EXTERNAL DEPENDENCIES MANAGEMENT (EDM)

Question Set with Guidance

April 2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

DM19-0492

1 Contents

Acquirer Information

Facilitator

Name:
Phone:
Email:

Date of EDM Assessment *(Please use popup calendar):*

Name of Acquirer/Business Unit:

Sector:

Critical Service:

Physical Location

City:

State:

Critical Service Point of Contact

Name:

Phone:

Email:

1 Relationship Formation

	Goal 1 – Acquirer service and asset priorities are established. The purpose of this goal is to assess whether the acquirer has identified its own critical services, assets, and control objectives because these are foundational activities for effectively managing external dependencies.	Guidance
	1. Are the acquirer's services identified and documented across the enterprise? [SC:SG2.SP1]	**Question intent:** To determine if the acquirer identifies and documents its critical services across the enterprise. **Typical work products:** • leadership communication or command media listing acquirer's services • services listed in current policy or similar guidance **Criteria for "Yes" Response:** • The acquirer has documented all of its services as a part of an established business process and the current list of services is accurate. **Criteria for "Incomplete" Response:** • The list of services is partially documented, or the practice appears otherwise incomplete.
	2. Are the acquirer's services prioritized based on an analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	**Question intent:** To determine if the acquirer's services are prioritized based on impact to the organization. Prioritizing critical services is foundational to making good enterprise decisions about protecting and sustaining these services. Prioritization of services is accomplished by considering the consequences of their loss. Typically prioritization is performed as part of a business impact analysis or as part of risk management activities. **Typical work products:** • prioritized list of acquirer services • results of security risk assessment and business impact analyses **Criteria for "Yes" Response:** • The acquirer's list of critical services indicates a priority, or there is an otherwise documented

		prioritization of critical services. **Criteria for "Incomplete" Response:** • The acquirer has a general sense of what the important services are, but there is no documented prioritization, or the prioritization is partially documented, or the practice appears otherwise incomplete.
	3. Are the acquirer's assets that directly support the critical service inventoried? [ADM SG1.SP1]	**Question intent:** To determine if the acquirer identifies and inventories its own assets that support the critical service. In the context of External Dependencies Management, identifying key assets is important because external entities may affect or otherwise have obligations with respect to these assets. The following are examples of obligations or duties that external entities may have with respect to assets that support the critical service. • Suppliers may serve as the 'containers' or have other obligations with respect to information for which the acquirer is responsible. For example, an acquirer in the medical industry may entrust protected health information to a third party. • Suppliers may have other specific obligations relative to acquirer assets, for example, maintenance or other support. • Local or regional governmental authorities may have a role in sustaining or ensuring that key assets are available – for example, in securing or managing transportation networks used by the acquirer's personnel. • External entities may be used as an entry point by malicious actors to harm or damage acquirer assets. For example, attackers may use access granted to a third party to enter and attack acquirer networks and systems. **Typical work products:** • asset inventories **Criteria for "Yes" Response:** • The acquirer has documented in one or more repositories the people, information, technologies, and facilities essential to the operation of the critical service and this documentation is current. **Criteria for "Incomplete" Response:** • The acquirer has documented some assets that support the critical service, or it has documented

<table>
<tr><td></td><td></td><td>some asset types but not others (for example, it documents the technology that supports the service but not the people), or the practice appears otherwise incomplete.</td></tr>
<tr><td></td><td>4. Have control objectives been established for acquirer assets that support the critical service(s)? [CTRL:SG1.SP1]</td><td>Question intent: To determine if control objectives have been established for the assets required to deliver the critical service.

A control objective is a performance target for a control or control system. Control objectives are important to external dependencies management because external entities are often responsible for establishing and maintaining controls over assets for which the acquirer is responsible. Control objectives provide a way to evaluate and correct the actions of third parties.

• Control objectives provide a set of high-level requirements for the protection and sustainment of a critical service and associated assets.
• Sources for identifying control objectives may be found in governance documents, policy documents, etc.

The following table provides examples of control objectives as they pertain to asset types.

<table>
<tr><th>Asset Type</th><th>Control Objective Example</th></tr>
<tr><td>People</td><td>• Prior to hiring candidates for employment, ensure they are trustworthy and reliable.
• All outside support personnel are identified.</td></tr>
<tr><td>Information</td><td>• Ensure the confidentiality and integrity of customers’ payment information.
• Information assets are disposed of according to policy.</td></tr>
<tr><td>Technology</td><td>• Ensure the databases that support one or more critical services remain available.
• Network integrity is protected.</td></tr>
<tr><td>Facilities</td><td>• Ensure environmental systems are maintained at an appropriate level to support datacenter equipment.
• Physical access to assets is managed and protected.</td></tr>
</table>

