Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

External Dependencies Management (EXD)

Richard A. Caralli
Julia H. Allen
David W. White
Lisa R. Young
Nader Mehravari
Pamela D. Curtis

February 2016

CERT Program

http://www.cert.org/resilience/

Carnegie Mellon

This material is based upon work funded and supported by various entities 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.

DM-0003234

EXTERNAL DEPENDENCIES MANAGEMENT

Operations

Purpose

The purpose of External Dependencies Management is to establish and manage an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities.

Introductory Notes

Outsourcing services, development, production, and even asset management have become normal and routine operational elements for many organizations because they often provide the ability to engage specialist skills and equipment at a cost savings over internal equivalents. Increasingly, organizations are also exposing technology systems, information, and other high-value assets to customers to enable the seamless and efficient flow of business processes. The External Dependencies Management process area addresses the identification of risks associated with the actions of external entities, the formalization of the relationship with such entities, and the ongoing management of those dependencies and relationships, all in a manner to ensure that appropriate resilience measures are in place to protect and sustain the organization's services and assets that are dependent upon such actions and entities.

For the purpose of this process area, the term *organization* is used to refer to the entity—the enterprise or a part of the enterprise such as an organizational unit or department—that is using the process area. An external dependency exists when an entity that is external to the organization has access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization. Such entities may be contractors or customers, but they may also be other units or groups within the enterprise. In this process area, all such entities are referred to as "external entities."

The success of the organization in accomplishing its overall mission depends on its ability to sustain mission assurance of services in a consistent and efficient manner. Some services are fully executed inside of organizational boundaries, giving the organization more direct control over mission assurance. However, in many cases, the organization does not control all of the activities in a service that contribute to meeting the service mission; instead, these activities may be performed by external entities.

Dependence on external entities may increase risk levels for organizations in managing the end-to-end resilience of their services. When the execution of a service extends outside of the organization's direct control, there is less ability to directly affect or predict mission assurance, in part because mission assurance is dependent on the resilience of the external entity. From an asset perspective—people, information, technology, and facilities—this can be problematic. In its role in support of a service, an external entity may

- use its own assets—If the external entity fails to protect and sustain these assets, the service and its outcome may be compromised.

- access the assets of the organization (which likely includes the ability to control or modify those assets)—The external entity's actions could affect the resilience of the assets and thereby compromise the service.
- possess and use the assets of the organization (which includes the responsibility for custodial care of those assets)—If the external entity fails to meet the resilience requirements of the assets (as specified by the organization), there is a potential impact on the service mission.
- develop, deliver, commission, or install a new or revised asset for the organization
- provide supporting services that aid in protecting and sustaining an organization's asset

Consider also that an external entity may not have a direct role in executing a specific service. In a support role (for example, storing information in an off-site storage facility), an external entity may also fail to adequately protect and sustain the asset such that it will not be available for use in a service when needed.

Regardless of the degree of external dependence, the organization retains responsibility for service mission assurance. The organization is responsible for setting the resilience requirements for services and related assets, communicating them to and requiring them of external entities, and monitoring to ensure external entities are meeting them. The evaluation and selection of external entities based on their abilities to sustain resilience are important first steps in ensuring service resilience.

External dependencies also arise when the organization outsources asset design or development activities—including facility development or software or system development. *(Refer to the Resilient Technical Solutions Engineering process area for more information about developing systems and software in a manner that supports the organization's resilience requirements.)* Additional external dependencies arise when the organization is reliant on services that are part of the environment in which it operates, such as energy, telecommunications, and emergency response providers. All such external dependencies can significantly affect an organization's ability to achieve its service missions.

The External Dependencies Management process area comprises four goals: to identify and prioritize external dependencies, to manage risks associated with external dependencies, to formalize binding relationships with external entities, and to monitor and manage external entity performance against all contractual specifications, including those for operational resilience.

Related Process Areas

The establishment and management of resilience requirements for the organization's assets, including those provided or controlled by external entities, are performed in the Resilience Requirements Development and the Resilience Requirements Management process areas.

The risk management cycle for external dependencies is addressed in the Risk Management process area.

The development, validation, testing, and improvement of plans to sustain service continuity for both the organization and external entities are addressed in the Service Continuity process area.

The availability of people to support the continued operation of services, including both employees of the organization and people provided by external entities, is addressed in the People Management process area.

Controls to manage the performance of people in support of the resilient operation of services, including both employees of the organization and people provided by external entities, are addressed in the Human Resource Management process area.

The identification, definition, management, and control of the organization's assets, including those provided or controlled by external entities, are addressed in the Asset Definition and Management process area.

The resilience of technology assets, including those in the control of the organization and those developed, provided, managed, or controlled by external entities, is addressed in the Technology Management process area.

The resilience of information assets, including those in the control of the organization and those provided, controlled, or accessed by external entities, is addressed in the Knowledge and Information Management process area.

The resilience of facility assets and control of the physical environment, including facilities in the full control of the organization and those provided or managed by external entities, are addressed in the Environmental Control process area.

The development of software and system assets that meet the organization's resilience requirements is addressed in the Resilient Technical Solution Engineering process area.

Summary of Specific Goals and Practices

Goals	Practices
EXD:SG1 Identify and Prioritize External Dependencies	EXD:SG1.SP1 Identify External Dependencies
	EXD:SG1.SP2 Prioritize External Dependencies
EXD:SG2 Manage Risks Due to External Dependencies	EXD:SG2.SP1 Identify and Assess Risks Due to External Dependencies
	EXD:SG2.SP2 Mitigate Risks Due to External Dependencies
EXD:SG3 Establish Formal Relationships	EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies
	EXD:SG3.SP2 Establish Resilience Specifications for External Dependencies
	EXD:SG3.SP3 Evaluate and Select External Entities
	EXD:SG3.SP4 Formalize Relationships
EXD:SG4 Manage External Entity Performance	EXD:SG4.SP1 Monitor External Entity Performance
	EXD:SG4.SP2 Correct External Entity Performance

Specific Practices by Goal

EXD:SG1 Identify and Prioritize External Dependencies

External dependencies are identified and prioritized to ensure the resilience of the high-value services that they support.

In this goal, the organization identifies, characterizes, and prioritizes its external dependencies. The prioritization of external dependencies establishes one or more subsets on which the organization must focus its operational resilience activities due to

the external dependencies' importance to the sustained operation of high-value services.

Prioritization of external dependencies is a risk management activity. The organization establishes the dependencies that are of most value to the services they support and that require controls to protect and sustain them. Failure to prioritize external dependencies may lead to inadequate operational resilience of high-value services and assets and excessive levels of operational resilience for services and assets that are not high-value.

EXD:SG1.SP1 Identify External Dependencies

A list of external dependencies is established and maintained.

Organizations have many types of external dependencies. Any asset or service that is subject to the actions of an external entity is the source of an external dependency. It is important for the organization to identify and characterize all such external dependencies so that they can be understood, formalized, monitored, and managed as part of the organization's comprehensive risk management process.

The most common type of external dependency occurs when the organization outsources certain activities of a service (or the entire service) to an external entity. Another example would be outsourcing the development of a technology asset, such as a software application, or an information asset, such as a custom database.

A less common type of external dependency occurs when the organization provides its customers with access to or use of high-value organizational assets. This is becoming more and more common in certain types of enterprises, particularly in cases where technology interfaces are provided to key customers for the seamless integration of services between the two organizations. (For example, the organization may process certain transactions on behalf of the customer through a tightly coupled technological interface that provides the customer with access to certain organizational assets.)

The organization may use any number of techniques to establish a catalog or detailed list of external dependencies. The organization's list of services should be examined to discover services that may be subject to external dependencies, in whole or in part. The organization's inventory of assets should also be examined to discover assets that are in the control of external entities or are in other ways subject to external dependencies. The organization may find value and efficiency in establishing close service links or overlap to facilitate information sharing between the external dependencies list, the services listing, and the asset inventory. *(Services are addressed in the Enterprise Focus process area; assets are addressed in the Asset Definition and Management process area.)*

The organization's customer database and supplier database may also be valuable sources of insight when establishing the catalog of external dependencies. The organization's set of current supplier and vendor

contracts and related service level agreements (SLAs) are additional sources.

