational risks referred to the organization's enterprise risk management process	risk strategy	RISK:SG1.SP2
RISK-M8	number of risk parameters defined	risk strategy	RISK:SG2.SP1
RISK-M9	elapsed time since validation of risk parameters performed	risk strategy	RISK:SG2.SP1
RISK-M10	number of risk criteria defined	risk strategy	RISK:SG2.SP2
RISK-M11	elapsed time since validation of risk criteria performed	risk strategy	RISK:SG2.SP2
RISK-M12	elapsed time since risk analysis performed	asset risk	RISK:SG3.SP1
RISK-M13	elapsed time since business impact analysis performed	asset risk	RISK:SG3.SP1
RISK-M14	percentage of assets for which some form of risk analysis has not been performed and documented (per policy or other guideline) within the specified time frame	risk assessment	RISK:SG3.SP1
RISK-M15	percentage of services for which some form of risk analysis of associated assets has not been performed and documented (per policy or other guideline)	risk assessment	RISK:SG3.SP2
RISK-M16	confidence factor that all risks that need to be identified have been identified (refer to template in [Allen 2010]) <sup>18</sup>	risk identification	RISK:SG3.SP1 RISK:SG3.SP2
RISK-M17	change in number of identified risks that exceed risk parameters and measurement criteria	risk identification; risk valuation	RISK:SG3.SP1 RISK:SG3.SP2 RISK:SG4.SP2
RISK-M18	percentage of risks for which the impact (refer to RISK:SG2.SP2) has not been characterized (qualitative, quantitative)	risk valuation	RISK:SG4.SP1
RISK-M19	percentage of risks that have not been categorized and prioritized	risk categorization; risk prioritization	RISK:SG4.SP2
RISK-M20	percentage of risks that have been characterized as "high" impact according to risk parameters (refer to RISK:SG2)	risk valuation	RISK:SG4.SP1
RISK-M21	percentage of risks that exceed established risk parameters and measurement criteria, by risk category	risk valuation; risk categorization	RISK:SG4.SP1 RISK:SG4.SP2
RISK-M22	percentage of risks that do not have a documented and approved risk disposition	risk disposition	RISK:SG4.SP3
RISK-M23	percentage of risks that have not been assigned to a responsible party for action, tracking, and closure	risk mitigation	RISK:SG5.SP1
RISK-M24	percentage of previously identified risks that have converted from any other risk disposition to a risk disposition of "mitigate or control"	risk disposition	RISK:SG4.SP3
RISK-M25	percentage of risks with a disposition of "mitigate or control" that do not have a defined mitigation plan	risk disposition; risk mitigation	RISK:SG5.SP1

ID	Measure	Type of Information	Applicable CERT-RMM SG.SP
RISK-M26	percentage of assets for which a mitigation plan has been implemented to mitigate risks as necessary and to maintain these risks within acceptable risk parameters	risk mitigation; risk status	RISK:SG5.SP1 RISK:SG5.SP2
RISK-M27	percentage of services with an implemented mitigation plan	risk mitigation; risk status	RISK:SG5.SP1 RISK:SG5.SP2
RISK-M28	percentage of risks with a “mitigate or control” disposition with mitigations <sup>a</sup> that are not yet started	risk mitigation; risk status	RISK:SG5.SP2 RISK:SG6.SP1 RISK:SG6.SP2
RISK-M29	percentage of risks with a “mitigate or control” disposition with mitigations that are in progress (vs. completely implemented)	risk mitigation; risk status	RISK:SG5.SP2 RISK:SG6.SP1 RISK:SG6.SP2
RISK-M30	percentage of risks with a “mitigate or control” disposition that are not effectively mitigated by their mitigation plans	risk mitigation; risk status	RISK:SG5.SP2
RISK-M31	percentage of open risks that have not been tracked to closure	risk status	RISK:SG5.SP2
RISK-M32	percentage of risks with a disposition of “mitigate or control” that have a defined mitigation plan but whose status is not regularly reported (per policy or other guideline)	risk status	RISK:SG5.SP2
RISK-M33	percentage of realized risks that exceed established risk parameters <sup>b</sup>	risk status	refer to comparable measures in EC, EXD, IMC, KIM, TM
RISK-M34	elapsed time since risks with the following dispositions were last reviewed and disposition confirmed: avoid, accept, monitor, research or defer, transfer	risk status	RISK:SG5.SP2

<sup>a</sup> Including controls and updates to Service Continuity (SC) plans.

