



## 8-External Dependencies 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.

External Dependencies Management CATT Resources:

- The Cybersecurity and Infrastructure Security Agency published a [user guide](#) for individuals tasked with completing their organization's External Dependencies Management (EDM) assessment.



# **CRR Supplemental Resource Guide**



Volume 8

## **External Dependencies 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-0003283

# Table of Contents

<b>I. Introduction .....</b>	<b>1</b>
Series Welcome.....	1
Audience.....	3
<b>II. External Dependencies Management.....</b>	<b>4</b>
Overview.....	4
Summary of Steps .....	7
<b>III. Plan for External Dependencies Management.....</b>	<b>9</b>
Before You Begin.....	9
Step 1. Establish external dependencies support and strategy. ....	10
Step 2. Plan the relationship formation process.....	12
Step 3. Plan a process for identifying and prioritizing external dependencies. ....	14
Step 4. Plan for relationship management. ....	16
Step 5. Plan an information management process. ....	18
Output of Section III .....	20
<b>IV. Implement the External Dependencies Management Plan.....</b>	<b>21</b>
Before You Begin.....	21
Step 1. Assign responsibility for implementing the plan. ....	22
Step 2. Establish and maintain implementation measurements.....	23
Step 3. Formalize relationships with external entities. ....	24
Step 4. Identify and prioritize dependencies. ....	26
Step 5. Maintain requirements. ....	28
Step 6. Manage ongoing relationships.....	29
Output of Section IV.....	33
<b>V. Monitor and Improve External Dependencies Management .....</b>	<b>34</b>
Before You Begin.....	34
Step 1. Define effectiveness measures.....	34
Step 2. Detect, analyze, and correct process exceptions. ....	35
Step 3. Report and review the program with stakeholders.....	36
Step 4. Improve the EDM program, plans, and procedures. ....	36
Output of Section VI.....	37
<b>VI. Conclusion .....</b>	<b>38</b>
<b>Appendix A. Example External Dependencies Management Policy Template .....</b>	<b>40</b>
<b>Appendix B. External Dependencies Management Resources.....</b>	<b>41</b>
Relationship and Cyber Information Resources.....	41
Other Resources.....	42
<b>Appendix C. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference.....</b>	<b>45</b>
<b>Endnotes.....</b>	<b>47</b>





## I. Introduction

### Series Welcome

Welcome to the CRR 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 external dependencies risk 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 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

<b>8. External Dependencies Management</b>
--

↔ *This guide*

9. Training and Awareness
10. Situational Awareness

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 External Dependencies Management guide describes the creation and documentation of a list of critical suppliers, which can also be used to inform planning activities described in the Service Continuity Management guide. Other examples include

- planning asset management to include assets owned or controlled by external entities
- scoping situational awareness activities to include threats to external entities that the organization relies on
- identifying training and awareness activities that focus on external dependencies
- identifying incident management roles and responsibilities that pertain to external entities

Each guide is based on best practices described in a number of sources, but primarily from the CERT<sup>®</sup> Resilience Management Model (CERT<sup>®</sup>-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). The model is meant to

- guide the implementation and management of operational resilience activities
- converge key operational resilience 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 C for a cross reference between the CRR and this guide.

This guide is intended for organizations seeking help in establishing an external dependencies management process or for organizations seeking to improve their existing external dependencies management process. More specifically this guide

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

The guide is structured as follows:

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

---

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

- III. Plan for External Dependencies Management—Outlines a strategy and plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization’s external dependencies management needs.
- IV. Implement the External Dependencies Management Plan—Outlines the process for ensuring that the organization’s external dependencies management plan is implemented and meets the standards set by the organization.
- V. Monitor and Improve External Dependencies Management—Outlines the process and considerations for improving and strengthening the external dependencies management process.
- VI. Conclusion—Provides a summary of key external dependencies management concepts and references for further information.

#### Appendices

- A. Example External Dependencies Management Policy Template
- B. Relationship and Cyber Information Resources
- C. External Dependencies Management Resources
- D. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

## Audience

The principal audience for this guide includes individuals responsible for managing external dependencies or supply chain activities that affect IT operations. Executives who establish policies and priorities for external dependencies management, managers and planners who are responsible for converting executive decisions into action plans, and operations staff who implement those external dependencies management plans may also benefit from this guide.

---

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

---



## II. External Dependencies Management

### Overview

In today's technology and business environment, organizations often rely on outside entities, including technology vendors, suppliers of raw materials, shared public infrastructure, and other public services that support the organization. External dependencies management (EDM) focuses on establishing an appropriate level of controls to manage the risks that originate from or are related to the organization's dependence on these external entities. The purpose of EDM is to ensure the protection and sustainment of services and assets that are dependent on the actions of external entities.

This guide is intended to help organizations with the lifecycle of EDM, including planning the activity, forming new relationships with external entities, managing existing relationships, and monitoring and improving the activity to refine the organization's approach. The guide is intended for organizations wishing to create an EDM capability or improve their existing capability. The sections of the guide itself are structured accordingly into planning, implementing, and improving.

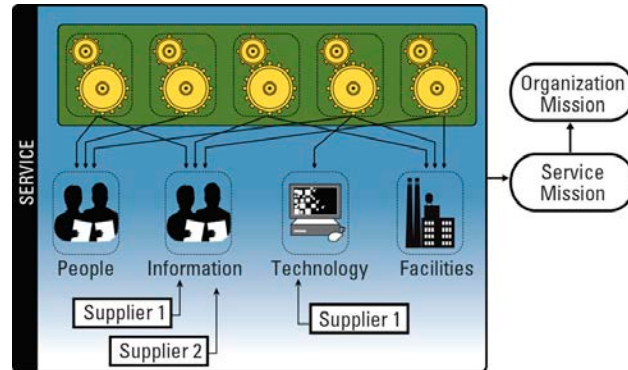


Figure 1: External Dependencies, Assets, and Organizational Mission

External dependencies and supply chain concerns are not new. Recently, however, advances in information and communications technology (ICT) have made it possible for businesses to realize great efficiency gains, cost savings, and flexibility. At the same time, global competitive pressures have driven organizations to take advantage of these gains through automation and outsourcing. These trends have sometimes outpaced organizations' ability to manage the resulting risks, making it a growing priority to establish and manage appropriate controls to ensure the delivery of critical services dependent on the actions of external entities. Additionally, events such as the attacks of September 11, 2001, and the 2011 tsunami in Japan have dramatically demonstrated the extensive and potentially cascading impacts of major shocks to interconnected supply chains around the world. Outsourcing to external entities may provide certain advantages, but it may introduce uncertainty concerning the operational resilience of the organization and its core services. An

organization must make management of this uncertainty one of the key considerations when establishing how it manages its broader operational risk posture.

The risk introduced by external dependency is one of the more challenging areas to manage because organizations have a limited ability to directly monitor and control the vulnerabilities and threats introduced. Ensuring that external entities are meeting the risk objectives of an organization, across the full range of resiliency management capabilities, is a broad scope to address. Moreover, managing the overall organization's operational risk profile when both the management and status of key external dependencies is uncertain is a challenge that has become one of the top priorities for organizations, governments, and regulators.

External dependencies management *includes activities commonly referred to by terms such as supply chain risk management, vendor management, or critical infrastructure risk management.*

External dependencies *exist when an entity that is external to the organization has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to one or more assets or services of the organization.*

Operational resilience *is an organization's ability to adapt to risk that affects its core operational capabilities.*<sup>4</sup>

Like any organization, the external entities that the organization depends on may be susceptible to a diverse and dynamic array of threats, which can negatively affect the dependent organization's people, information, technology, and facility assets and consequently the organization's ability to meet its objectives (Figure 2). The key challenge for many organizations is their limited ability to ensure the resilience of the external entities they rely on.

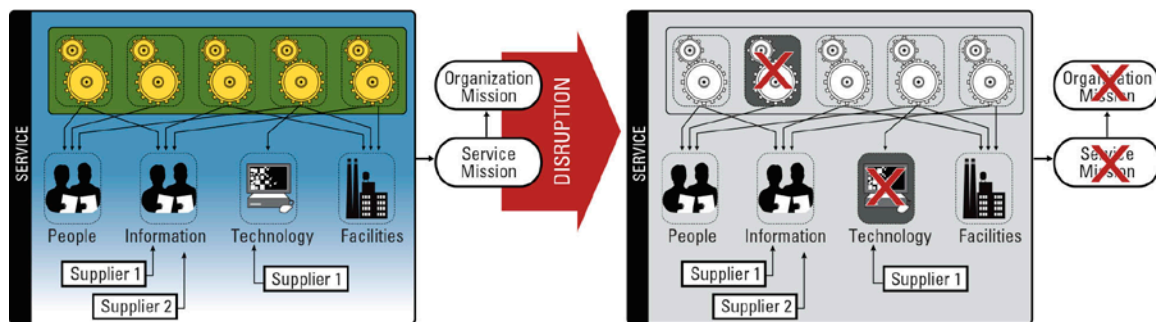


Figure 2: Disruption—Loss of the Technology Supplier

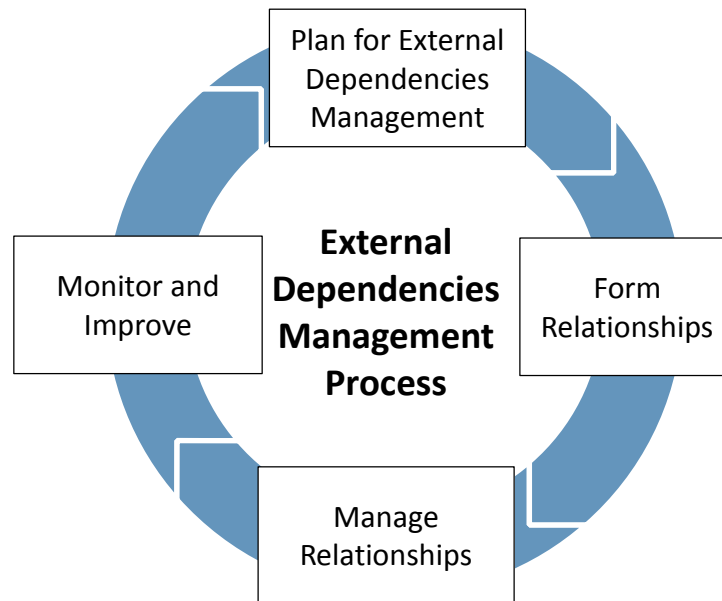
**“Threat** is a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.” DHS Risk Lexicon, 2010 Edition<sup>5</sup>

Identifying, prioritizing, and managing relationships with external entities over their entire lifecycle are foundational activities for the development of effective risk mitigation and disposition strategies. This document provides guidance for the management of external dependencies across this lifecycle. To effectively manage external dependencies, organizations should establish

- a strategy and basic plan for EDM
- key processes for identifying, prioritizing, monitoring, and tracking external dependencies
- guidance and procedures on the formation of relationships with external entities
- an approach for managing and governing existing external entity relationships
- ongoing oversight, reporting, and correction of external entity performance
- an approach for improving the organization's EDM processes and program

Like many key resilience practices, EDM should be thought of as a planned, continuous process. In the case of EDM in particular, many organizations may have only ad hoc or incomplete processes around forming new relationships with external entities or around managing existing relationships. It is also not unusual for particular organizations to have detailed procedures around the formation of new relationships, but for the ongoing management of relationships to run according to a substantially different set of objectives or standards. Effective EDM requires standard, planned guidance across the entire lifecycle of external entity relationships and continuous monitoring and improvement of the approach.