Typical work products:</td></tr>
</table>

		• A current documented set of control objectives for key assets that support the critical service • Internal correspondence or command media relevant to control objectives **Criteria for "Yes" Response:** • Control objectives are established and documented for all assets that support the critical service (people, information, technology, and facilities). **Criteria for "Incomplete" Response:** • Control objectives are established and documented for some assets that support the critical service, or the practice appears otherwise incomplete.
	Goal 2 – Forming relationships with external entities is planned. The purpose of this goal is to assess whether the acquirer has processes in place to enter into relationships and agreements with external entities.	**Guidance**
	1. Does the acquirer have an established process for entering into formal agreements with external entities? [EXD:SG3.SP3]	**Question intent:** To determine if the acquirer has an established process for selecting and forming relationships with external entities that support the critical service. Having an established process can help the acquirer make better selections, including choosing external entities that align more closely with the acquirer's needs and requirements. Having an established process means that: • There are specific steps or activities that acquirer staff must complete when completing the activity, in this case forming relationships on behalf of the acquirer. • The process is supported by documentation. The process need not be documented in one consolidated plan, but it should be documented to support the process. For example, staff responsible for sourcing suppliers may have written criteria for selecting suppliers. Staff may have a written checklist or other guidance to complete before submitting contracts for approval, etc. • The acquirer's staff is aware that the process exists and that they are expected to follow it. • The process applies to formal agreements with any type of external entity to support the critical service.

		Typical work products: • documented external entity selection criteria • roles and assignments of responsibility in job descriptions • internal reporting requirements • documented acquirer approval authorities • standard contract requirements **Criteria for "Yes" Response:** • The acquirer has an established process for entering into formal agreements with external entities that support the critical service. **Criteria for "Incomplete" Response:** • A process exists but some staff are not aware of it, or it is not supported by documentation, or it applies only to some types of external entities, or the practice appears otherwise incomplete.
	2. Has the acquirer identified and documented baseline (boilerplate) requirements that apply to any supplier that supports the critical service? [EXD:SG3.SP1]	**Question intent:** To determine if the acquirer has established a set of baseline requirements that apply to all formal agreements with suppliers that support the critical service. Consistency across multiple supplier contracts can help the acquirer achieve a higher degree of predictability and control among external entities and help to ensure that all suppliers meet at least a minimal level of requirements. Developing baseline requirements normally involves an evaluation of the acquirer's enterprise requirements. These are the requirements that the enterprise deems important for every supplier relationship. Regulatory requirements may often form the basis for these. For example, in the medical field, laws to protect the confidentiality of protected health information (PHI) require standard requirements for every third party that stores this information. **Typical work products:** • standard contract language that includes, for example, reporting, compliance, and flow down requirements **Criteria for "Yes" Response:** • The acquirer has a documented collection of baseline contractual requirements for suppliers that support the critical service. **Criteria for "Incomplete" Response:**

		• The acquirer has a partially documented collection of baseline contractual requirements for suppliers, or the baseline requirements apply to only some suppliers, or the practice appears otherwise incomplete.
	3. Does the acquirer have a process to identify and document resilience requirements for specific external entities (suppliers, infrastructure providers, and governmental services) that support the critical service? [EXD:SG3.SP2]	**Question intent:** To determine if the acquirer has processes to identify and document resilience requirements for each external entity that supports the critical service. Developing requirements is a basic resilience activity, regardless of the acquirer's ability to actually enforce requirements with a specific external entity. Resilience requirements for external entities are important because • They form the basis for supplier formal agreements. • Documented requirements are used as a means to evaluate external entity performance. • They inform risk management. Failures of an external entity to meet requirements should be monitored and managed as risks. Having an established process means that • There are specific steps or activities that acquirer staff must complete. • The process is supported by appropriate documentation. For example, there may be a documented schedule of meetings to identify requirements. • The acquirer's staff is aware that the process exists and that they are expected to follow it. The process to identify requirements for governmental services or infrastructure providers may differ widely across organizations. Many organizations manage these relationships centrally or at the corporate level. A process to identify requirements for governmental services or infrastructure providers is adequate if • It allows for requirements that support the critical service to be documented, and • It allows for the documented requirements to inform the acquirer's activities to manage governmental or infrastructure relations. **Typical work products:** • roles and responsibilities documented in job

		descriptions • meeting agendas • internal correspondence • documented resilience requirements of the critical service **Criteria for "Yes" Response:** • The acquirer has a process or processes to identify and document requirements for external entities that support the critical service. **Criteria for "Incomplete" Response:** • The process or processes appear ad-hoc, or only includes some types of external dependencies, or the practice appears otherwise incomplete.
	4. Does the acquirer's process to enter into formal agreements with suppliers ensure that resilience requirements are considered before entering into agreements? [EXD:SG3.SP3]	**Question intent:** To determine if the acquirer's established process to enter into formal agreements with external entities ensures that resilience requirements are considered. It is not unusual for organizations to have a well-documented process for entering into formal agreements with suppliers, which does not take into consideration the resilience requirements of the critical service. Some common reasons that the acquirer's process to form external entity relationships may be deficient include: • The process may be dictated or determined by other organizational units and not designed with the critical service in mind. • The appropriate staff have not been included in the process. • The process may be exclusively focused on other objectives, for example achieving the lowest cost or preventing undue influence over the formation of contracts. **Typical work products:** • checklists that require review of formal agreements to ensure inclusion of resilience requirements • meeting agendas and notes indicating participation by relevant staff • job descriptions that require participation in the process by relevant staff **Criteria for "Yes" Response:** • The acquirer's process to enter into formal