<sup>b</sup> May want to specifically categorize by source of realized risk that is of greatest interest such as incidents, control gaps, non-compliance, vulnerabilities, disruptions in continuity, etc.

## Appendix H. Risk Register Variables and Data to Consider

Risk Category	Risk #	Risk Owner	Date Identified	Date of Last Review	Risk Impact, 1 Low to 3 Hi	Risk Description	Risk Probability	Risk Score	Disposition	For Mitigated Risks, Provide Description	Date Mitigation Tested	Contingency
Technology	2.1	I Tuh	Jan-90	Mar-13	3	Sys fail	70%	2.1	Mitigate	Backup system	Dec-12	DR provider
Process	3.4	M Perez	May-80	Feb-13	2	Billing	20%	0.4	Mitigate	Procedures	Dec-12	Contractors
People actions	5.9	H Rusk	Nov-80	May-13	1	Training	10%	0.1	Mitigate	Annual training	Dec-12	None
External event	1.8	M Nate	Mar-70	Jan-13	3	Flood	5%	0.2	Accept	Building flooding	N/A	Work at home



## Appendix I. Risk Management Resources

### DHS

- Office of Risk Management and Analysis  
<http://www.dhs.gov/about-office-risk-management-and-analysis>
  - **Risk Management Fundamentals: Homeland Security Risk Management Doctrine**  
<http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf>
  - **Threat and hazard identification and risk assessment guide**  
[http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201\\_htirag\\_2nd\\_edition.pdf](http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf)

### Federal Emergency Management Agency (FEMA)

<http://www.fema.gov/>

- PS-Prep—Voluntary program, primarily serving as a resource for private and nonprofit entities interested in instituting a comprehensive business continuity management system. The program adopted the following three preparedness standards. For more information, see <http://www.fema.gov/about-ps-preptm>.
  - **ASIS International (PDF 1.2 MB)**  
[http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.asisonline.org%2Fguidelines%2FASIS\\_SP\\_C.1-2009\\_Item\\_No.\\_1842.pdf](http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.asisonline.org%2Fguidelines%2FASIS_SP_C.1-2009_Item_No._1842.pdf)
  - **British Standards Institution (BSI)**  
<http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.bsiamerica.com%2Fen-us%2FAssessment-and-Certification-services%2FManagement-systems%2FStandards-and-schemes%2FBS-25999%2F>
  - **National Fire Protection Association (NFPA)**  
<http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.nfpa.org%2Faboutthecodes%2FAboutTheCodes.asp%3FDocNum%3D1600%26cookie%255Ftest%3D1>
  - **Business Continuity Planning (BCP) Suite**  
<http://www.ready.gov/business-continuity-planning-suite>
  - **BCP resources to assist businesses with preparedness**  
<http://www.ready.gov/business>
  - **Exercise Design Materials**  
<http://www.training.fema.gov/emiweb/IS/is1391st.asp>

### Federal Financial Institutions Examination Council (FFIEC)

<http://www.ffiec.gov/>

- Management  
<http://ithandbook.ffiec.gov/it-booklets/management.aspx>

### Gartner (requires subscription)

<http://www.gartner.com/technology/home.jsp>

- Operational Risk Blog  
<http://blogs.gartner.com/business-continuity/tag/operational-risk-management/>

## **Forrester**

<http://www.forrester.com/home/>

- Risk management articles, tools, and templates (some require a fee)  
<http://www.forrester.com/search?tmtxt=Risk%20management&searchOption=10001&source=typed>