The purpose of the catalog of external dependencies is to support the identification and prioritization of external dependencies and the management of risks associated with selected dependencies.

The organization's external dependencies will change over time as a result of changes to relationships with essential suppliers and customers, changes in services, the life cycle of assets, and many other reasons. Once the list of external dependencies is established, it is important that it be maintained. A process for updating the list on a regular basis should be established.

Typical work products

1. List of external dependencies and entities
2. Documented process for updating the list of external dependencies and entities

Subpractices

1. Establish a process for creating and maintaining the list of external dependencies and entities.
2. Establish a set of information that is collected and stored to define each external dependency and the responsible external entity.

   The data that is collected, stored, and routinely updated as part of defining an external dependency and its corresponding external entity is used to help prioritize the external dependency and identify risks associated with the external dependency. The data fields should therefore be set in consideration of the criteria, thresholds, and process for prioritizing external dependencies *(see EXD:SG1.SP2)* and in consideration of the risk identification process for external dependencies *(see EXD:SG2.SP1)*.

   These are examples of information to collect, store, and update to define an external dependency:

   - a description of the external dependency, including
     - the organizational services that rely on the external dependency
     - the organizational assets that rely on the external dependency
     - the criticality and priority of the external dependency based on its importance to high-value services and assets
   - the organizational owner of the external dependency
   - the name of the external entity that is responsible for the external dependency
   - key points of contact at the external entity
   - the organizational owner of the external entity relationship (i.e., the department and/or person in the organization who is responsible for the relationship with the external entity)
   - compliance and other obligations that apply to the external dependency, the external entity, or the relationship with the external entity

These are examples of information to collect, store, and update to define an external entity responsible for an external dependency:

- the name of the external entity
- the names of the external dependencies for which the external entity is responsible
- the products, services, assets, or other inputs (external dependencies) that may be supplied by the external entity, which may include
  - general support services, such as producing the organization's payroll or staffing customer call centers
  - services that directly affect resilience processes such as security operations or IT service delivery and operations management
  - resilience-specific services such as backup and recovery of data, provision of backup facilities for operations and processing, and provision of support technology
  - environmental services such as power, telecommunications, fire and police support, emergency medical services, and emergency management services
  - technology and information assets, such as application software and databases
- key points of contact at the external entity
- the organizational owner of the external entity relationship (i.e., the department and/or person in the organization who is responsible for the relationship with the external entity)
- the external entity's legal entity type (corporation, government entity, etc.)
- the nature of the relationship with the external entity (customer, supplier, public service, or other)
- type, status, and duration of contracts or other agreements in place with the external entity
- the monetary value or other parameter used to describe the value of the relationship with the external entity
- the organizational assets that are owned, developed, controlled, used, operated, or otherwise influenced by the external entity
- the financial status of the external entity
- the status of any pending disputes or litigation with the external entity

3. Review the organization's asset inventory to ensure that any external entities that possess, develop, control, operate, or otherwise influence high-value assets are identified as external dependencies.
4. Review the organization's list of services to identify services that are subject to external dependencies; add any such dependencies to the list of external dependencies.
5. Review supplier and customer databases to identify additional external dependencies.
6. Review current contracts and SLAs to identify additional external dependencies.
7. Update the external dependency list on a regular basis.

   The frequency and timing of such updates should be adjusted as a function of the organization's risk tolerance to the external dependencies. It may be prudent to update

different external dependencies at different frequencies based on the risks and characterization details of external dependencies and the relevant external entities. It may be appropriate to increase the update frequency during times of increased risk to the organization or when an external entity is undergoing change or is at risk. Contract award, renewal, or termination should trigger appropriate updates to the external dependency list, as should changes in points of contact or other material changes in the relationship.

Understanding the risks identified in EXD:SG2.SP1 may assist in setting and revising the update frequency.

EXD:SG1.SP2 Prioritize External Dependencies

External dependencies are prioritized relative to their importance in supporting the delivery of high-value services.

The prioritization of external dependencies must be performed to ensure that the organization properly directs its operational resilience resources to the external dependencies that most directly impact and contribute to services that support the organization's mission. These external dependencies require the organization's direct attention because their disruption has the potential to cause the most significant organizational consequences.

External dependency prioritization is performed relative to services—that is, external dependencies associated with high-value services are those that must be given the highest priority for operational resilience activities.

However, the organization can use other criteria to establish high-priority external dependencies, such as

- actions of the external entity in the support, maintenance, or custodial care of high-value organizational assets
- the extent to which the organization would rely on the actions of the external entity during off-normal operations, crises, or other times of operational stress
- actions of the external entity in supporting the organization's resilience process
- an external dependency resulting from external entity access to highly sensitive or classified information or to the organization's trade secrets or proprietary information such as intellectual property *(Categorization of information assets is addressed in KIM:SG1.SP2, and intellectual property management is addressed in KIM:SG4.SP2.)*
- external dependencies that are of high value to more than one service
- actions of the external entity in developing, providing, or commissioning new assets for the organization
- the organization's tolerance for "pain"—the degree to which it can suffer degraded performance of the external dependency and continue to meet its mission

Several tiers or classes of prioritization may be appropriate depending on the complexity of the organization's operations and variations in the nature

of the external dependencies. It is important that consistent and meaningful criteria be developed for prioritizing the external dependencies and that the criteria be uniformly applied to the full set of external dependencies. The prioritization and criteria should be reviewed and updated on a regular basis to ensure that the prioritization scheme and the list of prioritized external dependencies are appropriate for the organization's risk environment and tolerance.

Typical work products

1. Criteria for prioritizing external dependencies
2. Prioritized list of external dependencies
3. Results of external dependency affinity analyses

Subpractices

1. Establish prioritization criteria and scheme for external dependencies.

   Prioritization criteria should express and distinguish the importance of external dependencies in the continued operation of the organization. The prioritization scheme should be developed in consideration of the various types of external dependencies and external entities on which the organization relies. Thresholds should be considered to distinguish one or more tiers of external dependencies so that appropriate controls can be applied to the various sets of external dependencies to protect and sustain the organization's operations.

2. Apply the prioritization criteria to the list of external dependencies to produce a prioritized list.

   Depending on the prioritization scheme developed by the organization, the result might be several lists, tiers, or sets of external dependencies.

   Be sure that external dependencies that are required for the successful execution of security activities and service continuity plans are prioritized appropriately.

3. Periodically validate and update the prioritization criteria and scheme based on changes to the operational environment.
4. Periodically update the prioritized list of external dependencies based on changes in the prioritization criteria and scheme, the operating environment, or the list of external dependencies.
5. Perform affinity analyses to inform dependency prioritization and risk identification.

   Affinity analyses should be performed to identify situations such as

   - the reliance of more than one high-value asset or service on a single external dependency or entity
   - external entities that are dependent on others to meet their agreements with the organization and thus may create chains of external dependencies that are very difficult to manage or control

EXD:SG2 Manage Risks Due to External Dependencies

Risks due to external dependencies are identified and managed.

The management of risk due to external dependencies is the specific application of risk management tools, techniques, and methods to these high-value relationships of the organization. Most organizations have many external dependencies, all of which can be the source of additional risks. Risks from external dependencies can result in consequences due to the impact on assets or services that may be in the control of, supplied by, operated by, or otherwise affected by external entities.

Managing risks due to external dependencies involves understanding the nature of each essential external dependency and the specifics of how the organization may be affected by the realization of such risks.

EXD:SG2.SP1 Identify and Assess Risks Due to External Dependencies

Risks associated with external dependencies are periodically identified and assessed.

Risks due to external dependencies must be identified and assessed so that they can be effectively managed to maintain the resilience of the organization's high-value services.