Figure 3 captures the primary phases of the EDM process.



*Figure 3: The External Dependencies Management Process*

### **Plan for External Dependencies Management**

Having a plan to drive EDM will increase the organization’s confidence in its ability to control dependency risk. Whether an organization is implementing a new program or improving existing processes, a plan can help ensure success and effectiveness. Plans should be documented, widely distributed, and regularly updated to ensure they remain current and reflect any refinements that are identified.

Developing an EDM plan is an enterprise-wide challenge, requiring extensive input and support. Therefore establishing manager and stakeholder support is a key component of planning EDM. Components of the plan include how the organization will identify and prioritize dependencies, processes for forming new relationships with external entities, and the management of ongoing or existing relationships.

### **Implement the External Dependencies Management Plan**

Establishing strong, productive relationships with external entities from the start requires early, clear definition of relationship requirements and expectations. This foundation can help build mutual trust between organizations, promoting the open exchange of information, innovation, and efficiency.

Creating and following clear, formal, and codified agreements with suppliers helps the organization manage its resilience over the life of the relationships but it also helps the suppliers understand the organization's requirements. Documented requirements form a valuable baseline of information that can be used to govern contracted relationships and to manage risks associated with relationships where the organization has limited control, such as shared infrastructure and public services suppliers.

*External suppliers or entities supporting organizations fall into three general relationship categories:*

*Vendor—Entities are chosen by the organization and are typically governed by negotiated agreements. Examples include providers of raw materials, labor, consulting, maintenance, hardware/software, and facilities.*

*Shared infrastructure—The supplier provides its services to a region or group. Agreements are usually standardized and are virtually the same across the customer base. Examples include power, water, and telecommunications.*

*Public—Typically these relationships are with a government entity such as a state, local, or federal agency and are not governed by a contract or agreement. Examples include security services (fire, police) and transportation networks.*

Monitoring, governing, and correcting supplier performance are essential activities. As with all aspects of dependency management the approach must be risk-based, reflecting the supplier's importance and the potential impact of its failure to meet the organization's requirements. When appropriate, the organization may take corrective actions such as imposing fines, transitioning to another vendor, or bringing the activity back into the organization. The organization might also mitigate risk through other means, such as adding suppliers or strengthening its service continuity and incident management plans.

## **Monitor and Improve External Dependencies Management**

Monitoring and improving the EDM processes and program help ensure that they continue to support the organization's objectives. This phase of the process focuses on maintaining the effectiveness of dependency and risk management, and involves assessing the effectiveness of EDM and any needed refinements to the plan.

## **Summary of Steps**

The following sections of this guide describe the steps for planning, implementing, and monitoring and improving EDM as described above:

### **Plan for External Dependencies Management**

1. Establish external dependencies support and strategy.
2. Plan the relationship formation process.
3. Plan a process for identifying and prioritizing external dependencies.
4. Plan relationship management.
5. Plan an information management process.

### **Implement the External Dependencies Management Plan**

1. Assign responsibility for implementing the plan.
2. Establish and maintain implementation measurements.
3. Formalize relationships with external entities.
4. Identify and prioritize dependencies.
5. Maintain requirements.
6. Manage ongoing relationships.

### **Monitor and Improve External Dependencies Management**

1. Define effectiveness measures.
2. Detect, analyze, and correct process exceptions.
3. Report and review the program with stakeholders.
4. Improve the EDM program, plans, and procedures.



### III. Plan for External Dependencies 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 developing an EDM plan.

	Input	Guidance
✓	Lists of stakeholders	<p>The list of stakeholders should include all appropriate entities, both internal and external. Potential candidates include</p> <ul style="list-style-type: none"> <li>• service/business owners within the organization</li> <li>• business partners and vendors</li> <li>• operations risk and/or other key organizational risk groups</li> <li>• technology and infrastructure owners in the organization</li> <li>• technology vendors</li> <li>• public and shared services supplier leaders</li> <li>• contract management</li> <li>• service continuity</li> <li>• information security</li> <li>• regulators and auditors</li> <li>• in-house counsel</li> <li>• customers and providers who may be impacted in the event of service interruption</li> </ul>
✓	Guidance from senior leadership and stakeholders on risk tolerance, resilience requirements, and program objectives	<ul style="list-style-type: none"> <li>• Preliminary/basic guidance on selection and requirements for contracted external entities</li> <li>• Key compliance and enterprise requirements</li> <li>• The business objectives on which EDM activities should focus</li> </ul>
✓	Assignment of responsibility for developing the EDM plan	<ul style="list-style-type: none"> <li>• Explicit assignment to a manager or set of managers in the organization for developing the plan</li> </ul>
✓	Budget for EDM planning	<ul style="list-style-type: none"> <li>• Identification of available funds and resources to plan EDM: <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> <li>○ training and communication</li> </ul> </li> </ul>
✓	Linkages to other EDM activities and plans	<ul style="list-style-type: none"> <li>• Coordination of other organizational activities around managing contracts, service-level agreements (SLAs), public and shared services supplier interaction, public outreach, or any other organizational activities that should be harmonized with EDM</li> <li>• Communication to risk stakeholders (i.e., audit, compliance, business partners, regulators) to gather support, expertise, and engagement</li> </ul>

External entities supporting the organization's key services become, in some respects, an extension of the organization itself. A strategy codified into a plan for EDM can provide managers with a higher degree of confidence that the organization uses consistent and appropriate standards and processes to form and sustain relationships with the right entities.

This section is intended to provide guidance for managers and leaders writing the EDM plan. The plan provides the framework and guidance for how the organization will approach and structure key EDM processes such as identifying and prioritizing dependencies, forming and managing relationships, and reliably managing all of the information associated with EDM. In almost any field of management or leadership, there are always nuances or considerations that are important to successfully implementing a plan. Some necessary procedures or refinements are sometimes too detailed for inclusion in a higher level plan. These kinds of considerations are discussed in Section IV, on implementation of the plan.

Note that this guide assumes that an external dependency is being formed or already exists. It does not directly address the broader question of how to decide whether or not to rely on an external entity for a business-critical service. In some cases, the external entity may have greater competence or capability in a particular area, which would ultimately lower the organization's risk exposure. However, the organization may have less flexibility to modify or tailor services provided by an outside entity than it would if it had fulfilled that function internally. Hidden long-term costs downstream, such as staff time and other vendor monitoring expenses, can also outweigh the benefits of outsourcing. In more serious cases, these costs may include failures such as breaches, outages, or fraud. The organization should consider, especially for its most essential services, all of these possible risks and cost implications and mitigate them through rigorous management and monitoring.

## **Step 1. Establish external dependencies support and strategy.**

Broad management support, participation, and adequate resource commitment are essential to the development of effective EDM. Managers developing an EDM strategy should obtain support and commitment from executives and leaders from across the organization, potentially including

- 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
- managers responsible for training and communications who can amplify the plans, strategies, and objectives of the program across the organization

Management support in an EDM plan is normally documented as a policy statement and preface to the plan which explains the emphasis and importance that executive leadership places on external dependency management. After management support is obtained, there are four primary inputs needed to develop a strategy for EDM:

- scope
- objectives
- enterprise requirements
- risk management planning



Managers should first consider how to scope the EDM program. This is often a choice among developing a dependencies program based on a single high-value organizational service, some set of the organization's services that constitute the core components of its mission, or some other set of risk, cost, or enterprise requirements. To establish a foundation for their scoping of the EDM program managers should identify the organization's high-value services (perhaps the top three to five) and their key supporting assets.

*It is highly recommended that organizations that have not previously developed a strategy for managing external dependencies start by focusing on a single critical service. Critical service in this sense means a set of the organization's activities whose disruption would prevent or seriously impede the organization's ability to carry out its mission. Even if the organization creates and implements an enterprise-wide strategy, a useful starting point for the strategy is to identify the organization's key high-value services.*

The organization and the plan writers should identify the objectives of the EDM plan. Normally, a basic objective is to ensure the resilience of the high-value service. Writing an objective statement, such as "The objective of the External Dependencies Management Plan is to effectively manage external dependencies risks in a cost-efficient manner and protect [high-value service] for the benefit of our organization and stakeholders," is a clear and useful first step. However, because EDM crosses a number of organizational functions and affects a number of stakeholders, managers developing the plan may want to consider other objectives that would benefit the organization or that would elicit a level of buy-in from other leaders in the organization. Examples include

- objectives relating to the technical diversity of systems. For example the organization may decide to engage external entities to protect its own services from vulnerabilities shared across common platforms.
- avoiding difficulties in certain legal jurisdictions that may affect the organization's rights in the event of a dispute with an external entity
- outsourcing areas not core to the organization's mission. Executives may decide to outsource secondary technology-supported functions so that it can focus on improving its efficiency or the quality of its principal product line.
- avoiding reputational risks related to the selection of certain external entities
- considering political or stability risks involved in forming relationships with entities in other countries
- considering the ability to scale the relationship to meet potential growth or quality demands when forming new relationships

Next the organization should document any enterprise requirements that will apply to all external dependencies. These may be based on a broad range of factors, business judgments, and inputs from other resilience processes (controls management, technology management, incident management, service continuity, and others). Enterprise requirements might include

- satisfaction of compliance obligations that extend to third-party entities (HIPAA business associate requirements are a common example from the health-care sector)
- maintenance of service continuity and incident management plans
- a level of financial stability desired in any external entity that supports the critical service

*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.*

Identifying the assets that support high-value services and their cybersecurity requirements can also help managers form meaningful enterprise requirements. For example, an organization might structure its



operations to prevent external entities from accessing critical information such as trade secrets or customer lists.

Finally, as part of the EDM strategy, the organization should document specifically how it will manage the risks of entering into and maintaining relationships with external entities. This part of the strategy should document the role of organizational risk managers in the external dependency management process and clarify the risk management responsibilities of the various parties or organizational components involved. In most cases managers who interface with external entities, typically in the areas of business operations, procurement, and IT operations, should work closely with enterprise-level risk managers to inform them and help make decisions.

*"Managing risks due to external dependencies involves understanding the nature of each external dependency and the specifics of how the organization may be affected by the realization of such risks." CERT-RMM<sup>6</sup>*

*The organization should plan its external dependencies risk management in conjunction with its overall risk management processes. See the Risk Management Resource guide, Volume 7 of this series, for detailed guidance on operational risk management and coordinated efforts that should be considered when managing external dependency risk.<sup>7</sup>*

The strategy for EDM should consist of guidance that organizational managers can understand and use on a daily basis, such as

- a clear statement from organizational management on the role and importance of EDM
- information on the scope of the strategy
- selection guidelines for external entities based on enterprise requirements
- restrictions on the size or location of suppliers
- identification of assets that must not be exposed to or accessible by external entities
- guidance on regulatory compliance
- critical information requirements for senior leaders (informs performance management)

The organization's managers should next develop the organization's formal EDM plan by documenting the processes described in the subsequent steps.

## **Step 2. Plan the relationship formation process.**

Forming relationships with suppliers sets a course for managing dependency risks over the lifecycle of the relationships. The quality of communications and collaboration can drive the management of external dependencies risk and establish effective support for the organization over the long term. Done well, collaborative relationships can spur efficiencies, information sharing, innovation, and growth. To make this a reality, the organization should carefully plan and document how it will form new relationships with external entities. This part of an EDM plan consists of several components:

1. approach
2. requirements development
3. external entity evaluation
4. approval authorities

The organization should first document its approach to forming relationships with external entities. A common and effective way to manage the resources and rigor associated with relationship formation is to use a risk-based approach. This means that external entity relationships for low-risk areas of the organization may receive less attention through practices such as standardized requirements, basic change management, less

rigorous cyber controls, and simple boiler-plate agreements. Forming relationships with entities that support high-value services, however, will receive a much higher level of attention and management. A key aspect of defining the approach is ensuring that all relationships are managed and tracked.