		agreements with external entities ensures resilience requirements are considered before entering into formal agreements. **Criteria for "Incomplete" Response:** • There are deficiencies in the process, for example resilience requirements are only sometimes considered, or the practice appears otherwise incomplete. **Additional guidance**
	Goal 3 – Risk management includes external dependencies. The purpose of this goal is to assess whether the acquirer's risk management capability includes external dependencies.	**Guidance**
	1. Has a plan for managing operational risk been established and agreed to by Stakeholders? [RISK:SG1.SP2]	**Question intent**: To determine if the acquirer has a plan for managing operational risk. An operational risk management plan provides a common foundation for the performance of risk management activities. For External Dependencies Management, having a plan that includes external dependencies helps to coordinate management of these risks with the acquirer's risk appetite and broader risk strategy. Operational risk is defined as the potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, deliberate or inadvertent actions of people, or external events (weather, disasters, war, etc.). Any of these sources of risk can affect both the acquirer directly and also the external entities on which the acquirer depends. Typical items addressed in an operational risk management plan include: • the scope of operational risk management activities • the methods to be used for operational risk identification, analysis, mitigation, monitoring, and communication • the sources of operational risk • how the sources of operational risk should be organized, categorized, compared, and consolidated • parameters for measuring and taking action on operational risks

		• risk mitigation techniques to be used, such as the development of layered administrative, technical, and physical controls • definition of risk measures to monitor the status of operational risks • time intervals for risk monitoring and reassessment **Typical work products:** • Complete, written risk management plan **Criteria for "Yes "response** • There is a documented plan for managing operational risks, and this document is used to guide risk management. **Criteria for "Incomplete" Response:** • The operational risk management plan is incomplete, or it exists but does not guide risk management in the organization, or the practice appears otherwise incomplete.
	2. Are the risks of relying on external entities to support the critical service identified and managed (accepted, transferred, mitigated, etc.)? [EXD:SG2.SP1] Suppliers Infrastructure providers Governmental services	**Question intent:** To determine if risks due to external dependencies are identified and managed as part of operational risk management at the acquirer. This question is separated into the three types of external entities in this assessment. In order to answer the question affirmatively for each type of entity, the organization's risk management activities must encompass or include the identification and management of risks relating to each type of entity. **Typical work products:** • an operational risk management plan that describes processes or activities to identify and manage external dependency risks • external dependency risk statements • a list of external dependency risks, with categorization and prioritization • assessment or audit reports of third parties to confirm they are meeting contractual obligations **Criteria for "Yes" Response:** • The acquirer identifies risks associated with external dependencies in each entity type specified, and all risks are managed (impacts identified and analyzed, and the disposition of risk determined). **Criteria for "Incomplete" Response:** • The acquirer identifies and manages risks associated with some external dependencies in

		each category, or the practice appears otherwise incomplete.
	3. Does the acquirer identify and manage the risk of an external entity being a single point of failure? [EXD:SG1.SP2]	**Question intent:** To determine if the acquirer identifies single points of failure in the external entities it depends on and manages the resulting risk. A single point of failure means that a single disruption or interruption involving an external entity would cause a failure or significant disruption of the critical service. An example of a single point of failure is a supplier that is the sole source of a critical service or critical asset, and for whom there is no substitute readily available (i.e., on standby or actively operating in parallel). This question asks about a specific risk management practice and requires that single points of failure be identified and managed as risks (i.e., formally accepted, mitigated, transferred, monitored, etc.). Failure to recognize single points of failure may result in neither the organization nor relevant external entities putting sufficient controls and mitigations in place to guard against this risk. Single points of failure need not be organizations with which the acquirer has a formal agreement or direct relationship. For example • Two or more of the acquirer's suppliers may rely on a third party or "second-tier" supplier. • Multiple suppliers (for example, two outsourced data centers) may be in the same geographic region and therefore subject to the same natural disaster. • Multiple suppliers may rely on the same infrastructure providers. These 'second tier' points of failure – which may affect multiple suppliers, for example – are also sometimes known as "common modes of failure." **Typical work products:** • guidance in the operational risk management plan concerning single points of failure • internal correspondence relating to the identification and management of single points of failure as risks • assessment or audit reports of third parties to confirm they are meeting contractual obligations

		Criteria for "Yes" Response: • The acquirer analyzes the external entities that support the critical service to identify single points of failure as a required part of risk management, and these risks are managed (impacts are identified and analyzed, and the disposition of risks assigned). **Criteria for "Incomplete" Response:** • The organization examines only some external entities that support the critical service for single points of failure, or risks are identified but not managed, or the practice appears to be otherwise incomplete.