The identification of risks due to external dependencies forms a baseline from which a continuous risk management process can be established and managed.

The subpractices included in this practice are generically addressed in RISK:SG3 and RISK:SG4 in the Risk Management process area.

Typical work products

1. External dependency risk statements, with impact valuation
2. List of external dependency risks, with categorization and prioritization

Subpractices

1. Determine the scope of risk assessment for external dependencies.

   Determining which external dependencies to include in regular risk assessment activities depends on many factors, including the impact on the organization of any disruption in a high-value service that could result due to the realization of such risks.

2. Identify risks due to external dependencies.

   Identification of risks due to external dependencies requires an understanding of the actions of the associated external entity in the operation, support, or resilience of the organization's services. External entities will be responsible for varying dependencies in the support of the organization's operations. The information gathered in the identification and characterization of the external dependencies in support of EXD:SG1.SP1 may be useful in identifying such risks.

   Issues to consider when identifying risks associated with a specific external dependency that relies on a specific external entity include

   - the financial condition of the external entity
   - risks to the availability of the external entity's vital staff

- reliance by the external entity on subcontractors
- risks to assets owned, developed, and operated by the external entity that are used in providing the necessary service to the organization
- scalability of the external entity to meet demand surges or growth in operations as may be required
- the ability of the external entity to protect and sustain its operations, particularly in times of disruption and stress, including service continuity plans, protective and detective controls, and other key risk management elements
- level of resilience experience or maturity of the external entity, including demonstrated strengths or weaknesses
- risks due to the location of the external entity, which may include specific environmental risks due to geography or operating risks associated with local public services
- unique regulatory and compliance risks associated with the external dependency or the external entity, especially as may be compounded by differing local laws (This may be particularly relevant if the external entity is based in another country.)
- reliance on communications infrastructure or other high-value technology assets that enable smooth conduct of operations between the organization and the external entity

Risk statements should be developed for each identified risk. *(RISK:SG3.SP1 and RISK:SG3.SP2 provide additional information about identifying risks and developing risk statements.)*

3. Analyze risks due to external dependencies.

   The analysis of risks should include an evaluation of the potential impact of the risk on the organization.

   Topics to consider when analyzing risks associated with a dependency on a specific external entity include

   - the value of assets or services that are accessed, modified, provided, developed, or controlled by the external entity
   - operational throughput that relies on the performance of the external entity (for example, the number of customers or the transaction volume that would be impacted by the realization of the risk)
   - legal liabilities that might accrue to the organization as a result of the risk
   - risks that could arise if the organization has not developed contingency plans or service continuity plans to minimize the impact of any disruptions to the external entity's operations on which the organization relies
   - alternative sources for whatever assets or services the external entity provides that could be or already are established
   - historical key performance measures of the external entity

4. Categorize and prioritize risks due to external dependencies.

   RISK:SG4.SP2 provides additional information about risk categorization and prioritization.

5. Develop a risk disposition strategy for each identified risk.

   RISK:SG4.SP3 provides additional information about risk disposition.

6. Monitor risk status on a regular basis to ensure that the risk, its mitigation strategy, and its risk mitigation plan do not pose additional threat to the organization.

EXD:SG2.SP2 Mitigate Risks Due to External Dependencies

Risk mitigation plans for risks to due external dependencies are developed and implemented.

The mitigation of risks due to external dependencies involves the development of strategies that seek to minimize the risks to acceptable levels. This includes reducing the likelihood of risks, minimizing exposure to them, developing service continuity plans, and developing recovery and restoration plans to address the consequences of realized risk.

Risk mitigation for external dependencies requires the development of risk mitigation plans (which may include the development of new controls or the revision of existing controls that apply to external dependencies and external entities) and the implementation and monitoring of these plans for effectiveness.

The subpractices included in this practice are generically addressed in RISK:SG5 in the Risk Management process area.

Typical work products

1. External dependency risk mitigation plans
2. List of those responsible for addressing and tracking risks
3. Status reports on external dependency risk mitigation plans

Subpractices

1. Develop risk mitigation plans for all risks due to external dependencies that have a “mitigate” or “control” disposition.
2. Validate the risk mitigation plans by comparing them to existing strategies for protecting and sustaining external dependencies.
3. Identify the person or group responsible for each risk mitigation plan and ensure that the person or group has the authority to act and the proper level of skills and training to implement and monitor the plan.
4. Address residual risk.
5. Implement the risk mitigation plans and provide a method for monitoring their effectiveness.
6. Collect performance measures on the risk management process.

EXD:SG3 Establish Formal Relationships

Relationships with external entities are formally established and maintained.

Requirements in the form of contractual specifications provide the basis for formal agreements that are established to define and govern the relationships between the organization and the actions of external entities. Enterprise-level requirements are established and included in any such agreement with an external entity. Specifications

(including those for satisfying resilience requirements) are established that are unique to a particular external dependency. Ideally, external entities are selected from a qualified set of candidates based on their demonstrable ability to achieve the specifications established by the organization; any specifications that cannot be met are identified and managed as risks by the organization. The entire relationship between the organization and the external entity is established, defined, and bound by a formal agreement that includes all contractual specifications. The agreement is updated throughout the life cycle of the relationship with the external entity as needed.

EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies

Enterprise specifications that apply in general to external entities are established and maintained.

The organization has a set of values and behaviors that it follows when carrying out its operations. These values and behaviors may be derived to support the organization's strategy or designed to create or reinforce the organization's public image. They may also be a reflection of the organization's market sector or the function of regulations or other constraints with which the organization must comply. Regardless of the source, the organization's values and behaviors should be reflected in high-level organizational policies that govern the behavior of staff and external entities whenever they are representing or performing services for the organization.

From a resilience perspective, such policies, standards, and guidelines are essential controls that aid in protecting and sustaining the organization's operation. For example, the organization may have a policy that requires certain minimum due diligence prior to allowing staff members to access certain information assets.

When external entities support the execution of the organization's services, they become an extension of the organization and should be subject to the same or similar policies, standards, and guidelines as the organization's staff. These enterprise-level policies, standards, and guidelines must be translated to a set of enterprise-level specifications and reflected in agreements with each external entity to ensure a seamless implementation of the organization's resilience strategy.

The enterprise specifications for external dependencies should consider the prioritization criteria and scheme for external dependencies *(see EXD:SG1.SP2)*. It may be appropriate for certain or all enterprise specifications to apply to all external entities. Alternatively, it may be appropriate for different sets of enterprise specifications to apply to different tiers or sets of prioritized external dependencies and the relevant external entities.

The organization's enterprise resilience requirements should be reflected in the enterprise specifications for external dependencies. *(Enterprise resilience requirements are addressed in the Resilience Requirements Development process area.)*

These are examples of enterprise specifications for external entities:

- compliance with regulations or legal statutes that affect the organization
- agreement related to the treatment of the organization's intellectual property
- adherence to certain staff and human resources policies
- policies regarding the security of certain information or technology assets, including the use of resilience guidelines in the development of software and system assets *(Refer to the Resilient Technical Solution Engineering process area.)*
- physical access policies for organization-owned or -managed facilities
- adherence to special agreement provisions such as non-disclosure statements
- requirements for contract flow-down provisions or pre-approval of subcontractors
- insurance and indemnification requirements related to the handling of certain assets
- indemnification and defense requirements associated with legal or contract violations
- security clearance requirements for facilities or staff
- policies on ethics, behavior, non-discrimination, and harassment
- procedural requirements related to staff turnover
- policies on performance monitoring and reporting
- minimum requirements for financial attributes of the organization and related reporting

Typical work products

1. List of enterprise specifications that apply to external dependencies and entities
2. Agreement templates that reflect enterprise specifications

Subpractices

1. Establish a list of enterprise-level specifications that apply to external dependencies and entities.
2. Include specifications to adhere to relevant policies, standards, and guidelines (particularly those that support or affect the resilience of the organization or its operations) in the list of enterprise specifications for external dependencies and entities.
3. Include relevant compliance and regulatory requirements in the list of enterprise specifications for external dependencies and entities.
4. Include the enterprise specifications for external dependencies and entities in contract and agreement templates as appropriate.
5. Review and update the enterprise specifications for external dependencies and entities on a regular basis.
6. Ensure that changes are initiated to agreements with external entities when the enterprise specifications change.