## **International Organization for Standardization (ISO)**

<http://www.iso.org/iso/home.html>

- ISO 31000 Risk management - Principles and guidelines (fee)  
<http://www.iso.org/iso/home/standards/iso31000.htm>
- ISO 31010 Risk management - Risk assessment techniques (fee)  
[http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=51073](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51073)
- ISO 27002 outlines potential cybersecurity controls and control mechanisms (fee)  
<http://www.27000.org/iso-27002.htm>

## **Information Systems Audit and Control Association (ISACA)**

<http://www.isaca.org>

- Control Objectives for Information and Related Technology (COBIT) 4.1  
<http://www.isaca.org/COBIT/Pages/default.aspx>
- Control Objectives for Information and Related Technology (COBIT) 5  
<http://www.isaca.org/COBIT/Pages/default.aspx>

## **National Institute of Standards and Technology (NIST)**

<http://www.nist.gov/index.html>

- NIST Computer Security Division, Computer Security Resource Center  
<http://csrc.nist.gov/>
  - NIST Special Publication 800-30, Guide for Conducting Risk Assessments  
[http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\\_30\\_r1.pdf](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)
  - NIST Special Publication 800-37, Risk Management  
<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
  - NIST Special Publication 800-39, Managing Information Security Risk  
<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>
  - NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations"  
<http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf>

## **Software Engineering Institute, CERT Division**

<http://www.sei.cmu.edu/>

- CERT Resilience Management Model  
<http://www.cert.org/resilience/products-services/cert-rmm/index.cfm>
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)  
<http://www.cert.org/resilience/products-services/octave/index.cfm>
- *Measures for Managing Operational Resilience* (CMU/SEI-TR-2011-019)  
<http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10017>

**United States Computer Emergency Readiness Team (US-CERT)**

<http://www.us-cert.gov>

- Situational awareness information

<https://www.us-cert.gov/>

**U.S. Department of Health and Human Services (HHS)**

<http://www.hhs.gov/>

- The basics of risk analysis and risk management

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf>

## Appendix J. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Table 5 cross-references CRR Risk Management Domain goals and practice questions to the NIST CSF Categories/Subcategories and the sections of this guide that address those questions. Users of this guide may wish to review the CRR Question Set with Guidance available at <https://www.us-cert.gov/ccubedvp> for more information on interpreting practice questions. The NIST CSF, available at <https://www.us-cert.gov/ccubedvp>, also provides informative references for interpreting Category and Subcategory statements.

*Table 5: Cross-Reference of CRR Goals/Practices and NIST CSF Categories/Subcategories Against the Risk Management Resource Guide*

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	Risk Management Resource Guide Reference
<b>Goal 1: A strategy for identifying, analyzing, and mitigating risks is developed.</b>		
1. Have sources of risk that can affect operations been identified? [RISK: SG1.SP1]	ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Section III, Step 2
2. Have categories been established for risks? [RISK: SG1.SP1]	ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Section III, Step 2
3. Has a plan for managing operational risk been established? [RISK: SG1.SP2]	ID.GV-4: Governance and risk management processes address cybersecurity risks ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Section III, Steps 1–4
4. Is the plan for managing operational risk communicated to stakeholders? [RISK: SG1.SP2]	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Section III, Step 5
<b>Goal 2: Risk tolerances are identified, and the focus of risk management activities is established.</b>		
1. Have impact areas been identified, such as reputation, financial health, and regulatory compliance? [RISK: SG2.SP2]	ID.RA-4: Potential business impacts and likelihoods are identified	Section III, Step 2
	RC.CO-2: Reputation after an event is repaired	
2. Have impact areas been prioritized to determine their relative importance? [RISK: SG2.SP2]	ID.RA-4: Potential business impacts and likelihoods are identified ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Section III, Step 2
3. Have risk tolerance parameters been established for each impact area? [RISK: SG2.SP2]	ID.RM-2: Organizational risk tolerance is determined and clearly expressed ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis	Section III, Step 2
4. Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK: SG2.SP1]	ID.RM-2: Organizational risk tolerance is determined and clearly expressed ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis	Section III, Step 2
	RC.CO-2: Reputation after an event is repaired	