	Goal 4- External entities are evaluated The purpose of this goal is to assess whether the acquirer evaluates external entities for their ability to meet the critical service's resilience requirements before entering into relationships.	Guidance
	1. Are resilience requirements included in written communications with prospective suppliers, for example in requests for proposals (RFPs)? [EXD:SG3.SP3]	**Question intent:** To determine if the acquirer includes resilience requirements in communications, such as solicitation packages and requests for proposals (RFPs), with prospective suppliers. This practice is important because it provides prospective suppliers with notice of what will be required of them to support the critical service, including relevant roles and responsibilities for cybersecurity staff. It can also help reduce the likelihood that the acquirer will contract with a supplier that is incapable of meeting the critical service's resilience requirements. **Typical work products:** • solicitation packages/RFPs that include documented resilience requirements **Criteria for "Yes" Response:** • The acquirer includes applicable resilience requirements in communications with all prospective suppliers. **Criteria for "Incomplete" Response:** • The acquirer includes applicable resilience requirements in communications with some prospective suppliers, or the practice appears otherwise incomplete.
	2. Does the acquirer consider the ability of suppliers to meet the resilience requirements of the critical service before entering into formal agreements? [EXD:SG3.SP3]	**Question intent:** To determine if the ability of suppliers to meet resilience requirements is considered before forming formal relationships. A basic component of external dependencies management is to form relationships with external entities that are capable of supporting, protecting, and sustaining the critical service. **Typical work products:** • internal communications or policy artifacts • SAS70 or SSAE16 reports **Criteria for "Yes" Response:** • The ability to meet resilience requirements is

		considered when selecting any supplier that supports the critical service. **Criteria for "Incomplete" Response:** • The ability to meet resilience requirements is considered when selecting some suppliers, or the practice appears otherwise incomplete.
	3. Does the acquirer identify suppliers from which it requires documented verification of their ability to meet the critical service's resilience requirements? [EXD:SG3.SP3]	**Question intent:** To determine if the acquirer identifies suppliers from which it requires documented verification of an ability to meet the resilience requirements of the critical service, before entering into formal agreements. This practice helps the acquirer to have more confidence in the relationships it forms with external entities. It is also a frequent feature of compliance and regulatory guidelines. The acquirer can use a number of means to verify that external entities can meet specific resilience requirements, for example • third-party audit • checklists • examination of specific artifacts, for example, their incident response or business continuity plans **Typical work products:** • SAS70 or SSAE-16 reports • list of supplier or supplier services for which the acquirer requires verification **Criteria for "Yes" Response:** • The acquirer identifies the need for documented verification of the supplier's ability to meet resilience requirements, and obtains this verification every time it contemplates entering into a formal agreement with a supplier to support the critical service. **Criteria for "Incomplete" Response:** • The acquirer inconsistently requires verification that suppliers can meet resilience requirements, or the acquirer's process is otherwise incomplete or ad hoc.
	4. Does the acquirer consider external entities' own external dependencies before entering into formal agreements to support the critical service? [EXD:SG3.SP3]	**Question intent:** To determine if the acquirer evaluates and considers the external dependencies of external entities with whom the acquirer is considering entering into formal agreements to support the critical service. This practice is important because managing external dependencies requires an understanding of the

		external entities that support the critical service. Failing to understanding the 'second tier', or how suppliers and infrastructure providers provide their support, can lead to missing important risks and problems. This practice is closely linked to managing the risks of single points of failure. Typical means to assess external entity dependency risk include • discussions with prospective suppliers • requests by the acquirer for lists of the external entity's sub-contractors who will be used to support the acquirer and efforts to identify risks associated with those subcontractors • contacting other firms or industry groups to gather information related to the external entity **Typical work products:** • internal correspondence concerning external dependencies • checklists that require an evaluation before entering into formal agreements • audit reports that include suppliers' external dependencies **Criteria for "Yes" Response:** • The acquirer collects information about and considers the external dependencies of suppliers and infrastructure providers before entering into formal agreements. **Criteria for "Incomplete" Response:** • The acquirer considers risks posed by external entity's dependencies with some external entities, or the process to conduct this activity appears otherwise incomplete.
	Goal 5 – Formal agreements include resilience requirements The purpose of this goal is to assess whether the acquirer includes appropriate requirements in formal agreements with suppliers.	Guidance
	1. Are resilience requirements for the critical service included in formal agreements with suppliers? [EXD:SG3.SP4]	**Question intent:** To determine if resilience requirements are included in formal agreements with suppliers. Including resilience requirements in formal agreements with suppliers that support critical