EXD:SG3.SP2 Establish Resilience Specifications for External Dependencies

Resilience specifications that apply to specific external dependencies and entities are established and maintained.

External dependencies occur as a result of an external entity's access to, control of, ownership in, development of, possession of, responsibility for (including operations, maintenance, or support), or other defined obligations related to one or more high-value assets or services of the organization. The organization's high-value assets and services all have specific resilience requirements that must be established as specifications for any associated external dependency and responsible entity.

For each external dependency, the organization should establish a detailed set of specifications that the external entity must meet in order to support and extend the resilience of the organization's operations. It is important that these specifications be thorough, detailed, definitive, adequate for use as criteria when selecting external entities, suitable as language in agreements with external entities, and appropriate for use as a basis for monitoring the performance of the external entity.

The specifications for a specific external dependency and entity include, as appropriate, required characteristics of the external entity (e.g., financial condition and experience), required behaviors of the external entity (e.g., security and training practices), and performance parameters that must be exhibited by the external entity (e.g., recovery time after an incident and response time to service calls).

When developing specifications for external dependencies, the organization should

- consider the type of organizational assets or services impacted by the external dependency and their importance to the organization's mission and operations
- understand the extent to which the external entity takes custodial control of the organization's assets, and any resilience requirements of those assets that must be satisfied
- consult internal and external stakeholders responsible for the associated assets and services
- be aware of other assets or services that may rely upon the same external dependency and entity (as would be indicated by the affinity analysis in EXD:SG1.SP2)
- review the resilience requirements established in the Resilience Requirements Development process area for the assets or services in question
- review and select appropriate resilience guidelines established in the Resilient Technical Solution Engineering process area for the development of all software and system assets
- include the enterprise-level specifications (as identified in EXD:SG3.SP1)

The resilience specifications for an external dependency must clearly cover the resilience requirements of the assets or services that rely on the external entity. They should also include key features and capabilities of the external entity.

Typical work products

1. Documented resilience specifications
2. Service level agreements

Subpractices

1. For each external dependency, establish a list of resilience specifications that apply to the responsible external entity.

   The process for determining and documenting the resilience specifications that apply to an external dependency and entity will vary based on the action of the entity in relation to the organization's operations and the priority of the external dependency (as determined in EXD:SG1.SP2).

   At a minimum, the resilience specifications should include a clear and definitive statement of the external entity's services, support, products, assets, or staff on which the organization relies.

2. Include specific characteristics of the external entity that are required.

   Specifications for characteristics are often expressed as minimum acceptable characteristics.

   Required external entity characteristics might include

   - industry experience
   - management experience
   - technology and systems architecture
   - process controls
   - financial condition
   - reputation, including references
   - degree of reliance on other external entities
   - legal, regulatory, and compliance history
   - ability to meet future needs
   - CERT-RMM capability ratings

3. Include resilience requirements for assets that will be developed, provided, or maintained by external entities.
4. Include behaviors, standards of performance, and service levels that are required of the external entity.

   Specifications that describe required behaviors and performance parameters are often documented as SLAs that are included in requests for proposals (RFPs) *(see EXD:SG3.SP3)*. It is valuable to develop the SLA before entering into a relationship with an external entity so that the SLA can be used as part of the evaluation process to select an external entity. Ultimately, the SLA should be incorporated into the formal contractual agreement with an external entity *(see EXD:SG3.SP4)*.

From a resilience perspective, the SLA should include the performance specifications for security, business continuity, and IT operations that are necessary to support the resilience of the associated asset or service (the external dependency). For example, if the external entity is performing payroll operations for the organization, the SLA may require that the external entity keep all payroll data confidential and destroy the data within a specific number of days of its use. SLAs often specify deadlines or time parameters for availability, support, and/or recovery activities (such as a requirement for X% availability over a Y-month period).

Consider the following topics when establishing required behaviors and standards of performance for external dependencies and entities:

- availability, including hours of operation and minimum uptime measures
- performance, including throughput, latency, response time, and other measures of operational performance
- change management, including minimum time frames for notifications, testing requirements, and patch management procedures
- quality of service, including response time, dispute and escalation procedures, service desk support, and problem tracking
- security, including incident management procedures and performance, vulnerability and penetration management, logical and physical access controls, identity management, and security standards compliance
- business continuity, including requirements for business continuity plan development, testing protocols and frequency, recovery time in the event of an incident, and prioritization of services or assets for recovery in the event of an incident. (This may also include recovery time objectives [RTOs] and recovery point objectives [RPOs] for specific technology assets *[see TM:SG5.SP1].)*
- asset segregation and marking
- physical and/or logical separation of technology and/or information assets
- monitoring and reporting requirements, including measurements and reporting criteria, required audits, rights to audit, audit protocols, reports on external dependencies, asset status reports, and dashboards
- communications and coordination, particularly in the event of security or business continuity incidents

5. Periodically review and update resilience specifications for external dependencies and entities as conditions warrant.

EXD:SG3.SP3 Evaluate and Select External Entities

External entities are selected based on an evaluation of their ability to meet the specifications for external dependencies.

External entities should be selected according to an organized and thorough process and according to explicit specifications and selection criteria. The selection process and criteria should be designed to ensure that the selected entity can fully meet the organization's specifications as established in EXD:SG3.SP1 and EXD:SG3.SP2.

From a resilience perspective, the selection process for external entities is often an extension of or supplement to the organization's standard procurement processes. Resilience specifications may simply serve as

additional requirements for consideration and evaluation as part of the standard procurement process. In all cases, due diligence should be performed on candidate external entities to evaluate their ability to meet the resilience specifications that have been established for the actions they hope to perform for the organization.

In some cases, external entities cannot be selected from a pool of candidates; they may be inherited in the course of an acquisition or merger, or they may be the only provider of a high-value service on which the organization depends (this is often the case for public services). In cases in which external entities cannot be selected, the due diligence process for selection should still be performed to identify any specifications that are not met by the external entity. It may be appropriate to alter the specifications by changing the actions or nature of the dependence on the external entity to resolve the unmet specifications. In cases where the specifications cannot be changed, any unmet specifications should be treated as risks under EXD:SG2.

Typical work products

1. Requests for proposals or other types of external entity solicitation documents that include specifications in cases in which proposals and bids are being sought by the organization
2. External entity selection criteria
3. Evaluation of each external entity proposal against the selection criteria
4. Selection decision and supporting rationale

Subpractices

1. Establish a selection process for external entities that includes consideration of applicable specifications.
2. Establish external entity selection criteria.

   The criteria should include measures and thresholds of the candidate external entity's ability to meet the resilience specifications established in EXD:SG3.SP1 and EXD:SG3.SP2.

   These are examples of factors that should be considered for the development of criteria for external entity selection:

   - organizational mission, vision, values, goals, objectives, purpose, and critical success factors
   - the risk tolerance of both the organization and the external entity
   - the type of external entity relationship and whether the relationship supports a high-value service or is an essential part of the service
   - the nature of the service—whether the external entity will take custodial control of the organization's high-value assets or use its own in providing the service
   - the nature of the asset—the extent to which the asset (such as software or information) supports a high-value service or is an essential element of accomplishing the service
   - the ability of the external entity to participate in monitoring, testing, and verification activities

- if the external entity is likely to have multiple customers, the ability of the external entity to provide service during periods of concurrent usage

3. Include the resilience specifications for external entities in RFPs, other solicitations of interest, and other documents or processes that are designed to identify and/or qualify candidate external entities.
4. Evaluate external entities based on their abilities to meet the resilience specifications and in accordance with the established selection criteria.
5. Perform due diligence on candidate external entities.