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	Risk Management Resource Guide Reference
<b>Goal 3: Risks are identified.</b>		
1. Are operational risks that could affect delivery of the critical service identified? [RISK: SG3.SP2]	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Section IV, Step 3
<b>Goal 4: Risks are analyzed and assigned a disposition.</b>		
1. Are risks analyzed to determine potential impact to the critical service? [RISK: SG4.SP1]	ID.RA-4: Potential business impacts and likelihoods are identified	Section IV, Step 4
2. Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK: SG4.SP3]	ID.RA-6: Risk responses are identified and prioritized	Section IV, Step 5
<b>Goal 5: Risks to assets and services are mitigated and controlled.</b>		
1. Are plans developed for risks that the organization decides to mitigate? [RISK: SG5.SP1]	ID.RA-6: Risk responses are identified and prioritized ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Section IV, Step 6
2. Are identified risks tracked to closure? [RISK: SG5.SP2]	ID.RA-6: Risk responses are identified and prioritized ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Section IV, Step 8

## Endnotes

1. For more information on the *Cyber Resilience Review*, please email the Cyber Security Evaluation Program at [CSE@hq.dhs.gov](mailto:CSE@hq.dhs.gov).
2. “Glossary of Terms,” *CERT-RMM* [Caralli 2010].
3. Caralli, R. A.; Allen, J. A.; & White, D. W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience (CERT-RMM, Version 1.1)*. Addison-Wesley Professional, 2010. For more information on the CERT-RMM, please visit <http://www.cert.org/resilience/rmm.html>.
4. Risk Steering Committee, Department of Homeland Security. *DHS Risk Lexicon – 2010 Edition*. Department of Homeland Security, 2010. <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>
5. Risk Steering Committee, Department of Homeland Security. *DHS Risk Lexicon – 2010 Edition*. Department of Homeland Security, 2010. <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>
6. Caralli, R. A.; Allen, J. A.; & White, D. W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience (CERT-RMM, Version 1.1)*. Addison-Wesley Professional, 2010. For more information on the CERT-RMM, please visit <http://www.cert.org/resilience/rmm.html>.
7. “External Dependencies Management (EXD),” *CERT-RMM* [Caralli 2010].
8. Risk Steering Committee, Department of Homeland Security. *DHS Risk Lexicon – 2010 Edition*. Department of Homeland Security, 2010. <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>
9. NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*, discusses categories (page 20) and threat sources in Appendix D. [http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\\_30\\_r1.pdf](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)
10. The *CERT-RMM* (KIM: SG6.SP1) [Caralli 2010] discusses testing the organization’s backup and storage procedures.
11. NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. [http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final\\_updated\\_errata\\_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated_errata_05-01-2010.pdf)
12. The Institute of Risk Management. *Risk Culture: Under the Microscope, Guidance for Boards*, p. 6. IRM, 2012. [http://www.theirm.org/documents/Risk\\_Culture\\_A5\\_WEB15\\_Oct\\_2012.pdf](http://www.theirm.org/documents/Risk_Culture_A5_WEB15_Oct_2012.pdf)
13. Risk Steering Committee, Department of Homeland Security. *DHS Risk Lexicon – 2010 Edition*. Department of Homeland Security, 2010. <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>
14. Risk Steering Committee, Department of Homeland Security. *DHS Risk Lexicon – 2010 Edition*. Department of Homeland Security, 2010. <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>
15. The *CERT-RMM* (RM: SG5) [Caralli 2010] discusses the implementation of mitigations.
16. NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>
17. Allen, Julia & Curtis, Pamela. *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019). Software Engineering Institute, Carnegie Mellon University, 2011. <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=10017>

18. Caralli, R. A.; Allen, J. A.; & White, D. W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience (CERT-RMM, Version 1.1)*. Addison-Wesley Professional, 2010. For more information on the CERT-RMM, please visit <http://www.cert.org/resilience/rmm.html>.