		services is an essential practice. Such requirements make it clear what suppliers are expected to do and the standards they are expected to meet. They also form the basis for other actions involving the formal agreement, for example, performance monitoring, detecting breach of the formal agreement, and termination if necessary. **Typical work products:** • formal agreement clauses • service level agreements • resilience requirements specification **Criteria for "Yes" response** • The acquirer includes resilience requirements in formal agreements with all suppliers that support the critical service. **Criteria for "Incomplete" Response:** • The acquirer includes resilience requirements in agreements with some external entities, or the practice appears otherwise incomplete.
	2. Do formal agreements require suppliers to manage their own external dependencies? [EXD:SG3.SP4, EXD:GG2.GP4]	**Question intent:** To determine if the acquirer includes terms in formal agreements that require suppliers to manage their external dependencies. Rarely do dependencies end with only the supplier with whom the acquirer is contracted. An external entity that fails to account for and manage its own external dependencies can represent an additional risk to the acquirer and critical service. An affirmative answer to this question does not require that a formal agreement state verbatim "The supplier agrees to manage its own external dependencies". Formal agreement terms may refer more generally to a requirement that the resilience requirements of the critical service also apply to subcontractors, or impose a duty on the supplier to include these terms in its own contracts. This practice is also sometimes referred to as including "flow-down" requirements in contracts. **Typical work products:** • Contract clauses that require suppliers to include similar requirements or clauses with their suppliers or sub-contractors **Criteria for "Yes" Response:** • The acquirer includes requirements in formal

		agreements with suppliers that the supplier will manage its own external dependencies to support the critical service. **Criteria for "Incomplete" Response:** • The acquirer includes requirements that some suppliers manage their own external dependencies, or the process to perform this practice is otherwise incomplete.
	3. Do formal agreements with suppliers include requirements to report incidents that affect the critical service? [EXD:SG3.SP4, IMC:GG2.GP4]	**Question intent:** To determine if agreements with suppliers require them to report incidents that may affect the critical service. Without a clear understanding that suppliers will report incidents that affect the critical service, the acquirer may incur additional risk or be simply unaware that the critical service has been disrupted or otherwise compromised. **Typical work products:** • clauses in formal agreements that require suppliers to report incidents to the acquirer **Criteria for "Yes" Response:** • All formal agreements with suppliers that support the critical service contain requirements for the suppliers to report incidents that may negatively affect the critical service. **Criteria for "Incomplete" Response:** • Some formal agreements with suppliers that support the critical service contain requirements for suppliers to report incidents that may negatively affect the critical service, or the practice appears otherwise incomplete.
	4. Do formal agreements require that suppliers manage vulnerabilities that may affect the critical service? [EXD:SG3.SP2, VAR:GG2.GP4]	**Question intent:** To determine if formal agreements include requirements for suppliers to manage vulnerabilities that affect the critical service. While vulnerabilities of suppliers represent potential risk to the acquirer, acquirers are typically constrained in their ability to manage vulnerabilities across arms-length agreements. The purpose of this practice is to ensure that suppliers accept responsibility to manage vulnerabilities as part of meeting the resilience requirements of the critical service. **Typical work products:** • Clauses in formal agreements that require the management of vulnerabilities

		Criteria for "Yes" Response: • Formal agreements with all suppliers supporting the critical service include a requirement to manage vulnerabilities that affect the critical service. **Criteria for "Incomplete" Response:** • Formal agreements with some suppliers include requirements to manage vulnerabilities, or the practice appears otherwise incomplete.
	5. Do formal agreements require suppliers that support the critical service to maintain disruption management plans (incident management, service continuity, etc.)? [IMC:GG2.GP4, SC:GG2.GP4]	**Question intent:** To determine if formal agreements with suppliers include requirements to maintain plans to manage disruption to the critical service. Typically these are incident management or service continuity plans as appropriate. This practice is important because it helps ensure that suppliers that support the critical service have adequate planning in place to protect and sustain the critical service. **Typical work products:** • contractor clauses or other language in formal agreements • provision of supplier incident and continuity planning information **Criteria for "Yes" Response:** • The acquirer has requirements or language in all agreements with suppliers that support the critical service to maintain service continuity or incident management plans, as appropriate, to protect and sustain the critical service. **Criteria for "Incomplete" Response:** • The acquirer has requirements or language in some agreements with relevant external entities to maintain disruption management plans, or the practice appears otherwise incomplete.
	6. Do formal agreements with suppliers that support the critical service require their participation in disruption management planning and exercising? [IMC:GG2.GP7, SC:GG2.GP4]	**Question intent:** To determine if agreements include requirements or language requiring participation in the acquirer's incident management and service continuity planning and maintenance activities. Writing and maintaining service continuity and incident management plans is particularly challenging when the critical service is supported by suppliers and other external entities. This is because the continuity of the critical service may depend on the actions of suppliers during a disruption, and because information that is necessary for planning purposes may reside