   The due diligence process should be designed to verify that the candidate can meet the organization's specifications. If the external entity is engaged with a high-value service or asset in support of the organization's mission, it may be appropriate to test the controls that are in use by the candidate to protect and sustain its services and assets as part of the due diligence process.

   The due diligence may be performed iteratively as part of a staged procurement process with multiple down-select stages, or the due diligence may be performed completely on each qualified candidate to help understand and reveal differences among the candidates.

   The due diligence process and results should be documented. The resulting documents should be adequately protected in accordance with the organization's policies and in compliance with any non-disclosure or other agreements in place with the candidate.
6. Select external entities and document the selection and decision rationale.
7. If any resilience specifications are unmet by the selected external entity, revise the selection criteria to adjust the specifications or treat the unmet specifications as identified risks in EXD:SG2.SP1.

EXD:SG3.SP4 Formalize Relationships

Formal agreements with external entities are established and maintained.

Formal agreements should be established with external entities. The agreement content may take different forms depending on the

- type of relationship between the organization and the external entity
- type of products or services (external dependencies) being provided by the external entity (particularly if the services are for sustaining security and resilience rather than general services)
- level of integration of the external entity with the service (i.e., the extent to which the organization relies on the external entity to meet the service mission)
- degree to which the external entity takes custodial control of the organization's asset(s) in order to provide necessary products and services

Types of agreements may include contracts, memoranda of agreement, purchase orders, and licensing agreements. In some cases, agreements such as mutual-aid agreements may spell out what services a public authority provides for the organization during normal operations and during crises. In cases in which the external entity and the organization are part of the same legal entity or share a common parent legal entity, the organization or the parent entity may have special procedures for establishing and enforcing agreements. Agreements are often composed from multiple sections or multiple documents, each of which describes some aspect of the arrangement and agreement. In all cases, the agreement, regardless of form, should

- be enforceable by the organization
- include detailed and complete specifications that must be met by the external entity *(See EXD:SG3.SP1 and EXD:SG3.SP2.)*
- include any required performance standards or work products from the organization
- be changed to reflect changes in specifications over the life of the relationship

Typical work products

1. Agreements with external entities

Subpractices

1. Select an agreement type that best fits the performance standards required by the organization and that is enforceable if problems arise.
2. Properly document the agreement terms, conditions, specifications, and other provisions.

   All agreement provisions should be documented in the agreement in language that is unambiguous.

   The agreement should not contain any general exceptions for achieving the resilience specifications unless they are carefully considered and negotiated. It may, however, contain scenarios of types of unforeseen events for which the external entity is not expected to prepare. Any exceptions granted to resilience specifications or scenarios for which the external entity is not required to prepare should be treated as risks under EXD:SG2.

   All agreements should establish and enable procedures for monitoring the performance of external entities and inspecting the services or products they deliver to the organization.

   These are examples of elements and dependencies that should be addressed in the agreement (sourced in part from *Outsourcing Technology Services IT Examination Handbook* [FFIEC 2004]):

   - work to be performed, services to be provided, or products to be delivered—Clearly describe the responsibilities of the external entity, including required activities, services, deliverables, and time frames.
   - all relevant enterprise-level specifications *(See EXD:SG3.SP1.)*
   - external entity resilience specifications *(see EXD:SG3.SP2)*, including

  - performance standards—Clearly and measurably define minimum service requirements and remedies for failing to achieve them. These are commonly expressed as SLAs, which are incorporated and made part of the agreement.
  - security, confidentiality, and privacy—The agreement should define obligations of the external entity to protect the organization's assets. The external entity should be prohibited from using such assets except as necessary for the performance of the agreement and should be required to protect against unauthorized use or disclosure. Define disclosure obligations for security breaches and disclosures. The agreement should include any regulatory, legal, or compliance obligations.
  - business resumption and contingency plans—Address the external entity's responsibility for backup and record protection, including equipment, program, and data files, and maintenance and testing of service continuity plans. Include a requirement for any specific recovery time frames and require copies of plans.
  - staff performance or prescreening—Address any requirements related to external entity staff, including any performance or licensing requirements, prescreening requirements, or other qualifications. If any external entity staff members are considered to be vital to the successful performance of the external entity, provisions should be included to address the availability of the vital staff, including notification requirements in the event that they become unavailable.
- controls—Include provisions that address external entity internal controls, compliance with regulations, record keeping, records access, notification and approval rights for material changes in external entity legal structure or form, financial health and reporting, and insurance.
- change procedures—Include procedures for changing any of the agreement provisions by mutual agreement.
- audit—Address audit requirements and provisions for independent audit and review, including audit report requirements and any required periodic reviews.
- reporting—Include frequency and type of reports required.
- subcontracting provisions—The external entity's rights and ability to subcontract its obligations under the agreement to others should be included.
- cost—Fully describe all costs associated with the agreement (base, recurring, special, etc.), including provisions and circumstances for changing cost agreements.
- dispute resolution—Consider including specific provisions for escalation and dispute resolution procedures. Include responsibilities for continued operation and delivery during dispute periods.
- termination—Consider events that would warrant or allow termination by either the organization or the external entity and include time frames for notification and expenses for termination.
- regulatory compliance—Ensure that the external entity will comply with applicable regulations and provide access to regulatory agencies as necessary.
- escrow provisions—If the external entity is providing services based on proprietary or single-source software or other single-source assets, consider including an escrow agreement that would allow the organization to secure the software or single-source assets during extraordinary events.
- external entity assets—If the external entity will be using assets that are supplied by entities external to itself, the agreement should include provisions, as appropriate, for the repair or replacement of the assets, insurance provisions for

the assets, conditions under which the assets may be withdrawn by the external entity, and provisions to replace the assets as needed.

- legal topics such as ownership and license, indemnification, liability, assignment of the agreement to others, and jurisdiction including considerations for foreign-based providers

3. Ensure that the organization and the external entity agree to all agreement provisions and specifications before executing the agreement.

   Negotiation may be required to reach agreement with the external entity on all of the agreement provisions. Any specifications that are waived as a result of negotiations should be treated as risks under EXD:SG2. Once negotiations are complete and the organization and the external entity agree to all of the agreement provisions, the agreement should be executed by representatives from both organizations.

4. Update the agreement as required throughout the duration of the agreement according to provisions established in the agreement.

EXD:SG4 Manage External Entity Performance

The performance of external entities is managed.

The organization must manage external entities by monitoring performance against specifications and taking corrective actions as appropriate.

EXD:SG4.SP1 Monitor External Entity Performance

The performance of external entities is monitored against the specifications.

The performance of external entities against the agreement terms and specifications—particularly those focused on the resilience of the organization's assets and services—must be periodically monitored. This includes all external dependencies for which the entity is responsible. The organization uses the specifications and formal agreements established in EXD:SG3 as the basis and criteria for monitoring the external entity. Any deviations from the established specifications must be analyzed to understand the potential impact on the organization.

To ensure that performance monitoring is performed on a timely and consistent basis, the organization should establish procedures that determine the frequency, protocol, and responsibility for monitoring a particular external entity. (Responsibility is typically assigned to the organizational owner of the relationship.) These procedures should be consistent with the terms of the agreement with the external entity *(see EXD:SG3.SP4)*. It may be appropriate to adjust the monitoring frequency in response to changes in the risk environment, changes to external dependencies, or changes in the external entity.

When the external entity is responsible for producing or delivering assets to the organization, the monitoring process should include inspection of the assets to ensure that they meet all stated specifications including asset resilience requirements.

Typical work products

1. Reports on external entities
2. Relationship management databases showing current performance monitoring information
3. Inspection reports on external entity deliverables

Subpractices

1. Establish procedures and responsibility for monitoring external entity performance and inspecting any external entity deliverables.

   Procedures should be consistent with the agreement between the organization and the external entity and should be based on verifying that the external entity is achieving the specifications as defined in the agreement. All agreement specifications should be considered for monitoring; it may be appropriate to prioritize monitoring and inspection activities based on a risk analysis of the specifications (which includes all external dependencies). Monitoring and inspection procedures should address the external entity's required characteristics, required behaviors, and required performance parameters.