*In many organizations, business owners and developers attempt to go around or circumvent the EDM process. The individuals involved may perceive that the EDM process is burdensome, or these individuals may be naturally aggressive in attempting to provide new services or expand the business.*

*Regardless of the root cause, external dependencies managers must be on guard against this possibility. It can be mitigated by involving appropriate staff in the EDM planning and process so that they have input and a stake in it, and by instituting controls to guard against it.*

The plan should also specify how the organization will ensure that the correct requirements are developed for each external entity. Though enterprise requirements (discussed previously) are a very important part of the agreements between the organization and the external entity they usually form only part of the requirements for a particular external entity. The full set of requirements will be based on the specific service or support provided by the external entity and its role in support of the critical service or services that the organization provides to its own stakeholders. The following is an example list of requirements:

- resilience capabilities or level of cybersecurity maturity
- operational and technology availability and history/capability
- financial viability
- use and oversight of subcontractors
- disruption management capabilities (e.g., incident management and business continuity)
- environment factors (geographic, political, or weather event exposures)
- infrastructure exposures or risks
- cybersecurity threat and vulnerability management

Accurate requirements development depends on the involvement and input of the organizational personnel directly involved in or responsible for the production of the critical services that are the focus of the plan. This part of the external dependency management plan should document these personnel and their role in developing correct requirements for external entities.

The plan should document how the organization will evaluate and confirm that the candidate external entity can actually meet the requirements. Normally the particular steps or measures to do so will vary according to the risk level presented by the proposed relationship. Some example methods for evaluating the capability of external entities include

- third-party audit or assessment (process maturity or penetration testing)
- completion of standard checklists
- research on the external entity, for example, customer references
- direct examination of artifacts (e.g., the entity's incident response plan )

Finally, the relationship formation section of the plan should specify the approval authorities within the organization. As with external entity evaluation, the authority level required to sign off on new external entity relationships is normally commensurate with the risk level or exposure that the relationship presents.

### Step 3. Plan a process for identifying and prioritizing external dependencies.

*"An external dependency exists when an entity that is external to the organization has access to, control of, ownership in, possession of, responsibility for...or other defined obligations related to one or more assets or services of the organization."*  
CERT-RMM<sup>8</sup>

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 2: Risks due to external dependencies are identified and managed.</b>	
1. Are risks due to external dependencies identified and managed? [EXD:SG2.SP1]	ID.BE-1: The organization's role in the supply chain is identified and communicated.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

Having developed the strategy and plan for forming relationships the next step an organization should take is to plan how the organization will manage its existing or ongoing relationships with external entities. The purpose of having a process to identify and prioritize external dependencies is to ensure that the organization applies a suitable degree of controls and oversight to the right external entities and can sustain this ability over time.

#### A. Identify external dependencies.

Organizations increasingly rely on external entities for information and communications technology services, often to interact with assets that are essential to achieving the organizational mission. The organization should document a process for how it will reliably and sustainably identify existing external dependencies. This part of the plan should contain two sections:

- a statement about how the organization will approach dependency identification
- the staff roles that will be directly responsible for ensuring that the list of external dependencies is populated and updated

The Cyber Resilience Review's focus on services and assets and its underlying approach provide a framework for identifying external dependencies. By first understanding the organizational assets that most closely support the high-value services, managers can then identify those assets' related external dependencies. For example, an organization that depends on access to its customer data—a particular type of information asset—might focus on managing external dependencies associated with the data's custodianship, maintenance, protection, and support; raising the priority of the current controls and mitigations to prevent a data breach; ensuring the availability of the data; and mitigating data center outages or failures of the networks used to access the data.

*Table 1: Example Relationships Between External Entities and High-Value Assets*

External Entity	Relationship	High-Value Asset (Type)
A cloud service provider that	processes	customer purchase orders (information)
A data center that	houses	the server infrastructure (technology)
A maintenance company that	maintains	automated teller machines (technology)
A security company that	monitors and protects	the company's data center (facility)
A staffing company that	provides	database administrators for the big project (people)
A security company that	investigates	the background of employees entrusted with sensitive information (people)

A telecommunications company that	transmits	inventory and production data for a manufacturing company (information)
-----------------------------------	-----------	---

*An essential first step to managing external dependencies is knowing what they are, by developing a list of suppliers. The second step, prioritization of dependencies, determines which entities pose the greatest dependency risk; see the Controls Management guide and Risk Management guide, Volumes 2 and 7 of this series, for more information.*

The plan should next document the staff positions and roles that will help the responsible manager identify dependencies. Leveraging existing processes and communications channels where possible facilitates a smoother transition to a new or improved external dependency identification approach. For example, business continuity planners collect information on suppliers, contract groups are involved in managing existing suppliers and typically know which are key to the business, and senior executives have insight into long-term strategies in which suppliers play leading roles. Internal service or product line owners will also normally have a good sense of their dependencies. The following are some typical data sources and artifacts for dependency and supplier information:

- contracts and supplier agreements
- supplier and customer databases
- asset management database
- business continuity plans

While using internal personnel and data sources is usually necessary to identify dependencies it may not always be sufficient. It is not unusual, for example, for organizations to form relationships with multiple external entities for the sake of redundancy only to find that this support is subject to an unknown single point of failure. This may be the case when an organization signs multiple contracts with telecommunications providers only to discover that all of their traffic is over the same physical line, or that an unknown third party supports all of these providers.

## **B. Prioritize external dependencies.**

Organizations should next plan how to determine and rank the priority and importance of their external dependencies. The organization should use a risk-based approach that focuses resources on managing only those external entities that most directly impact essential services. For example, suppliers providing facilities maintenance may require less attention because they typically have minimal impact on service delivery and can be easily replaced should they fail to perform as expected. The prioritization process should be documented and typically includes the following steps:

1. Determine and standardize the prioritization criteria used to distinguish the relative importance of each dependency or external entity.
2. Establish thresholds for dependency grouping (e.g., Tier 1, Tier 2), for controls management and oversight.
3. Document the frequency of follow-up priority reviews.

*Prioritization criteria should be clearly established and standardized to help ensure that dependency risks are effectively identified and managed. Use of disparate or vague criteria can lead to misplaced priorities, confused strategies, and wasted resources.*

Identifying the most important services and assets provides the foundation for prioritizing and documenting dependencies. To help ensure that all key dependencies are considered, it is a good practice to consider each of the key asset types (technology, people, facilities, and information).

Criteria to consider when prioritizing external dependencies include

- the dependencies that support the most important assets (including technology, people, facilities, and information)
- the criticality of external entities to the essential service(s) or to assets that support the essential service(s)
- the sensitivity of the information the external entity manages or has access to (e.g., secret, confidential, personal)
- the availability of alternative suppliers or sources of services and products
- support of multiple services provided by single external entities
- external entity's role in supporting a key service
- reliance on the external entity to ensure and control the integrity, confidentiality, or availability of high-value assets
- the extent to which the organization would rely on the external entity during a disruption or crisis

These are examples of approaches to criteria that an organization could take to prioritizing external dependencies. All of them may apply and be useful in the organization or managers may decide that dependencies should be prioritized using only one or two defined criteria. Regardless of the actual criteria chosen the prioritization of external dependencies should reflect and be based on the prioritization of services and assets.

For these criteria to be useable and effective, the organization should determine how it will communicate internally about its various dependencies. For example, identifying situations where a single external entity supports multiple high value organizational services frequently depends on discussion and analysis between business and service owners in an enterprise.

*By establishing a process to identify and prioritize external dependencies, the organization can comprehensively analyze and manage the risks associated with key external relationships.*

## **Step 4. Plan for relationship management.**

The organization will next need to plan and document how it will manage ongoing relationships with external entities. Organizations often have rigorous processes around the formation of new relationships but fail to sustain that management for ongoing relationships. With effective relationships management essential entities can become collaborative partners who work closely with the organization to manage risk, cost, and change. Effective relationship management requires the coordinated effort of internal and external stakeholders. To make this process as efficient as possible the degree of oversight and governance applied to a particular relationship should be commensurate with the criticality of the assets and services the entity supports.

This section of the EDM plan normally consists of the following components:

- information and reporting requirements
- roles and responsibilities

Planning relationship management is challenging because external entities span varying types ranging from vendors contracted to carry out specific and well-defined duties for the organization, to shared infrastructure such as electricity providers, to federal government agencies and security services. In the case of contracted vendors the organization's ability to monitor and control the vendor may be significant. By contrast, with some external entities—for example public infrastructure or security services—the organization may not only have no control over the entity, it may also never have had the opportunity to select the external entity.

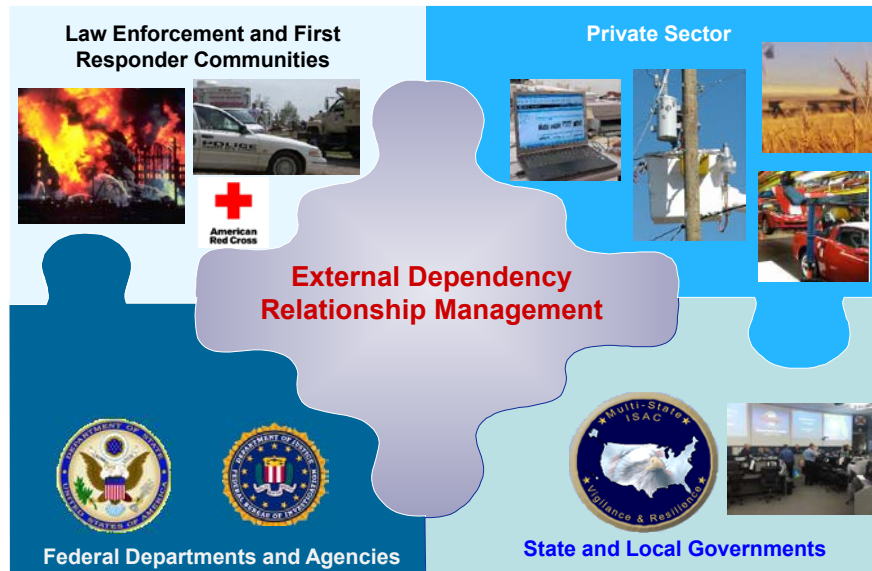


Figure 4: External Dependencies Management—Coordinating Relationships with a Variety of Entities

If any external entity, regardless of type, supports a key organizational service it is in the organization’s best interest to manage the relationship and the associated dependency risks.

The purpose of information and reporting requirements is to ensure that decision makers in the organization receive relevant, accurate information about the external entities they rely on as quickly as possible. In the case of contracted vendors this information is typically used to manage vendor performance and correct problems. In the case of shared or public infrastructure this information may be used to coordinate relationships, inform organizational risk management, or connect specific internal processes (e.g., vulnerability or incident management) to external entities as appropriate.

The organization should first document what information it requires to manage its set of external entity relationships. In the case of contracted vendors these may take the form of reporting requirements focusing on data, changes, or incidents pertaining to the vendor’s performance in support of the organizational service. Information requirements for public or shared infrastructure may be basic (points of contact and contact information) or sophisticated (threat and vulnerability information sharing, disaster planning).