		with the external entity, rather than with the acquirer itself. Examples of supplier participation in disruption planning and exercising may include • engagement in the acquirer's incident management and service continuity plan development or maintenance processes • accountability for the provision/maintenance of supplier information, such as contact(s), technology, or facility details • provision of supplier incident management and continuity planning information • required input to the acquirer's incident and service continuity plan testing process **Typical work products:** • contractor clauses or other language in formal agreements **Criteria for "Yes" Response:** • The acquirer has language in all agreements with relevant suppliers requiring participation in the acquirer's incident and service continuity planning and exercising activities. **Criteria for "Incomplete" Response:** • The acquirer has language in some agreements with relevant suppliers requiring participation in the acquirer's incident management and service continuity planning activities, or the practice appears otherwise incomplete.
	Goal 6 – Technology asset supply chain risks are controlled. The purpose of this goal is to assess whether the acquirer institutes controls over the risks posed by deploying technology internally. These risks may include, for example, counterfeit or maliciously tainted technology.	**Guidance**
	1. Does the acquirer have a process to identify and document the resilience requirements for technology assets that support the critical service? [TM:SG2.SP1]	**Question intent:** To determine if the acquirer has a process to document the resilience requirements for its own technology assets that support the critical service. This practice – to document requirements for technology that supports the critical service — is important because having documented requirements

		forms the basis for other activities, such as selecting trusted vendors and acceptance testing (if appropriate). Having an established process means that • There are specific steps or activities that acquirer staff must complete. • The process is supported by appropriate documentation. For example, there may be a documented schedule of meetings to identify requirements. • The acquirer's staff is aware that the process exists and that they are expected to follow it. **Typical work products:** • documented resilience requirements for the technology that supports the critical service • internal correspondence **Criteria for "Yes" Response:** • The acquirer has a process to identify and document requirements for all technology that supports the critical service. **Criteria for "Incomplete" Response:** • The acquirer's process identifies and documents resilience requirements for some technology that supports the critical service, or the process appears otherwise incomplete.
	2. Does the acquirer evaluate technology assets that support the critical service for vulnerabilities before they are acquired? [VAR:SG2.SP2]	**Question intent:** To determine if the acquirer has a process to evaluate technology assets for vulnerabilities prior to completing the acquisition of these assets. This practice is important because it helps the acquirer obtain technology that is more likely to satisfy the requirements and importance of the critical service. An affirmative answer to this question requires that the acquirer has some process or have assigned responsibility to staff to become aware of vulnerabilities to technology that the acquirer intends to purchase to support the critical service. In practice, the acquirer's ability to gather effective, complete vulnerability information may vary substantially depending on the specific technology item. Some ways that the acquirer can evaluate technology vulnerabilities before acquisition include • incorporating vulnerability-reporting requirements in

		formal technology purchase agreements • participating in ICS-CERT or other organizations to become aware of vulnerabilities • reviewing system configurations for potential vulnerabilities • communicating with peer acquirers that also use particular external entities • researching vulnerability information in publicly available databases and sources **Typical work products:** • vulnerability reports • assignment of responsibility in job descriptions • internal correspondence **Criteria for "Yes" Response:** • The acquirer evaluates all technology assets to support the critical service for vulnerabilities before acquiring and deploying these assets internally. **Criteria for "Incomplete" Response:** • The acquirer evaluates some technology assets for vulnerabilities before acquiring them, or this practice appears otherwise incomplete.
	3. Has the acquirer identified the criteria or standards required for technology vendors to be considered trusted? [EXD:SG3.SP1]	**Question intent:** To determine if the acquirer has criteria that are used to designate technology suppliers as "trusted". Acquirers can manage and reduce risks from integrity problems with hardware and software by only purchasing technology to support the critical service from trusted vendors. A basic practice is for acquirers to have documented criteria for vendors to be considered trusted. These criteria often involve compliance with standards set forth by an acknowledged authority. Examples include • The vendor has been selected as an authorized distributor by the OEM manufacturer. • The vendor may meet established standards set out by an industry organization (for example, The Open Group Trusted Technology Provider or similar standard). **Typical work products:** • list of criteria or standards **Criteria for "Yes" Response:** • The acquirer has documented standards that