   These are examples of appropriate periodic monitoring activities:

   - reviews of the financial condition, viability, and risks of the external entity
   - audits of the external entity's controls and control environment both for the entity and for external dependencies for which the entity is responsible
   - testing the external entity's service continuity plans independently or in an integrated manner
   - information security risk assessments, vulnerability scans, penetration tests, log reviews, and access control inspections
   - review of compliance activities and records
   - audits of performance specifications
   - evaluations of changes in staff and review of staff prescreening activities
   - inspection of deliverables against any or all specifications
   - review of insurance coverage
   - evaluation of any subcontractor usage

2. Meet periodically with external entity representatives to review the result of monitoring activities, the specifications in the agreement, and any changes in either the organization or the external entity that might impact performance under the agreement.
3. Evaluate any deviations in the performance of the external entity from the established specifications to determine the risk to the organization's operation and to inform the selection of corrective actions.

EXD:SG4.SP2 Correct External Entity Performance

Corrective actions are implemented to support external entity performance as necessary.

Implementing corrective actions is a necessary part of managing external entity performance. The objective of any corrective action is to minimize the disruption to the organization's operation or the risk of any such disruption based on external dependencies. The range of corrective actions should be established in the agreement with the external entity, and an evaluation of alternatives should be completed prior to implementing corrective actions.

In cases in which the external entity is developing or otherwise providing an asset or assets to the organization, the appropriate corrective action may be to reject the delivery of the assets.

Corrective actions should be documented in accordance with specifications in the agreement and used to inform and improve ongoing monitoring of the external entity.

Typical work products

1. Corrective action reports or documentation
2. Correspondence with an external entity documenting corrective actions

Subpractices

1. Evaluate alternative corrective actions to select the optimal corrective action.

   The agreement should be reviewed to identify appropriate and allowable corrective actions for consideration. The various alternatives should be evaluated based on their likelihood to succeed in correcting the situation and mitigating any associated risks.

   It may be valuable and appropriate to include the external entity in the discussion and consideration of alternatives, especially if both the organization and the external entity desire to continue the relationship.

2. Communicate with the external entity to review selected corrective actions.

   Communication provisions in the agreement should be followed to formalize the communication.

3. Implement selected corrective actions.
4. Monitor as appropriate to ensure that issues are remedied in a timely manner.
5. Update the agreement with the external entity as required.

Elaborated Generic Practices by Goal

Refer to the Generic Goals and Practices document in Appendix A for general guidance that applies to all process areas. This section provides elaborations relative to the application of the Generic Goals and Practices to the External Dependencies Management process area.

EXD:GG1 Achieve Specific Goals

The operational resilience management system supports and enables achievement of the specific goals of the External Dependencies Management process area by transforming identifiable input work products to produce identifiable output work products.

EXD:GG1.GP1 Perform Specific Practices

Perform the specific practices of the External Dependencies Management process area to develop work products and provide services to achieve the specific goals of the process area.

Elaboration:

Specific practices EXD:SG1.SP1 through EXD:SG4.SP2 are performed to achieve the goals of the external dependencies management process.

EXD:GG2 Institutionalize a Managed Process

External dependencies management is institutionalized as a managed process.

EXD:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the external dependencies management process.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the external dependencies management process area.

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the external dependencies management process may be exhibited by

   - extending the role of the chief acquisition or procurement officer (or equivalent) to include ensuring that all RFPs and agreements with external entities reflect resilience specifications
   - developing and publicizing higher level managers' objectives and requirements for managing the process
   - providing oversight of external entity access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization
   - sponsoring and providing oversight of policy, procedures, standards, and guidelines for evaluating, selecting, and managing relationships with external entities, including the management of the process
   - providing oversight of the process for establishing formal agreements with external entities, including contracts and SLAs

- making higher level managers aware of applicable compliance obligations related to external dependencies, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- oversight over the establishment, implementation, and maintenance of an appropriate level of controls to ensure the resilience of services and assets that rely upon the actions of external entities
- sponsoring and funding process activities
- providing guidance for prioritizing external dependencies relative to the organization's high-priority strategic objectives
- providing guidance on identifying, assessing, and managing operational risks related to external dependencies
- providing guidance for resolving violations of enterprise and resilience specifications by external entities
- verifying that the process supports strategic resilience objectives and is focused on the assets and services that are of the highest relative value in meeting strategic objectives
- regular reporting from organizational units to higher level managers on process activities and results
- creating dedicated higher level management feedback loops on decisions about external dependencies and recommendations for improving the process
- conducting regular internal and external audits and related reporting to appropriate committees on the effectiveness of the process
- creating formal programs to measure the effectiveness of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

Elaboration:

The external dependencies management policy should address

- responsibility, authority, and ownership for performing process activities
- procedures, standards, and guidelines for
  - identifying and prioritizing external dependencies
  - associating external dependencies with services and assets
  - managing operational risks resulting from external dependencies
  - evaluating and selecting external entities
  - formalizing and enforcing agreements with external entities, including changing any provisions by mutual agreement
  - developing and documenting enterprise and resilience specifications for external entities, including organizational policies to which external entities are expected to adhere
  - standards of performance and service levels *(Refer to EXD:SG3.SP2 subpractice 4.)*
  - establishing service continuity plans and procedures for external entities
  - monitoring the performance of external entities, including inspecting the services or products they deliver (Such procedures specify frequency, protocol, and responsibility for monitoring and inspection.)
  - terminating relationships with external entities as specified in formal agreements

  - issue escalation and dispute resolution
- requesting, approving, providing, and terminating access for external entities *(Refer to the Access Management process area for more information about granting access [rights and privileges] to organizational assets. Refer to the Identity Management process area for more information about creating and maintaining identities for persons, objects, and entities.)*
- methods for measuring adherence to policy, exceptions granted, and policy violations

EXD:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the external dependencies management process.

Elaboration:

A plan for performing the external dependencies management process is developed to ensure that the organization can satisfy its operational resilience requirements when an external entity has access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization. The plan must address the enterprise and resilience specifications for the service being performed or the product being provided (i.e., the external dependency) by the external entity. In addition, because external entities can be located in many geographical locations, the plan must address those external entities and stakeholders that can enable or adversely affect operational resilience.

The plan for the external dependencies management process should not be confused with service continuity (recovery, restoration) plans for assets and services that are under the control of external entities. The plan for the external dependencies management process details how the organization will manage external dependencies and relationships with external entities, including the development of service continuity plans where such entities are involved. *(The generic practices for service continuity planning are described in SC:SG1 through SC:SG4 in the Service Continuity process area.)*

Subpractices

1. Define and document the plan for performing the process.
2. Define and document the process description.
3. Review the plan with relevant stakeholders and get their agreement.
4. Revise the plan as necessary.

EXD:GG2.GP3 Provide Resources

Provide adequate resources for performing the external dependencies management process, developing the work products, and providing the services of the process.

Elaboration:

A wide range of organizational resources and skills is required to oversee and manage external entity access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization. This includes the diversity of activities

required to identify, prioritize, evaluate, select, formalize agreements with, and manage a wide range of relationships with external entities. In addition, these activities may require a major commitment of financial resources (both expense and capital) from the organization.

Subpractices

1. Staff the process.

   Elaboration:

   These are examples of staff required to perform the external dependencies management process:

   - staff responsible for
     - identifying and prioritizing existing external dependencies and keeping this information up-to-date based on changing business conditions
     - service continuity as it involves external dependencies and entities
     - preparing RFPs, including applicable SLAs
     - evaluating proposals and selecting external entities
     - establishing formal agreements with external entities
     - monitoring the performance of external entities to ensure they are meeting their agreements and specifications, and taking corrective action when appropriate
     - inspecting deliverables
   - staff involved in identifying, assessing, and mitigating risks that may arise due to external dependencies and when engaging external entities
   - facilities management staff for physical assets that are under the control of external entities
   - asset and service owners and custodians (to identify and enforce resilience specifications that must be satisfied by external dependencies and entities)

   Refer to the Organizational Training and Awareness process area for information about training staff for resilience roles and responsibilities.