The variety of external entities that an organization may depend on also means that relationship management planning may be performed by different parts of the organization. For example, it is not unusual for the business unit or IT operations to have information requirements that pertain to data-hosting vendors while the corporate security department does its own planning for public security authorities. Documented reporting requirements may include reporting by the external entities themselves as well as intra-organizational reporting.

Next, the organization should determine which job roles or units will have ownership of the various relationships and document these responsibilities, including in job descriptions. Staff responsibilities usually include monitoring external entity performance and correcting performance when necessary. Corrective options can range from simple dialogue with the supplier to transitioning the relationship to another vendor or even bringing the activity into the organization. Each option should correspond to the criticality of the relationship and the seriousness of the deficiency.

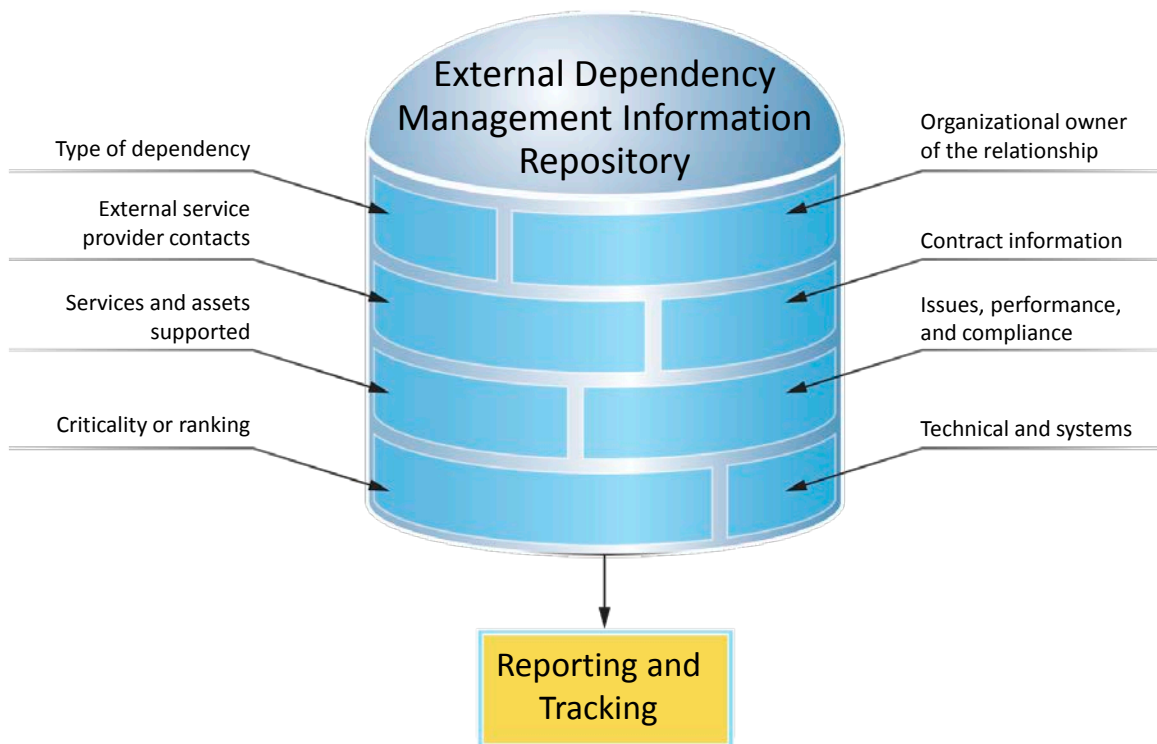
Planning and documenting requirements and roles for the management of external entities are essential parts of the external dependency management plan because external entities are often an extension of the organization itself. In addition, because of the dependence that many organizations have on external entities and the complexity of many business structures, external entity considerations may affect the planning of other resilience processes, for example

- change management and control—collaborating and working with the organization’s change management process
- planning service continuity and incident management to account for external dependencies
- information management controls—protecting the organization’s information and intellectual property in a manner that is consistent with its confidentiality and sensitivity
- human resources—reporting HR issues that might affect the organization or its services
- communication and notification—reporting incidents, events, or issues that originate with external entities and may affect the organization
- service continuity and incident management—understanding the organization’s reliance on external entities such that it can be accounted for when planning against disruptions
- situational awareness and threat management—identifying and disseminating information about threats that may originate from or affect external dependencies

## **Step 5. Plan an information management process.**

While some organizations have a list of external dependencies and suppliers it is often incomplete or outdated. A planned, consistent process for the collection and storage of key information helps to ensure that external dependencies documentation remains current and can be managed appropriately across supplier lifecycles. The significant challenge of collecting, maintaining, and reporting external dependencies information can be eased by establishing a central information repository.





*Figure 5: Information Management Repository*

Reporting from a managed repository can help keep external dependencies information accurate and complete. An EDM repository typically includes information such as

- type of dependency (e.g., data processing, power, software support, situational awareness information)
- name, location, and contacts for external service providers
- services and assets supported
- financial information on agreements and suppliers
- resilience requirements (i.e., confidentiality, integrity, availability)
- criticality or ranking of the external entity (e.g., high, medium, low)
- contract information (e.g., term, contract contact, key contractual obligations, or SLAs)
- documentation on known issues, performance, or compliance concerns
- technical overview (e.g., systems, networks, and information/data managed)
- internal owner of the relationship

The external dependency information management process depends on the clear assignment of ownership. Accountability and responsibility for the overall information management process might best be assigned to the individual or group responsible for the overall external dependency program. The more granular level of information management—the collection, reporting, and maintenance of dependency information for each relationship—is also critical to the management information process and typically falls to the owner of the supplier relationship. For relationships whose internal ownership is not easily defined, such as with government, emergency responders, and critical infrastructure providers, information management responsibility may need to be assigned by those responsible for the broader EDM program.



## Output of Section III

	Output	Guidance
✓	Enterprise objectives, strategy, and plan for EDM	Organization-wide program, standards, and documentation for performing EDM activities
✓	Scope of EDM plan	This statement defines what the EDM plan is intended to address. The 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. Organizations that are not sure where to start might begin with one of their essential services and the assets that directly affect its performance. This approach can allow an organization to begin addressing external dependencies in areas most important to achieving the organizational mission and begin mitigating their impact while management practices are being more fully developed. If the organization has participated in a Cyber Resilience Review (CRR), it may be beneficial to begin with the essential service addressed during the CRR.
✓	Management support	An endorsement by senior management for planning and focusing on EDM and the implementation of related processes. This often appears in the form of a policy statement and the commitment of adequate support and funding.
✓	Key foundational processes and plans documented	<ul style="list-style-type: none"> <li>• A documented EDM strategy and plan</li> <li>• Process to identify dependencies</li> <li>• Process to prioritize dependencies and external entities</li> <li>• Requirements to document dependencies and related information</li> <li>• Enterprise and service-specific requirements documented</li> <li>• Process for the formation and management of external relationships</li> <li>• An external dependency information management process</li> </ul>
✓	Linkage to other management processes established	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.



## IV. Implement the External Dependencies 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 an EDM plan.

	Input	Guidance
✓	Objectives and plan	The objectives and plan provide direction for the management of external dependencies. For example, the plan might detail how the organization will identify external dependencies, the tiering structure used to prioritize external dependencies, and the key stakeholders to be engaged in dialogue on status, events, and issues.
✓	Articulated strategy	<ul style="list-style-type: none"> <li>• Clear objectives and the approach used to achieve those objectives</li> <li>• Relationship to other enterprise standards, for example, risk tolerance and compliance obligations</li> <li>• Information management and reporting requirements and approach</li> <li>• Communications processes that engage stakeholders and facilitate the program</li> </ul>
✓	Lists of stakeholders	<p>The list of stakeholders should align to the program objectives and include all appropriate internal and external entities. Potential candidates include</p> <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>• service continuity</li> <li>• information security</li> <li>• contract management</li> <li>• legal</li> <li>• vendors</li> <li>• shared and public services providers</li> <li>• regulators and internal auditors</li> </ul>
✓	Management support	An endorsement by senior management supporting the establishment and implementation of an EDM program
✓	Externally imposed requirements	Regulatory requirements that affect the organization's external dependencies
✓	Budget for EDM	<ul style="list-style-type: none"> <li>• Identification of available funds to perform EDM, 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>

The EDM plan discussed in the previous section provides the organization with the framework for managing external dependencies. It provides clarity about the objectives and importance of EDM, documents how the

organization will approach key activities in EDM, and specifies the process's high-level roles and responsibilities. This section provides guidance concerning how to implement the EDM plan in the organization, including considerations for managers. These include areas related directly to implementation, for example assigning responsibility for implementation, determining whether or not the plan is actually being implemented, and maintaining procedures that are too granular or detailed to specific external entities for inclusion in the overall plan.

In addition, the implementation guidance below addresses considerations and nuances that are normally difficult to plan for, such as ways of thinking about external dependencies and the need to think about them more holistically, deeply, and broadly. The guidance also include recommendations that focus on particular pitfalls that organizations commonly experience during EDM, for example the need to ensure that tools such as legal contracts, which are sometimes not under the direct control of the implementing manager, are written in such a way to reinforce the operational resilience of critical services.

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

As with any organizational process or improvement plan, clearly assigning responsibility is an essential element for success. Any one of a variety of internal entities, such as a single executive, a committee, or a steering group, can be responsible for implementing the EDM plan. Because EDM can encompass a range of organizational components (business units, contracts, legal, risk, operations, information security, etc.), ownership might best belong to a group that oversees risk, such as enterprise risk or operational risk. Each organization must consider the best fit for its culture and business model.

The responsible organizational entity must be able to implement the EDM plan and distribute accountability for it across virtually all levels of the organization. The responsible entity should widely distribute the plan, its objectives, and its target dates. Training should be considered as a core activity to facilitate a common understanding of the plan across the various groups that will support its implementation. Leveraging existing management resources, project management processes, reporting, as well as training existing management personnel can help integrate dependency management into the organization. Existing organizational resources may include

- business unit managers
- project managers
- operations managers
- resilience managers
- stakeholders
- information and physical security leaders
- contracts and legal teams
- asset management process owners
- operational risk managers and teams

An important step in implementing the plan across the organization is to review the job descriptions and performance rating criteria of all the organizational positions that will be involved in EDM. The internal executive or component should then work with the responsible managers to ensure that job duties and performance criteria that directly support the plan are included in the appropriate job descriptions.

Suggested implementation management practices also include the following:

- Communicate dependency management plan objectives, strategies, and accountabilities from the executive level.
- Provide regular awareness communications on the importance of EDM.
- Establish a central repository for policy, standards, procedures, plans, and supporting documentation.
- Engage stakeholders and define ownership of external dependencies areas and mitigations.
- Document implementation action/project plans with timelines.
- Develop management reporting and metrics for implementation performance.
- Provide a physical or virtual forum for project updates, issues identification, and resolution tracking.
- Conduct regular reviews of the external dependencies implementation plan and modify it as necessary.
- Establish a process to communicate or escalate significant issues.

Managing the implementation of the external dependencies plan can be challenging but clearly delineating objectives and timelines and assigning them to specific individuals can help. Reporting on the progress and issues associated with implementation helps foster visibility and stakeholder engagement.

## Step 2. Establish and maintain implementation measurements.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: External dependencies are identified and prioritized to ensure sustained operation of high-value services.</b>	
1. Are dependencies on external relationships that are critical to the service identified? [EXD:SG1.SP1]	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
3. Are external dependencies prioritized? [EXD:SG1.SP2]	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
<b>Goal 5: Dependencies on public services and infrastructure service providers are identified.</b>	
1. Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified? [EC:SG4.SP3]	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
2. Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4]	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.