		describe when a technology provider is "trusted" for the purpose of providing technology to support the critical service. **Criteria for "Incomplete" Response:** • The acquirer has partially documented criteria, or these criteria apply only to some types of technology, or this practice appears otherwise incomplete.
	4. Has the acquirer identified trusted suppliers from which it obtains technology assets that support the critical service? [TM:SG3.SP2, TM:GG2.GP2]	**Question intent:** To determine if the acquirer has identified technology suppliers who are designated as "trusted" from which it acquires technology assets to support the critical service. Using trusted suppliers for technology assets that support the critical service cannot provide complete assurance against counterfeits, malicious tampering, or similar threats. However, this is a basic control against this specific risk. **Typical work products:** • list of trusted suppliers or technology vendors **Criteria for "Yes" Response:** • The acquirer has a documented list of technology vendors who are designated as "trusted", from which it purchases technology that supports the critical service. **Criteria for "Incomplete" Response:** • The acquirer has a partially documented list of trusted suppliers, or the list exists but is used inconsistently, or this practice appears otherwise incomplete.
	5. Does the acquirer formally evaluate the need to conduct acceptance testing for technology assets that support the critical service and conduct such testing (if appropriate)? [TM:SG2.SP2]	**Question intent:** To determine if the acquirer has a process to consider and perform acceptance testing of technology assets before deployment to ensure that the assets meet the critical service's resilience requirements. In some cases acceptance testing can be expensive and beyond the capability of many organizations. Therefore, an affirmative answer to this question does not require that testing is done in all cases. Instead, this practice asks if the acquirer has a decision making process to evaluate the need for this control, and whether it conducts acceptance testing if appropriate. Acceptance testing involves verifying that acquired technology meets the acquirer's resilience

		requirements for the critical service, for example confidentiality, integrity, availability, and maintainability, as well as other requirements that support the critical service. For example, acceptance testing may be used to verify that • the technology has the necessary functionality or features, or • the technology is not counterfeit, or • the technology has not been maliciously tainted or tampered with **Typical work products:** • documented resilience requirements for acquired technologies • acceptance testing results or reports • criteria that are used to determine which technology assets should undergo acceptance testing • procedures and/or standards for acceptance testing of acquired technology **Criteria for "Yes" Response:** • The acquirer has a process to identify acquired technology assets which should undergo acceptance testing prior to deployment, and it conducts the appropriate testing. **Criteria for "Incomplete" Response:** • The acquirer conducts some acceptance testing of technology assets but does so inconsistently, or the acquirer has identified technology that should be subject to acceptance testing but does not conduct the testing, or the practice otherwise appears incomplete.

2 Relationship Management and Governance

The purpose of Relationship Management and Governance is to assess whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk. This includes identifying the external entities that support the critical service, ongoing risk management, communicating with external entities about key aspects of protecting the critical service, and controlling external entities' access to the acquirer.

	Goal 1 – External dependencies are identified and prioritized. The purpose of this goal is to assess whether the acquirer identifies the external entities that it depends on to support the critical service and prioritizes them in order to make decisions about managing these dependencies.	Guidance
	1. Are dependencies on external entities that are critical to the service(s) identified? [EXD:SG1.SP1 Suppliers Infrastructure providers Governmental services	**Question intent:** To determine if external dependencies that are critical to the service are identified. An external dependency exists when an external entity has: • access to • control of • ownership in • possession of • responsibility for or • other defined obligations related to the critical service or its associated assets Examples of services provided to an acquirer by external entities include: • outsourced activities that support operation or maintenance of the critical service • security operations, IT service delivery and operations management, or services that directly affect resilience processes • backup and recovery of data, provision of backup facilities for operations and processing, and provision of support technology • infrastructure providers such as power • telecommunications (telephony and data) • governmental services such as fire and police support, emergency medical services, and emergency

		management services **Typical work products:** • list of external dependencies and entities **Criteria for "Yes" Response:** • The acquirer has documented all external dependencies that support the critical service in each category. **Criteria for "Incomplete" Response:** • The acquirer has documented some of the external dependencies that support the critical service in each category, or the practice appears otherwise incomplete.
	2. Are external dependencies prioritized? [EXD:SG1.SP2]	**Question intent:** To determine if external dependencies are prioritized. Prioritization is important to ensure that the acquirer properly directs its resources to managing the external dependencies that most directly impact the critical service. Prioritization criteria may include dependencies that: • directly affect the operation and delivery of the critical service • support, maintain, or have custodial care of critical service assets • support the continuity of operations of the critical service • have access to highly sensitive or classified information • support more than one critical service in the acquirer enterprise • supply assets that support the critical service • impact the recovery time objective of the critical service **Typical work products:** • documented criteria for prioritizing external dependencies • prioritized list of external dependencies **Criteria for "Yes" Response:** • The acquirer has a current prioritization – a list or other documented indication of priority - for all external dependencies that affect the critical service.

		Criteria for "Incomplete" Response: • The acquirer has a prioritization that includes some external dependencies, or this practice appears otherwise incomplete
	3. Has a process been established for maintaining a list of external dependencies and related information? [EXD:SG1.SP1]	**Question intent:** To determine if a process has been established for creating and maintaining the list of external dependencies and related information. The acquirer's external dependencies will change over time as a result of changes to relationships with suppliers and customers, changes in services, the lifecycle of assets, and other factors. Once the list of external dependencies is established, it is important that it be maintained and updated. The list should include information that is relevant to managing the dependency, for example point of contact information and the acquirer services supported. Having an established process means that • There are specific steps or activities that acquirer staff must complete. • The process is supported by appropriate documentation. For example, there may be a documented schedule of meetings to updates information. The acquirer's staff is aware that the process exists and that they are expected to follow it. **Typical work products:** • list of external dependencies • assignment of responsibility in job descriptions • documented standards for reviewing the list • edits and changes to the list • reports from centralized information management tools **Criteria for "Yes" Response:** • The acquirer has established a process for maintaining the list of external dependencies that support the critical service, and the information relevant to managing these dependencies. **Criteria for "Incomplete" Response:** • The acquirer is developing the process, or the process exists but there is no documentation, or the practice appears otherwise incomplete.