   Refer to the Human Resource Management process area for information about acquiring staff to fulfill roles and responsibilities.

2. Fund the process.

   Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for external dependencies.

3. Provide necessary tools, techniques, and methods to perform the process.

   Elaboration:

   These are examples of tools, techniques, and methods to support the external dependencies management process:

   - methods, techniques, and tools for identifying and prioritizing the list of external dependencies and keeping it up-to-date
   - methods, techniques, and tools for identifying and managing risks due to external dependencies, including tracking open risks to closure and monitoring the effectiveness of risk mitigation plans
   - templates for RFPs, SLAs, and formal agreements

- proposal evaluation checklists
- methods, techniques, and tools for monitoring and reporting the performance of external entities
- methods, techniques, and tools for inspecting deliverables
- relationship management databases

EXD:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the external dependencies management process, developing the work products, and providing the services of the process.

Elaboration:

Those responsible for services and assets are involved in identifying and prioritizing external dependencies and establishing resilience specifications that external entities must fulfill. Formal agreements identify external entity actions, including ensuring continuity of operations during times of stress. EXD:SG1.SP1 calls for identifying the organizational owner of each relationship with an external entity; EXD:SG4.SP1 calls for monitoring the performance of external entities against their specifications. Similarly, EXD:SG2.SP2 requires the identification of those responsible for addressing, tracking, and mitigating risks that arise from external dependencies and relationships with external entities.

In EXD:GG2.GP4, responsibilities are assigned to activities of the external dependencies management process.

Refer to the Human Resource Management process area for more information about establishing resilience as a job responsibility, developing resilience performance goals and objectives, and measuring and assessing performance against these goals and objectives.

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   The organization must ensure that responsibility and authority extend to all external entities and to any entities with which the external entity has contracted to provide services or products in support of the external entity's formal agreement with the organization.

2. Assign responsibility and authority for performing the specific tasks of the process.

   Elaboration:

   Responsibility and authority for performing external dependencies management tasks can be formalized by

   - defining roles and responsibilities in the process plan
   - including process tasks and responsibility for these tasks in specific job descriptions
   - developing policy requiring organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to

participate in the process for services and assets under their ownership or custodianship

- developing and implementing agreements, including contracts, SLAs, memoranda of agreement, purchase orders, and licensing agreements
- including process tasks in staff performance management goals and objectives, with requisite measurement of progress against these goals

3. Confirm that people assigned with responsibility and authority understand it and are willing and able to accept it.

EXD:GG2.GP5 Train People

Train the people performing or supporting the external dependencies management process as needed.

Refer to the Organizational Training and Awareness process area for more information about training the people performing or supporting the process.

Refer to the Human Resource Management process area for more information about inventorying skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.

   Elaboration:

   These are examples of skills required in the external dependencies management process:

   - identifying and prioritizing external dependencies
   - affinity analyses
   - elicitation of resilience specifications to be reflected in RFPs and agreements with external entities
   - evaluating and selecting external entities
   - negotiating agreements with external entities
   - prioritizing external entities based on the priority of the external dependencies for which the entity is responsible
   - knowledge of tools, techniques, and methods that can be used to identify, analyze, mitigate, and monitor operational risks resulting from external dependencies and from relationships with external entities
   - managing relationships with external entities
   - monitoring the performance of external entities, including the inspection of deliverables and knowing when corrective actions are called for

2. Identify process skill gaps based on available resources and their current skill levels.
3. Identify training opportunities to address skill gaps.

Elaboration:

These are examples of training topics:

- contract negotiation
- prioritizing external dependencies based on established criteria
- developing resilience specifications for external entities
- cross-training to ensure adequate knowledge and coverage for all external dependencies
- terminating agreements with external entities
- supporting service owners and asset owners and custodians in understanding the process and their related roles and responsibilities
- using process methods, tools, and techniques, including those identified in EXD:GG2:GP3 subpractice 3

4. Provide training and review the training needs as necessary.

EXD:GG2.GP6 Control Work Products

Place designated work products of the external dependencies management process under appropriate levels of control.

Elaboration:

These are examples of external dependencies work products placed under control:

- list of external dependencies, with priorities
- criteria for prioritizing external dependencies
- affinity analyses results to inform dependency prioritization and risk identification
- information that defines external dependencies, stored as a maintainable information repository or database
- risk statements with impact valuation
- list of external dependency risks with categorization and prioritization, risk disposition, mitigation plans, and current status
- agreement templates, including enterprise specifications that apply to external entities
- external dependencies and resilience specifications that apply to each external entity
- RFPs, including applicable SLAs
- criteria for selecting external entities
- proposal evaluation results and decision rationale
- agreements with external entities, including contracts, memoranda of agreement, purchase orders, and licensing agreements
- performance-monitoring reports
- relationship management databases
- inspection reports on deliverables
- corrective-action reports
- process plan
- policies and procedures

EXD:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the external dependencies management process as planned.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   Because external entities may reside in a wide range of physical locations and provide and support numerous processes, services, and assets, a substantial number of stakeholders are likely to be external to the organization.

   These are examples of stakeholders of the external dependencies management process:

   - internal and external owners and custodians of organizational assets
   - internal and external service owners
   - organizational unit and line of business managers responsible for high-value assets and the services they support
   - staff responsible for managing operational risks arising from external dependencies and relationships with external entities
   - staff responsible for establishing, implementing, and maintaining an internal control system for organizational assets where an external dependency and an external entity are involved
   - staff required to develop, test, implement, and execute service continuity plans that involve external dependencies and external entities
   - acquisition and procurement staff
   - internal and external auditors

   Stakeholders are involved in various tasks in the external dependencies management process, such as

   - planning for evaluating, selecting, and managing relationships with external entities
   - creating and maintaining a prioritized inventory of all external dependencies
   - establishing and periodically reviewing prioritization criteria
   - analyzing services and assets to determine their dependencies on external entities
   - identifying resilience specifications for external entities
   - ensuring that service continuity plans reflect all external dependencies as well as the actions of external entities
   - managing operational risks that arise from external dependencies and relationships with external entities
   - monitoring the performance of external entities
   - renegotiating and terminating relationships with external entities
   - reviewing and appraising the effectiveness of process activities
   - resolving issues in the process

2. Communicate the list of stakeholders to planners and those responsible for process performance.

3. Involve relevant stakeholders in the process as planned.

EXD:GG2.GP8 Measure and Control the Process

Measure and control the external dependencies management process against the plan for performing the process and take appropriate corrective action.

Refer to the Monitoring process area for more information about the collection, organization, and distribution of data that may be useful for measuring and controlling processes.

Refer to the Measurement and Analysis process area for more information about establishing process metrics and measurement.

Refer to the Enterprise Focus process area for more information about providing process information to managers, identifying issues, and determining appropriate corrective actions.

Subpractices

1. Measure actual performance against the plan for performing the process.
2. Review accomplishments and results of the process against the plan for performing the process.