After responsibility is assigned the next basic implementation practice is to develop the set of internal measurements that organizational managers will use to determine whether or not the plan is actually being implemented. Managers will need to base these measurements on the EDM plan itself and the structure, objectives, and culture of the organization. The following is a non-exclusive list of measurements that can be used:

- percentage of job descriptions that accurately reflect the EDM duties of the staff member
- completeness of fields in EDM information system
- number of personnel trained on the EDM process
- percentage of third-party audits completed on external entities
- percentage of identified requirements that are included in formal agreements with external entities

As with any type of measurement of business or security performance, managers must have a solid and nuanced understanding of what they hope to learn by measuring their organization's implementation of EDM, and they must be cautious against creating unintended consequences or incentives. For example, parties responsible for including requirements in formal agreements with external entities could drive that measurement higher if they do not thoroughly evaluate services and requirements, resulting in a minimal and

generic set of requirements. Using measurements like these to encourage the flow of information about the process, rather than as a driver for punitive action against staff, can alleviate these concerns. Regardless of its potential complexities, a set of defined measurements or data collection objectives can help managers know whether the process is actually being implemented and actually meeting the objectives for the program.

### Step 3. Formalize relationships with external entities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 3: Relationships with external entities formally established and maintained.</b>	
1. Have resilience requirements of the critical service been established that apply specifically to each external dependency? [EXD:SG3.SP2]	ID.BE-1: The organization's role in the supply chain is identified and communicated. ID.BE-5: Resilience requirements to support delivery of critical services are established.
2. Are these requirements reviewed and updated? [EXD:SG3.SP2]	ID.BE-1: The organization's role in the supply chain is identified and communicated. ID.BE-5: Resilience requirements to support delivery of critical services are established.
3. Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3]	ID.BE-1: The organization's role in the supply chain is identified and communicated. ID.BE-4: Dependencies and critical functions for delivery of critical services are established. ID.BE-5: Resilience requirements to support delivery of critical services are established.

As discussed above in Section III the EDM plan should drive how the organization forms new relationships with external entities. The specific requirements for forming new relationships should draw on both the organization's set of enterprise requirements and the specific requirements of the organizational service being supported and the particular vendor.

Supplier or vendor relationships are the most common external dependencies and are typically bound by legal agreements or contracts. Figure 6 provides an overview of the critical role the agreement and contracting process has within the broader EDM process. Contracts and agreements codify what is expected of the vendor and the contracting organization, as well as remedies for breach by either party. Contracts should clearly define expectations, means to measure performance, and means to recover damages.



From a resilience perspective, formal agreements should also include performance standards and the ability to modify or change specifications and standards over the life of the agreement. Performance standards should be included so that the external entity knows how it will be evaluated relative to satisfaction of the contract. Including language that allows terms and specifications to be updated is very important because the resilience requirements that apply to the external entity may change and require modification over time. The appropriate organizational staff should be involved so that the terms and specifications of these formal agreements can be as effective as possible. Individuals most familiar with the resilience requirements and specific technological requirements of the high-value services being supported must be directly engaged in contract negotiation. These personnel should actively communicate with the legal and procurement departments and have a stake in the process of formalizing relationships.

For example, one of the basic purposes of any legal contract is to drive the desired behavior of the contracted entity. Contracts and SLAs often fail to do so effectively however, especially in contracts with technology-based service providers, whose specific duties and required standards may be unclear. Vague contract language (“reasonable security” or “meet industry standards”) frequently confuses rather than clarifies.

Organizational managers and technical staff can strengthen contracts and their efficacy by asking direct questions as contracts are being formed. For example, in response to contract terms specifying “reasonable industry standards” some helpful questions might be

- What industry standards, specifically?
- Assessed by what entity, and how?
- Assessed when, and how often?

#### Step 4. Identify and prioritize dependencies.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 3: Relationships with external entities formally established and maintained.</b>	
4. Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4]	ID.BE-1: The organization's role in the supply chain is identified and communicated.
	ID.BE-5: Resilience requirements to support delivery of critical services are established.
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities.
<b>Goal 4: Performance of external entities is managed.</b>	
2. Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1]	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
	ID.BE-1: The organization's role in the supply chain is identified and communicated.

Identifying and prioritizing dependencies are essential management activities that help the organization determine the

- dependency exposures that should receive the most attention
- type and extent of controls to be put in place
- extent of resource investments needed to manage associated risks

As discussed above, dependencies may arise from the organization’s use of suppliers of services or products in support of its mission. The organization may have great freedom when selecting suppliers or its direct discretionary control may be limited by factors such as geographic location, industry sector, or service type.



Regardless, the dependency landscape is increasingly complex and requires careful, risk-based identification and prioritization. Figure 7 provides a simplified illustration of the multi-supplier dependency environment faced by today's organizations. Generally dependencies or suppliers are one of the following types:

1. vendors—Entities that have been chosen by the organization, with which the organization has typically negotiated an agreement. Examples include providers of raw materials, labor, consulting, maintenance, hardware, software, and facilities.
2. shared infrastructure—The supplier provides its services to a region or group. Agreements are usually standardized and are virtually the same across the customer base. Examples include power, water, telecommunications, trade groups, and consortia.
3. public—Typically these relationships are with a government entity such as a state, local, or federal agency and are not governed by a contract or agreement. Examples include security services (fire, police) and transportation networks.

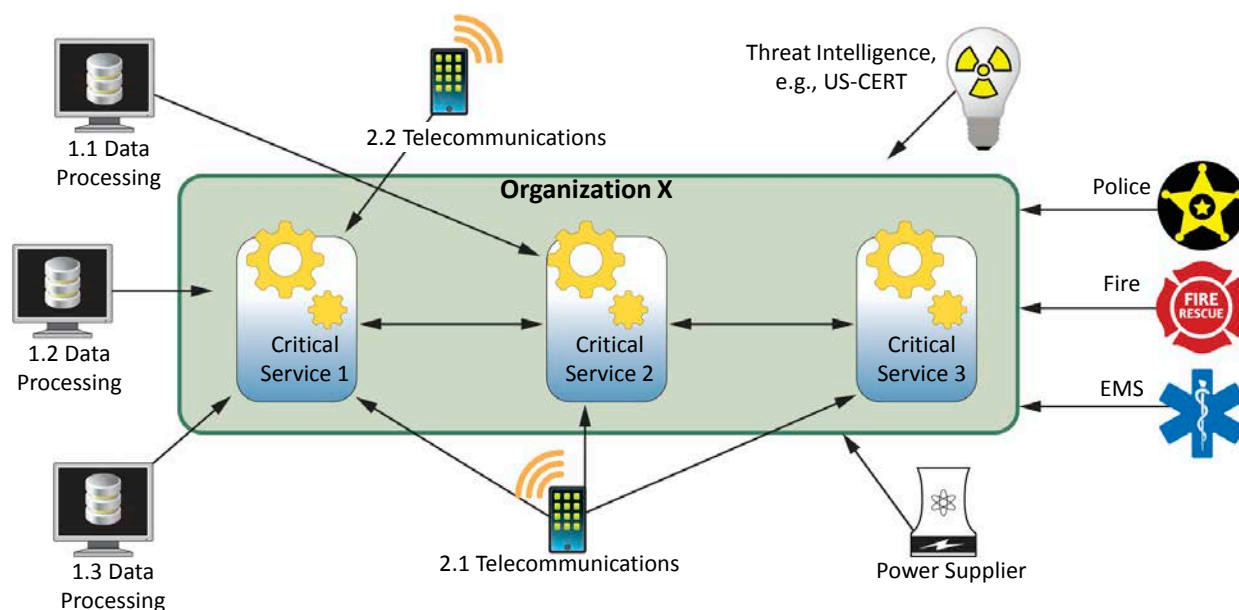


Figure 7: Example of Supplier Dependencies

Organizational managers often identify and are aware of external dependencies during their daily, routine interactions with external entities. However, managers should strive to deepen and broaden their understanding of the external entities that their organization actually relies on. Doing so will mitigate the risk of missing less obvious dependencies that are equally important to the organization's high-value services.

A deeper understanding of external dependencies means considering the second-tier entities that the organization's vendors may rely on. For example, it is not unusual for organizations to contract with more than one telecommunications provider for redundancy only to find after a disruption that each vendor relied on the same third party, such as the owner or operator of the physical telecommunications infrastructure. Managers with a deep understanding of external dependencies must know the structure of the vendors' business or operations.

A broad understanding of external dependencies means considering external entities that are not directly contracted with the organization or the organization's vendors, such as emergency authorities. In that example, broad understanding of this dependency would account for the planned actions of emergency authorities in the event of a disruption and how those actions might affect the organization.



Dependencies among the organization's external dependencies and their services may lead to unexpected impacts that are difficult to manage. One common way to address this type of supply chain risk is to hold each external supplier accountable for managing its subcontractors, developing dependency priorities, and monitoring for changes that may affect the supplier's own EDM process and related supplier risk. The only way to be sure these activities are happening is to constantly communicate with, monitor, and manage external entities.

A related best practice is to examine the organization's set of external entities for common modes of failure and single points of failure. Common modes of failure exist when multiple external dependencies are vulnerable to the same threats or conditions. Single points of failure occur when the organization depends on only one external entity to support its high-value assets or services. These useful practices also rely on building solid relationships with external entities, good communication, and a basic understanding the high-value external entities themselves.

The organization's planned approach and process for identifying external dependencies can guide managers toward thinking more inclusively about dependencies. The dependency identification process is most effective when it uses a common set of variables, characteristics, and specifications established for the organization. Utilizing a common identification process that has close ties to the organization's external dependencies and risk management plans can help ensure that the organization takes a consistent, systematic approach to managing dependencies and supporting the organization's mission. Without a common basis for dependency evaluation organizations may develop unclear, misplaced dependency priorities and suffer risk management failures.

*Grouping external dependencies into categories can simplify the process of managing the risk and overseeing suppliers.*

## Step 5. Maintain requirements.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 4: Performance of external entities is managed.</b>	
1. Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1]	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.
	ID.BE-1: The organization's role in the supply chain is identified and communicated.
3. Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2]	ID.BE-1: The organization's role in the supply chain is identified and communicated.
4. Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]	ID.BE-1: The organization's role in the supply chain is identified and communicated.

Having requirements is a foundational part of managing the resilience and security of any service. Requirements form the basis for the provider selection process and for agreements and contracts that codify the terms of the relationship. To strengthen the quality of the overall relationship formation and management process, the organization should maintain clear and measurable external-entity requirements that support the critical service.

*Clear and unambiguous communications with suppliers on requirements, information exchange, change management, and performance are key activities for relationship management and are crucial to effective external dependencies risk management over the supplier management lifecycle.*

Unfortunately, requirements can become stale; the organization should periodically review the currency of requirements, particularly for the most critical suppliers and high-risk dependency areas. Requirements that

were useful at the start of a vendor relationship often become quickly outdated, usually because the facts or assumptions on which requirements were originally based have changed. For example, these changes may occur when

- the service or product supported by the external entity becomes successful and more important to the organization, increasing its criticality
- for cost saving reasons, other vendors that provided redundancy to the critical service are eliminated, leaving one vendor as the single point of failure
- internal staff and stakeholders become completely reliant on a new, IT- or web-based internal application, and older, manual methods are phased out
- changes at the external entity itself (for example, strained capacity or business or market changes) encourage the organization to institute new or strict requirements

When an organization identifies changes to requirements it should update those requirements in any formal agreements that govern the external entity relationship in question. Of course, organizations are often not able to modify original agreements; the original contract might not have included the right to update requirements, or the vendor might perceive the contract as small, leaving the organization with little recourse. In such cases risk managers should be made aware of the gap in requirements and the problem should be managed and mitigated like other risks.

Requirements are also important for dependencies with public and shared infrastructure providers, though the organization's ability to negotiate and enforce their requirements is typically limited with these entities (see Step 6D, which provides additional information on public and shared infrastructure suppliers).

## Step 6. Manage ongoing relationships.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: External dependencies are identified and prioritized to ensure sustained operation of high-value services.</b>	
2. Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1]	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.

An established plan or process should drive the objectives and approach to relationship management (see Section III, Plan for External Dependencies Management). The implementation of the EDM plan relies heavily on the relationship management components of the process.

Relationships with external entities may be established or managed by different business units or stakeholders in the organization making it vitally important to structure the relationship formation process consistently and in accordance with the external dependencies plan. It is not unusual to find a particular business unit or manager attempting to circumvent the dependency management plan in order to advance specific objectives (e.g., cost, growth, local business unit priorities). External dependencies risk policies, standards, plans, training, and oversight should be organization-wide to ensure consistency of approach and accountability for failure to follow policy.

It is not uncommon for important requirements relating to the organization's high-value services to be missing, weak, or vaguely addressed in formal agreements. For example, the eventual importance of the external entity may not have been apparent when the agreement was signed or a disparity in negotiating power may have limited the organization's original agreement. It is also very common for security or resilience requirements to take a back seat to other priorities such as cost or delivery commitments. Ensuring that information on external

dependencies is as current, accurate, and complete as possible is a foundational aspect of a process for monitoring the risks associated with dependencies.

#### **A. Establish ownership.**

The organization should establish internal ownership of each relationship to provide coordination and accountability across its lifecycle. Relationship owners provide coordination points to external entities to facilitate not only performance management and risk management but also communication and collaboration more generally. Ownership of a relationship is usually more effective when it includes specific responsibilities concerning the associated external entity, for example

- reviewing, vetting, and refining formal agreements
- developing requirements
- monitoring and reporting external entity performance
- executing aspects of change management, for example, changes to SLAs and other agreements
- interfacing with internal organizational processes such as incident management or service continuity

It may be appropriate for the manager of a principal service or product to own the external-entity relationships that directly support it. In other cases the defined role of an organizational component might dictate its ownership of certain external relationships. For example, physical security teams are typically responsible for internal alarm monitoring and often benefit from relationships with external police and firefighting providers which can be leveraged in both normal and emergency situations to share information, monitor performance, and reduce risks to the organization.

Another example is the organization's information security team which will often work with private and public groups to share information. Building relationships and collaborating with agencies, such as the United States Computer Emergency Readiness Team (US-CERT) or the National Cybersecurity and Communications Integration Center, can provide valuable insights, risk assessments, and mitigation suggestions to benefit the entire organization.

#### **B. Define procedures.**

The external dependencies implementation plan described in Section III documents the structure for managing external dependency risks. Relationship management across the lifecycle of external supplier engagements joins the plan and the day-to-day supplier interactions to establish how the implementation will meet the needs of the organization. Effective execution of the plan requires the development of detailed processes and procedures to implement that plan. The EDM plan typically will not define many of these procedures because their actual execution may depend on the type of specific external entity and the typical, applicable, and relevant business practices. Relationship owners will need to define these procedures, including details about the following areas:

- initial dialogue with the entity to define and clarify the organization's priorities
- requirements definition and qualification gathering
- communication of specifications and control requirements to supplier
- validation of external entity's capabilities to meet requirements and verification of qualifications
- performance monitoring and audits
- communication of performance results and required corrective actions
- change management communication and coordination
- risk information exchange and collaborative efforts to manage those risks

- requirements and agreement adjustments and renewals
- termination or alteration of relationship, or transition to another supplier

### **C. Manage performance.**

Relationship management with contracted vendors typically focuses on performance management: ensuring that the external entities meet their obligations to support the organization and taking appropriate steps when they do not. Like other parts of EDM, requirements make this practice easier. If the organization has already documented how and to what extent it relies on the entity in the first place (as outlined above in Steps 3 through 5), then evaluating external entity failure becomes easier and faster.

Effective performance management of external entities requires the reporting of their performance deficiencies. To provide context, reporting should ordinarily include an estimate of the deficiency's actual or potential impact on the organization. Reporting should also identify trends, resolution timelines, and the internal owners responsible for managing the external supplier. Contract, technical, security, and legal support teams should engage in the reporting where appropriate to help manage the overall risk of the relationship. Standards for reporting, as well as the identification those responsible for the relationship's management, make the reporting of performance deficiencies easier and more effective.

Organizations should regularly communicate with key external suppliers and stakeholders to resolve performance issues or challenges in fulfilling requirements. Establishing an open dialogue with suppliers can foster trust and collaboration that can be essential to managing external dependencies risks. Constant, effective communication on performance can prevent service disruptions or other costly outcomes such as relying on the legal system to resolve vendor issues. Effective relationship management and communication are particularly important in relationships where agreements with suppliers do not contain financial or other incentives for the supplier to uphold organizational requirements.

The organization should identify corrective actions to address issues, gaps, or weaknesses in external entity performance. To ensure all concerns are resolved in a timely manner the organization should systematically track identified, open items. If corrective actions are problematic or the issues, gaps, and weaknesses remain unresolved, the organization should consider deploying other risk management mitigations, reviewing requirements, or transitioning to other suppliers or approaches.

If key external entities fail to satisfy resilience requirements the organization should first analyze the failure's impact to the critical service. The results of the impact analysis should feed into a process that determines if corrective action, when considered in a broader context, is productive or required. Understanding root causes and impact improves the process of managing external entities by ensuring the program remains effective and robust in the face of constant change. Examples of corrective actions include

- discussion with the external entity
- enforcement of the SLA or other contracts
- financial penalties or payment freezes pending resolution
- identification of improvements in the EDM activities
- escalation of issues that require higher level management input for resolution
- transition to alternative service providers

The organization should establish ongoing communications with key suppliers not only to monitor performance but also to manage changes, quality, cost, and evolving threats or risks. To ensure that any

performance or contract compliance issues are actually remedied the organization should also routinely review the status of external entities and any actions taken to correct their performance.

*Performance management not only provides an opportunity to monitor and resolve issues, but it is also a forum for collaborative dialogue with suppliers and stakeholders to address challenges such as change, evolving threats, and risk.*

Beyond strictly managing external entity performance, organizations should consider monitoring external entities for changes or factors that may affect the service or product supported by the external entities.

Monitoring activities may track external entities'

- financial condition, viability, and internal financial controls
- oversight of subcontractors
- change management and problem management processes
- technology and security controls
- business continuity and incident response plans
- disruptive incidents that affect the organization
- compliance activities and audit results
- HR procedures, including turnover, background checks, ethics, and training activities
- satisfaction of specifications and quality expectations of service provided
- insurance coverage and terms

#### **D. Manage shared infrastructure or public services.**

Organizations may have some ability to control the behavior of many of their contracted external entities. By contrast, organizations usually have very little meaningful control over shared or public external entities such as electric and water utility companies, police and fire departments, state and local emergency operations centers, and security services. These entities usually do not consider any individual organization's requirements when providing services and in most cases the organization will have little ability to negotiate the terms of the relationship. Managing relationships with these shared and public suppliers requires a collaborative approach and a somewhat different set of tools.

*Shared and public services providers may be a source of dependency risk. They require a broader set of risk mitigation actions in addition to the oversight of supplier agreements. This may include internal risk mitigations and participation in collaborative initiatives such as Sector Coordinating Councils or industry groups.*

Public agencies such as emergency responders, police, or fire services do not normally enter into service agreements with specific organizations. Organizations usually begin to manage the dependency risk associated with these public services by opening a dialogue with them and finding opportunities to work together, for example, by participating in simulated disruption response exercises, providing input to local response plans, and attending training on event response procedures. Establishing collaborative relationships with local and national groups focused on information sharing and incident response (e.g., InfraGard, local emergency operations centers, regional coalitions) is an excellent strategy not only for improving the risk management support these groups provide, but also for building stronger information sharing and response partnerships.

Below are examples of tools and mitigations that an organization should consider for shared infrastructure and public services or when agreements and contracts do not adequately manage dependency risks:

- develop and document hypothetical requirements for these services as a way to identify and analyze risks
- develop internal alternatives (e.g., backup generators, water well, satellite-based communication circuits, private security and fire protection)

- establish relationships with multiple, alternative suppliers and develop a plan for transitioning from one supplier to another
- utilize suppliers across a variety of regions or international locations
- leverage regulatory agencies and industry groups to facilitate communications, strategy development, service improvements, and risk mitigations

## 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>
✓	EDM plan implemented	<ul style="list-style-type: none"> <li>• Organizational risk management activities and operations include dependency management</li> <li>• Formation of entity relationships is conducted based on the plan</li> <li>• Process in place to identify and prioritize dependencies</li> <li>• Process in place to establish and maintain requirements</li> <li>• Processes or systems are in place to collect and manage dependency information</li> </ul>
✓	Stakeholder engagement and communication	<ul style="list-style-type: none"> <li>• Stakeholders identified and engaged in the implementation of the program</li> <li>• Two-way communication to facilitate the integration of the risk program into the organization</li> </ul>
✓	Formation and management of external entity relationships	<ul style="list-style-type: none"> <li>• Enterprise and service-level requirements included in formal agreements</li> <li>• Supplier oversight, governance, and monitoring established</li> <li>• Shared and public infrastructure requirements documented</li> <li>• External entity performance managed</li> </ul>
✓	Training and awareness	<ul style="list-style-type: none"> <li>• Processes established to provide risk training in support of the program objectives</li> <li>• Dependency management plan objectives and strategies are widely communicated and understood</li> </ul>



## V. Monitor and Improve External Dependencies 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 EDM.

	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>Ensure stakeholders are engaged and that interactive dialogue is ongoing</li> <li>Determine if the level of external dependencies risk is within the organization's tolerance parameters</li> <li>Identify needed changes in strategy, oversight, governance, and reporting</li> <li>Ensure that emerging or evolving dependency issues are considered</li> </ul>
✓	Requirements and related documentation for external entities	<ul style="list-style-type: none"> <li>EDM information is current and effectively managed</li> <li>Program assessment and risk review</li> <li>External dependencies risk measurement and analysis</li> <li>Stakeholder perspectives on supplier assurance and approach</li> </ul>
✓	Incident and issue reports related to external entity performance	<ul style="list-style-type: none"> <li>Identify any trends that may suggest that adjustments need to be made in the relationship engagement, monitoring, and management procedures</li> <li>Review supplier reporting to identify areas of poor performance, escalating risks, or communications challenges</li> <li>Monitor processes used to engage and coordinate with relationship owners</li> </ul>

The organization should have a process for monitoring the performance of external entities. At the most basic level this monitoring should verify that external entities are satisfying the requirements established by the organization, whether they are formally codified in agreements with the entities or not. At a more strategic level, however, monitoring the trends within the day-to-day management of external entities can inform a better understanding of how to improve the process and the overall external dependency management program.

### Step 1. Define effectiveness measures.

Organizations should monitor, measure, and report on EDM activities to ensure that they are not only being conducted in accordance with planned activities, but are effective in fulfilling the goals and objectives of the program. To measure the effectiveness of the EDM program the organization will need to document the program's goals and consider what metrics about EDM to collect. These are normally drawn from and based on the stated goals, risks, and objectives that appear in the EDM plan. External dependency management, like other risk programs, can add overhead and cost, making it important to track and confirm that the activity is providing the value specified.