   Elaboration:

   These are examples of metrics for the external dependencies management process:

   - percentage of services that rely on the external dependency
   - percentage of assets that rely on the external dependency
   - number of services that rely on the external entity, by type of service (if applicable)
   - number of assets that rely on the external entity, by type of asset
   - number of external dependencies which rely on the external entity
   - number of compliance obligations that rely on or apply to the external entity
   - monetary value of the relationship with the external entity
   - number of agreement changes by change type
   - number of entities external to itself upon which the external entity relies to meet its obligations
   - percentage of assets that rely on external entities
   - percentage of services that rely on external entities
   - number of external entities by relationship status (RFP, source selection, awarded, agreement/contract executed, performing as expected, out of compliance, in dispute or litigation, terminated, renewed, etc.)
   - number of external entities at each CERT-RMM capability level by process area
   - percentage of external dependencies without a designated owner
   - percentage of external entities without a designated owner
   - percentage of external dependencies involved in meeting compliance obligations
   - percentage of external entities involved in meeting compliance obligations
   - number of external entities that are providing “commodity” services (easily replaced)
   - number of external entities that are providing “specialized” services (difficult to replace)

- number of external entities in the same geographic region (for assessing geographic and socio-political risk)
- number of external entities for which the relationship is managed by another part of the organization than the one owning the relationship
- percentage of external dependencies that have not been reviewed and updated as scheduled
- elapsed time since risk assessment of external dependencies
- percentage of external dependencies for which a risk assessment has not been performed and documented (per policy or other guidelines) according to plan
- percentage of external dependency risks that have not been assigned to a responsible party for action, tracking, and closure
- percentage of external dependency risks with a disposition of "mitigate or control" that do not have a defined mitigation plan
- percentage of external dependency risks with a "mitigate or control" disposition that are not effectively mitigated by their mitigation plans
- percentage of realized risks for external dependencies that exceed established risk parameters
- percentage of RFPs for external entities that do not include resilience specifications
- percentage of candidate external entities whose due diligence process is on track per plan
- percentage of selected external entities without documented selection and decision rationale (this should be zero)
- number of resilience specifications unmet by the selected external entity
- number of resilience specifications unmet by the selected external entity that are identified as risks to be managed (ranked)
- percentage of agreements/contracts with external entities with specifications that have been waived as a result of negotiations
- percentage of external entities that are achieving all specifications as defined in the agreement
- percentage of external entity agreements that have not been reviewed as scheduled (including in response to changes in enterprise and resilience specifications)
- percentage of external entities whose status (monitoring and inspection activities) has not been reviewed as scheduled
- percentage of external entities that have undergone reviews as required by agreement/contract
- percentage of external entities that have undergone risk assessments as required by agreement/contract percentage of external entities that have undergone, as required by agreement/contract
- percentage of external entities that have undergone testing or other evaluations as required by agreement/contract
- percentage of external entities that have undergone inspections or audits as required by agreement/contract
- percentage of external entities with corrective actions that have not been implemented as scheduled
- percentage of external entities whose deliverables have failed to pass inspection
- for all or specific external entities, elapsed time since last:
  - risk assessment

  - performance review
  - compliance audit
  - joint service continuity exercise
- for all applicable external entities, elapsed time since source code was last updated in source code escrow
- percentage of external entity risks that have not been assigned to a responsible party for action, tracking, and closure
- percentage of realized risks for external entities that exceed established risk parameters
- percentage of external entities whose financial health is at risk (beyond risk parameters)
- percentage of external entities whose performance deviates sufficiently from specifications (beyond risk parameters) to cause a risk to be referred to the risk management process
- percentage of external entities that play a key role in fulfilling service continuity plans during disruptive events
- percentage of external entities that have tested their service continuity plans, including participating in tests conducted of organization's service continuity plans
- percentage of external entities that failed to perform as expected during a disruptive event

3. Review activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues.

Elaboration:

Reviews will likely verify the accuracy and completeness of the list of external dependencies and their current status.

Periodic reviews of the external dependencies management process are needed to ensure that

- criteria for selecting and evaluating external entities reflect current business objectives and priorities
- new external dependencies are included and prioritized in an information repository or database, and terminated dependencies are removed
- agreements with external entities include stated resilience specifications
- the mapping of external dependencies to services and assets (and vice versa) is accurate and current
- ownership of external dependencies and external entities is established and documented
- the relationship management database captures the performance of all external entities
- poor or failed performance, disputes, and areas of non-compliance are addressed in a timely manner
- status reports are provided to appropriate stakeholders in a timely manner
- process issues are referred to the risk management process when necessary
- actions requiring management involvement are elevated in a timely manner
- the performance of process activities is being monitored and regularly reported

- key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
- actions resulting from internal and external audits are being closed in a timely manner

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.
5. Identify problems in the plan for performing and executing the process.
6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.

   Elaboration:

   Corrective action may require the revision of existing formal agreements.

7. Track corrective action to closure.

EXD:GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the external dependencies management process against its process description, standards, and procedures, and address non-compliance.

Elaboration:

These are examples of activities to be reviewed:

- identifying and prioritizing external dependencies
- specifying resilience specifications in agreements with external entities
- identifying and managing risks due to engaging with external entities
- evaluating and selecting external entities
- formalizing relationships with external entities
- reflecting the involvement of external entities in organizational service continuity plans and ensuring that external entities have service continuity plans for their own operations that are periodically tested
- monitoring the performance of external entities and taking corrective action as required
- identifying and managing changes to agreements with external entities
- aligning stakeholder requirements with process plans
- assigning responsibility, accountability, and authority for process activities
- determining the adequacy of external dependencies reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any

These are examples of work products to be reviewed:

- prioritized list of external dependencies with their current status
- risk statements related to external dependencies and external entities
- risk mitigation plans
- service continuity plans for external entities, including vital staff
- agreements with external entities
- process plan and policies

- process issues that have been referred to the risk management process
- process methods, techniques, and tools
- metrics for the process *(Refer to EXD:GG2.GP8 subpractice 2.)*

EXD:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the external dependencies management process with higher level managers and resolve issues.

Elaboration:

Status reporting on the external dependencies management process may be part of the formal governance structure or be performed through other organizational reporting requirements (such as through the chief acquisition or procurement officer level or equivalent). Audits of the process may be escalated to higher level managers through the organization's audit committee of the board of directors or similar construct in private or non-profit organizations.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management system.

EXD:GG3 Institutionalize a Defined Process

External dependencies management is institutionalized as a defined process.

EXD:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined external dependencies management process.

Elaboration:

Managing external dependencies, including relationships with the external entities responsible for them, is typically carried out at the organizational unit or line of business level (where ownership of the relevant service or asset resides) and may have to be geographically focused (due to the location of specific external entities). However, to achieve consistent results in managing these relationships, the activities at the organizational unit or line of business level must be derived from an enterprise definition of the external dependencies management process. Agreements (including resilience specifications), dependency priorities, and performance monitoring may be inconsistent across organizational units, particularly when a specific external entity supports multiple units or multiple external entities support a specific service or asset. Inconsistencies in managing relationships with external entities across the enterprise can impede operational resilience.

Establishing and tailoring process assets, including standard processes, are addressed in the Organizational Process Definition process area.

Establishing process needs and objectives and selecting, improving, and deploying process assets, including standard processes, are addressed in the Organizational Process Focus process area.

Subpractices

1. Select from the organization's set of standard processes those processes that cover the external dependencies management process and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization's tailoring guidelines.
3. Ensure that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.
5. Revise the description of the defined process as necessary.

EXD:GG3.GP2 Collect Improvement Information

Collect external dependencies work products, measures, measurement results, and improvement information derived from planning and performing the process to support the future use and improvement of the organization's processes and process assets.

Elaboration:

These are examples of improvement work products and information:

- prioritized list of active external dependencies and their current status
- inconsistencies and issues with external dependencies
- improvements based on risk identification and mitigation
- effectiveness of executed service continuity plans that rely upon external dependencies and entities
- metrics and measurements of the viability of the process *(Refer to EXD:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect external dependencies and relationships with external entities
- lessons learned in post-event review of external entity incidents and disruptions in continuity
- conflicts and risks arising from external dependencies and reliance on external entities
- lessons learned in managing the life cycle of an engagement with an external entity
- resilience specifications that are not being satisfied or are being exceeded

Establishing the measurement repository and process asset library is addressed in the Organizational Process Definition process area. Updating the measurement repository and process asset library as part of process improvement and deployment is addressed in the Organizational Process Focus process area.

Subpractices

1. Store process and work product measures in the organization's measurement repository.
2. Submit documentation for inclusion in the organization's process asset library.

3. Document lessons learned from the process for inclusion in the organization's process asset library.
4. Propose improvements to the organizational process assets.