Some examples of metrics concerning program effectiveness include

- external dependencies risks or potential risks that remain unresolved
- open or unresolved high-risk supplier issues
- aging statement for corrective action reporting
- count of external entity relationships formed outside of the process
- emerging threats or risks that may affect key dependencies or suppliers
- number and frequency of critical service outages traceable to external entities
- percentage of external entities that have successfully passed third-party audits
- percentage of missed deliveries or shipping delays from external entities
- contracts or agreements that did not follow established procedures or policy
- percentage of SLAs across key external entities (e.g., tier 1 and tier 2 suppliers) that include resilience requirements in their agreements
- response times and other metrics relating to business continuity or cybersecurity drills conducted with external entities

In addition to using defined measures it is useful to look for trends or incidents that may suggest failures in EDM procedures and processes. For example, the occurrence of availability problems involving technology suppliers or an increase in contract compliance issues may be linked to weaknesses in EDM processes. It is also useful to explore disruptive events involving suppliers to determine the root cause and identify actions that may avert or limit future problems such as control failures, procedural violations, or new cyber threat vectors impacting the organization.

## **Step 2. Detect, analyze, and correct process exceptions.**

Managers should periodically review the dependencies program to detect, analyze, and correct procedural exceptions that may be creating risk. A common challenge is the formation or modification of relationships with external entities without obtaining the proper management review and approval. Detecting this type of exception can be challenging but the use of systematic internal accounting and process controls may be particularly effective; periodic internal auditing can also help in this regard.

After a process exception is corrected or otherwise addressed administratively the manager should understand the root cause and the control failure: how was the relationship formed outside the process? Program reporting, issues, and exceptions should be updated regularly and reviewed with operations personnel, stakeholders, and business risk managers. Implementation measures, discussed in Section IV, can be used to determine adherence to plan.

Process exceptions may be addressed singly in response to particular situations. Alternatively, analyzing the effectiveness of and exceptions to EDM management may stimulate broader efforts to refine EDM objectives and strategies. Leadership across the organization must continually evaluate dependency management failures, successes, trends, exceptions, and objectives to keep the program on track. The information, analytics, and reporting that result from detecting, analyzing, and correcting process exceptions provide the core foundation supporting the successful management and mitigation of dependency risk.



### **Step 3. Report and review the program with stakeholders.**

EDM is an enterprise activity requiring engagement and input from across the organization. The right stakeholders must play a central role in refining and maturing the program. To facilitate stakeholders' active engagement reporting on dependency risks and processes must be useful and actionable. Stakeholder feedback and input must be actively gathered, vetted, and, where appropriate, actioned.

Different types of stakeholders may require different types of reporting and engagement. Some stakeholders (board, C-suite, enterprise and operational risk committees, external regulators, and shared and public supplier executives) may require less frequent, more summarized reporting that is oriented toward executives. Often this reporting and dialogue consists of overviews of program status against objectives and strategic direction as well as the gathering of feedback on the program's design and direction.

The reporting to midlevel managers is generally more frequent and detailed to help ensure that day-to-day activities remain on track. Ownership, status, and timeline information are key aspects of midlevel reporting. As the EDM objectives, strategies, or plan change it is crucial to inform midlevel managers and give them an opportunity to provide input. Typically the mid-level managers will be the most effective at translating bigger picture strategies and plans into more detailed procedures and operational implementation activities. This group can also provide valuable feedback to identify challenges and issues that may result from refinements or changes to EDM strategies and plans.

### **Step 4. Improve the EDM program, plans, and procedures.**

To mature the organization's EDM capability the responsible manager should propose any necessary changes and improvements during periodic reviews. The manager should communicate with and engage all stakeholders to help ensure their support, input, and buy-in for changes. As with the initial creation of the EDM plan, senior management support is essential for any major proposed changes.

Organizations may choose to improve their EDM capability to different levels of maturity. Typically these improvements are achieved by increasing the consistency and repeatability of the program processes across the enterprise. Of course, making improvements requires increased investment, usually cost or expense, in the short term. Sometimes the pressure to minimize initial costs can be a barrier to positive, long-term outcomes such as lower risk, increased efficiency, lower long-term cost, compliance, and market differentiation.

Each organization must determine how much focus and investment to make in its EDM program. A key tenant of resilience management is establishing the right balance between risk and cost to the organization. Each situation is unique and often depends on the larger business context. Resilience and risk management investment decisions often have long-term consequences and require coordinated interaction with key stakeholders and the organization's executives. Maturity and resilience management generally involve

- maintaining consistent results from key processes
- standardizing key processes across the organization
- building key processes into the organizational culture so they are retained during times of stress

A large organization may wish to standardize all of its essential EDM practices and activities across disparate business units. This can help ensure that relationships are managed in accordance with the enterprise's needs and in a manner that reflects the EDM objectives, strategies, and plan. For example, to ensure a consistent approach across the enterprise, an organization could standardize the following aspects of EDM across all business or geographical units:

- selection of external entities (vendors) based on enterprise requirements
- cooperation and collaboration on information sharing, change, and threat management
- performance monitoring and resolution
- relevant processes around incident management or service continuity
- relevant reporting and other requirements

*A principal challenge of effective resilience and external dependency management is getting all areas of an organization to coalesce around common goals, practices, and objectives. Consistency across the organization is essential to achieving the organization's goals and objectives.*

The organization may wish to collect experiences, lessons learned, successes, and best practices and disseminate them across the organization through communication and training. The organization may need to target this knowledge to the appropriate staff depending on their specific role. Disseminating and reinforcing this knowledge across the organization can help ensure that staff adequately retains important skills and knowledge so that EDM processes can remain effective during times of stress such as service disruptions, staff changes, data breaches, and natural disasters.

Just as executive involvement, buy-in, and emphasis were important aspects when creating the EDM plan they are also intrinsic and important when improving the process. Higher level executives should be made aware of issues relating to EDM. As part of their review process, they should also be evaluating not just the risks of particular external relationships, but the risks of deficiencies in the EDM process and organizational capability themselves. Because of their responsibility for the future and direction of the organization and their awareness of the organization's role as critical infrastructure this is properly an executive function.

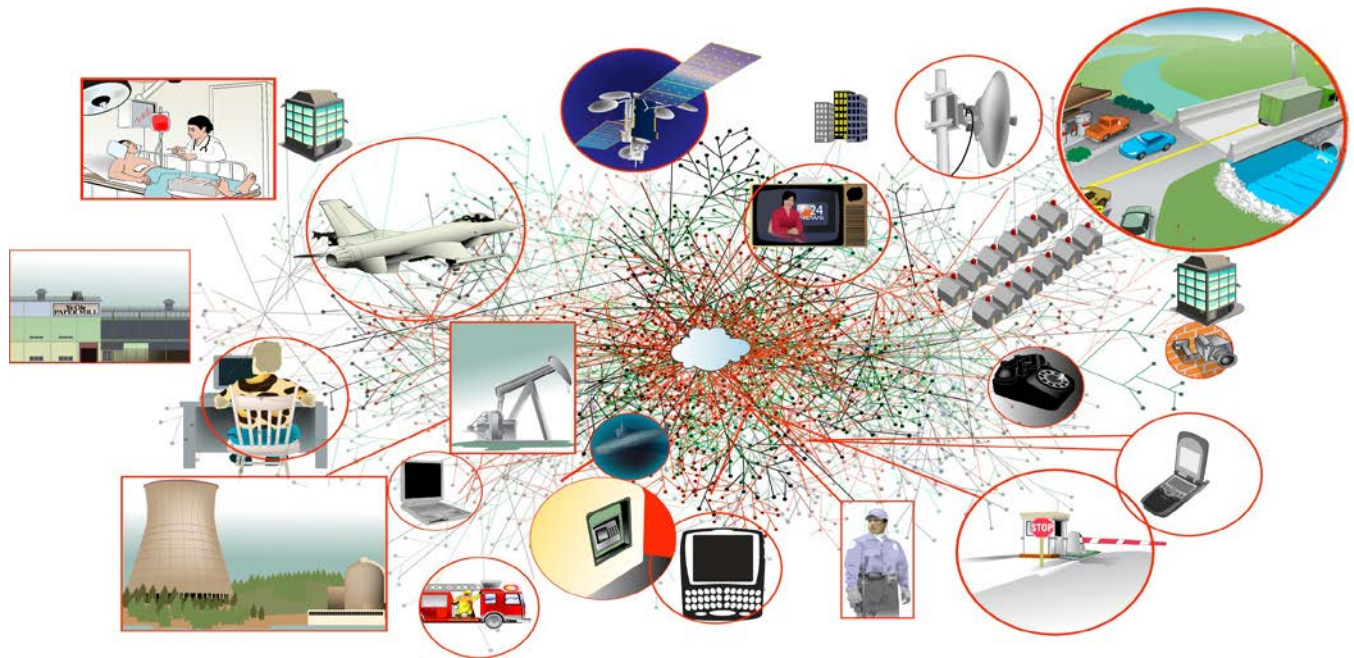
## Output of Section VI

	Output	Guidance
✓	Updated program processes	<ul style="list-style-type: none"> <li>• Detected, analyzed, and reported EDM trends, issues, and risks</li> <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>• Stakeholder engagement, input, and support garnered via their participation in the external dependencies review and update process</li> <li>• Approved changes</li> </ul>
✓	Updated risk documentation, tracking, and action plans	<ul style="list-style-type: none"> <li>• Updated objectives, strategies, and plan</li> <li>• Updated accountabilities and job descriptions as appropriate</li> <li>• A database, spreadsheet, or list showing the current documentation update status</li> <li>• Updated tracking database</li> <li>• Updated EDM risk action plans for all affected areas, showing tasks and timelines in support of the EDM program objectives</li> </ul>

## VI. Conclusion

Growing organizational interdependencies and the expanded use of outsourcing have increased the urgency of EDM and its improvement. Managing new, more complex threats is a key challenge made difficult when the potential for disruptions extends to a web of external suppliers. For those in regulated industries such as energy, finance, and health care, new regulatory guidance and oversight are driving actions and investments that are difficult to prioritize. This guide was developed to help organizations of all types, in any industry, and of all sizes manage those challenges by providing a comprehensive, step-by-step, risk-based approach to addressing EDM.

This guide focuses on the relationships with service suppliers with whom the organization may have established carefully negotiated, contracted relationships (e.g., raw materials, technology, and maintenance). It also focuses on relationships over which the organization has very limited control (e.g., utilities, government agencies, emergency responders).



*Figure 8: External Dependencies and Interdependencies Originate from Many Sources and Suppliers*

Relationship management is a key component of dependency management. This guide advocates an approach that addresses the entire end-to-end supplier lifecycle and stresses communication and collaboration throughout. Lastly, this guide emphasizes a risk-based approach to prioritizing and structuring dependency management. This provides the basis for determining requirements for each supplier, as well as how much rigor and oversight to place on it. By utilizing relationships, lifecycle, and requirements-based prioritization

concepts in conjunction with a process improvement approach, organizations can mature their EDM activities to meet the challenges of today's increasingly dependent relationships.

The methodology of this guide emphasizes the following:

- Manage relationships across the entire supplier lifecycle, from early dialogue, to performance monitoring, to termination or transition.
- Take a risk-based approach to prioritizing effort and resources.
- Engage and communicate closely with internal and external stakeholders.
- Establish resilience requirements and expectations with suppliers early to help ensure efficient and effective dependency risk management.
- Communicate and collaborate to achieve process effectiveness and to gain shared trust.
- Build on existing practices and processes; leverage and improve organizational practices and process.
- Scope across the entire organization to ensure that all areas that manage relationships are engaged and familiar with EDM plans and strategy.

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

- NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Management Systems*  
[http://csrc.nist.gov/publications/drafts/800-161/sp800\\_161\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf)
- ISO/IEC 27036:2013+ — *IT Security — Security techniques — Information security for supplier relationships*
- NISTIR 7622, *Notional Supply Chain Risk Management Practices*  
<http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf>
- *CMMI for Acquisition*, Version 1.3  
<http://www.sei.cmu.edu/reports/10tr032.pdf>
- *The CERT Resilience Management Model (CERT-RMM)* [Caralli 2010]. This 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 <http://www.us-cert.gov/ccubedvp/self-service-crr>.

## Appendix A. Example External Dependencies Management Policy Template

**[Organization Name]**

### **POLICY [XX-X]: External Dependencies Management**

External dependencies management is the ongoing process of managing external entity relationships and risks and facilitating the effective use of external suppliers to support *[Organization Name]* in achieving its mission. This policy lays the framework for a formal external dependencies risk management program by establishing responsibility for the management of external entity relationships and risks. The external dependencies management responsibilities include the identification, analysis, oversight and monitoring of external dependencies risks as well as the management of the external relationships that are essential to successful, predictable, and consistent delivery of services.

#### **POLICY STATEMENT:**

All employees, contractors, and business partners will take all appropriate actions to manage external dependencies risks and relationships with external entities in a manner that promotes *[Organization Name]*'s risk management, business, and mission objectives.

#### **OBJECTIVE:**

The objective of this policy is to ensure that *[Organization Name]*'s relationships with external entities are managed in a manner that meets its business and risk management goals.

#### **SCOPE:**

This policy applies to all individuals and functions internally or externally that 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 external dependencies risk policies, standards, and guidelines
- be familiar with and support external dependencies risk objectives
- report any actual or suspected risks associated with external dependencies and/or external relationships
- take all appropriate actions to support the confidentiality, availability, and integrity of the information, technology, facility, and people assets of the organization that may be impacted by external entities

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

Executive and senior management shall

- support the development and maintenance of the external dependencies risk management plan
- implement the external dependencies risk management plan
- provide support for adequately resourcing the external dependencies risk management plan
- ensure all employees, contractors, and business partners understand their external dependencies risk management responsibilities
- take all appropriate actions to ensure relationships with external entities are effectively managed to limit the risks of external dependencies on *[Organization Name]*

#### **Document History**

Version	Release Date	Comments

## Appendix B. External Dependencies Management Resources

### Relationship and Cyber Information Resources

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

US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS. US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans.

*US-CERT:* <http://www.us-cert.gov/>

*National Cyber Alert System:* <http://www.us-cert.gov/ncas>

#### Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

ICS-CERT provides a control system security focus in collaboration with US-CERT. ICS-CERT serves as a key component of the Strategy for Securing Control Systems, which outlines a long-term, common vision where effective risk management of control systems security can be realized through successful coordination efforts.

*ICS-CERT:* [http://www.us-cert.gov/control\\_systems/ics-cert/](http://www.us-cert.gov/control_systems/ics-cert/)

*SCADA and Control Systems Procurement Language Project*, September 2009, U.S. Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT: [https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement\\_Language\\_Rev4\\_100809.pdf](https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf)

*CSSP Training:* [http://ics-cert.us-cert.gov/sites/default/files/DHS\\_CyberSecurity\\_CSSP-Traning-v12.pdf](http://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_CSSP-Traning-v12.pdf)

*Cyber Security Evaluation Tool (CSET):* <http://ics-cert.us-cert.gov/Assessments>

#### National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC is a 24x7 center responsible for the production of a common operating picture for cybersecurity and communications across federal, state, and local government; intelligence; law enforcement communities; and the private sector.

*NCCIC:* <http://www.dhs.gov/about-national-cybersecurity-communications-integration-center>

#### Daily Open Source Infrastructure Report

Each business day, the DHS collects a summary of open-source published information concerning significant critical infrastructure issues.

*Daily Open Source Infrastructure Report:* <http://www.dhs.gov/dhs-daily-open-source-infrastructure-report>

#### Homeland Security Information Network (HSIN)

HSIN is a national secure and trusted web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private-sector, and international partners engaged in the homeland security mission.

*HSIN:* <http://www.dhs.gov/homeland-security-information-network>



## **Multi-State Information Sharing and Analysis Center**

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments.

*MS-ISAC:* <http://msisac.cisecurity.org/resources/videos/free-training.cfm>

## **United State Secret Service (USSS) Electronic Crimes Task Force (ECTF)**

Partnership of not only federal, state, and local law enforcement, but also prosecutors, private industry, and academia. Its common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures.

*USSS ECTF:* <http://www.secretservice.gov/ectf.shtml>

## **Federal Bureau of Investigation (FBI) InfraGard**

InfraGard, a partnership between the FBI and the private sector, is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members.

*InfraGard:* <https://www.infragard.org/>

## **Internet Crime Complaint Center (IC3)**

The IC3 is a partnership between the [FBI](#) and the [National White Collar Crime Center](#) (NW3C). The IC3 provides a central point for internet crime victims to report to and alert an appropriate agency online at [www.ic3.gov](http://www.ic3.gov). The IC3 collects, reviews, and refers internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts and identify current crime trends across the internet.

*IC3:* <http://www.ic3.gov/default.aspx>

## **iGuardian**

The iGuardian portal, currently in its pilot stage, is available to 58,000 companies that make up the FBI's InfraGard network. If the pilot succeeds, the FBI plans to open it up to more organizations, probably at first in critical infrastructure sectors. Participating companies can submit a form online in the instance of a cybersecurity breach to their networks. The National Cyber Investigative Joint Taskforce (NCI-JTF) handles the information provided by these companies.

*iGuardian:* <http://www.fbi.gov/news/podcasts/thisweek/iguardian.mp3/view>

*NCI-JTF:* <http://www.fbi.gov/about-us/investigate/cyber/ncijtf>

## **Other Resources**

### **DHS**

*National Strategy for Global Supply Chain Security:*  
<http://www.dhs.gov/national-strategy-global-supply-chain-security>

*Office of Cybersecurity and Communications:*

<http://www.dhs.gov/office-cybersecurity-and-communications>

*Critical Infrastructure Cyber Community C<sup>3</sup> Voluntary Program:*

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

*Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach:*

<http://www.dhs.gov/publication/executing-critical-infrastructure-risk-management-approach>

*Office of Cyber & Infrastructure Analysis:*

<http://www.dhs.gov/office-cyber-infrastructure-analysis>

### **Federal Emergency Management Agency (FEMA)**

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

### **Federal Financial Institutions Examination Council (FFIEC)**

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

*Supervision of Technology Service Providers:*

[http://ithandbook.ffiec.gov/ITBooklets/FFIEC\\_ITBooklet\\_SupervisionofTechnologyServiceProviders\(TSP\).pdf](http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_SupervisionofTechnologyServiceProviders(TSP).pdf)

### **Federal Reserve Board Guidance on Managing Outsourcing Risk**

<http://www.federalreserve.gov/bankinfo/reg/srletters/sr1319a1.pdf>

### **Gartner (requires subscription)**

*Operational Risk Blog:*

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

### **Forrester**

*Risk management articles, tools, and templates (some require a fee):*

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

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

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

*ISO/IEC 27036:2013+ — IT Security — Security techniques — Information security for supplier relationships (parts 1, 2 & 3 published, remainder in draft*

<http://www.iso27001security.com/html/27036.html>

*ISO 28000 series of standards on supply chain security management system*

<http://www.iso.org/iso/home/search.htm?qt=28000&sort=rel&type=simple&published=on>

*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) 5, AP008 – Manage Relationships*

<http://www.isaca.org/COBIT/Pages/default.aspx>



**Information Technology Infrastructure Library (ITIL) 2011, Service Strategy, Supplier Design**  
<http://www.itil-officialsite.com/>

**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 800-161, *Supply Chain Risk Management Practices for Federal Information Management Systems*  
[http://csrc.nist.gov/publications/drafts/800-161/sp800\\_161\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf)

NISTIR 7622, *Notional Supply Chain Risk Management Practices*  
<http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf>

NIST Special Publication 800-30, *Guide for Conducting Risk Assessments for Federal Information Systems and Organizations*  
[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 800-39, *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>

**NERC/FERC**  
<http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

**Software Engineering Institute, CERT Division**  
<http://www.cert.org>

*CERT Resilience Management Model*  
<http://www.cert.org/resilience/rmm.html>

*CMMI for Acquisition, Version 1.3*  
<http://www.sei.cmu.edu/reports/10tr032.pdf>

**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 C. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Table 2 cross-references CRR External Dependencies 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 2: Cross-Reference of CRR Goals/Practice and NIST CSF Category/Subcategory Against the External Dependencies Management Resource Guide*

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	External Dependencies Management Resource Guide Reference
<b>Goal 1: External dependencies are identified and prioritized to ensure sustained operation of high-value services.</b>		—
1. Are dependencies on external relationships that are critical to the service identified? [EXD:SG1.SP1]	<b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established.	Section IV, Step 2
2. Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1]	<b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established.	Section IV, Step 6
3. Are external dependencies prioritized? [EXD:SG1.SP2]	<b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established.	Section IV, Step 2
<b>Goal 2: Risks due to external dependencies are identified and managed.</b>		—
1. Are risks due to external dependencies identified and managed? [EXD:SG2.SP1]	<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated. <b>ID.RA-5:</b> Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	Section III, Step 3
<b>Goal 3: Relationships with external entities formally established and maintained.</b>		—
1. Have resilience requirements of the critical service been established that apply specifically to each external dependency? [EXD:SG3.SP2]	<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated. <b>ID.BE-5:</b> Resilience requirements to support delivery of critical services are established.	Section IV, Step 3
2. Are these requirements reviewed and updated? [EXD:SG3.SP2]	<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated. <b>ID.BE-5:</b> Resilience requirements to support delivery of critical services are established.	Section IV, Step 3
3. Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3]	<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated. <b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established. <b>ID.BE-5:</b> Resilience requirements to support delivery of critical services are established.	Section IV, Step 3
4. Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4]	<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated. <b>ID.BE-5:</b> Resilience requirements to support delivery of critical services are established.	Section IV, Step 4

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	External Dependencies Management Resource Guide Reference
	<b>PR.AT-3:</b> Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities.	
<b>Goal 4: Performance of external entities is managed.</b>		—
1. Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1]	<b>DE.CM-6:</b> External service provider activity is monitored to detect potential cybersecurity events. <b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated.	Section IV, Step 5
2. Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1]	<b>ID.AM-6:</b> Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. <b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated.	Section IV, Step 4
3. Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2]	<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated.	Section IV, Step 5
4. Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]	<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated.	Section IV, Step 5
<b>Goal 5: Dependencies on public services and infrastructure service providers are identified.</b>		
1. Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified? [EC:SG4.SP3]	<b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established.	Section IV, Step 2
2. Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4]	<b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established.	Section IV, Step 2

## 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. 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>.
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. “EXD:SG2 Manage Risks Due to External Dependencies,” pg. 350. *CERT-RMM* [Caralli 2010].
7. “External Dependencies Management (EXD),” *CERT-RMM* [Caralli 2010].
8. “External Dependencies Management (EXD),” pg. 341. *CERT-RMM* [Caralli 2010].