	Goal 2 – Supplier risk management is continuous. The purpose of this goal is to assess whether the acquirer continuously manages the risks of relying on suppliers to support the critical service.	Guidance
	1. Does the acquirer periodically review and update resilience requirements for suppliers? [RRM:SG1.SP3]	**Question intent:** To determine if the acquirer periodically reviews and updates resilience requirements for suppliers. Periodically means that a specific period for the activity has been identified and documented by the acquirer. **Typical work products:** • internal policy or command media documenting activity and period • recurring meetings • internal correspondence **Criteria for "Yes" Response:** • The acquirer periodically reviews and updates the resilience requirements that apply to all suppliers. **Criteria for "Incomplete" Response:** • The acquirer reviews and updates the resilience requirements for some suppliers, or the review is done inconsistently, or the practice otherwise appears incomplete.
	2. Does the acquirer periodically review risks due to suppliers? [EXD:SG2.SP1]	**Question intent:** To determine if the acquirer periodically reviews risks due to suppliers as part of its risk management processes. Periodically means that a specific period for the activity has been identified and documented by the acquirer. A key component of external dependencies management is active, ongoing risk management. This includes ongoing risk monitoring, assessments, and decision making. **Typical work products:** • internal correspondence • current risk register or other risk tracking tool **Criteria for 'Yes" Response:** • The acquirer periodically reviews risks due to all suppliers that support the critical service. **Criteria for "Incomplete" Response:**

		• The acquirer reviews risks related to suppliers occasionally, but not according to any documented period or schedule, or risks due to some suppliers are reviewed, or the practice appears otherwise incomplete.
	3. Does the acquirer periodically discuss and review risks to the critical service with suppliers? [EXD:GG2.GP7, RISK:GG2.GP8]	**Question intent:** To determine if the acquirer exchanges risk information with suppliers that support the critical service. Much of the information needed to accurately evaluate and manage the risks of depending on external entities may be held or known by the external entities themselves, rather than the acquirer. By discussing risks to the critical service with relevant suppliers and adjusting risk assessments as needed, the acquirer can help to ensure that risk management decisions are based on all of the pertinent information. In addition, the exchange of information can help ensure that suppliers themselves are managing risks based on correct information. Periodically means that the acquirer has assigned a documented time interval that governs the execution of the practice. **Typical work products:** • correspondence • meeting notes • internal correspondence or command media listing a review period **Criteria for "Yes" Response::** • The acquirer reviews risks to the critical service with all of the relevant suppliers that support the service based on a documented period. **Criteria for "Incomplete" Response:** • The acquirer reviews risks to the critical service with some of the relevant suppliers, or the reviews occur inconsistently, or the practice appears otherwise incomplete.
	4. Does the acquirer conduct periodic reviews with suppliers to verify that vulnerabilities relevant to the critical service are continuously managed? [VAR:GG2.GP7, VAR:GG2.GP8]	**Question intent:** To determine if the acquirer conducts periodic reviews with suppliers to verify that vulnerabilities relevant to the critical service are continuously managed. Managing vulnerabilities is a very important part of ensuring the resilience of critical services. Vulnerability management is complicated by supplier relationships, where the assets used to support the critical service are

		under the direct control of an external entity. The purpose of this practice is to ensure that suppliers who support the critical service are managing vulnerabilities that may affect the critical service. **Typical work products:** • supplier reports • service review reports • internal correspondence or command media listing a review period **Criteria for "Yes" Response:** • The acquirer conducts reviews with suppliers according to a documented period to ensure that the relevant suppliers are managing vulnerabilities that may affect the critical service. **Criteria for "Incomplete" Response:** • The acquirer conducts reviews with some suppliers, or the reviews are conducted inconsistently, or the practice appears otherwise incomplete.
	5. Does the acquirer's risk monitoring include critical service resilience requirements not codified in supplier agreements? [RISK:SG5.SP2]	**Question intent:** To determine if the acquirer monitors resilience requirements not codified in formal agreements with suppliers as ongoing risks. The critical service's resilience requirements may not be codified in formal agreements with suppliers for a variety of reasons. For example, the requirements may have changed or the acquirer may have insufficient negotiating power to compel suppliers to agree to all of the relevant requirements. For business reasons acquirers will often accept this risk. However, the acquirer ultimately owns the risk of failures of the critical service. Therefore, any time a supplier agrees to support the critical service without sufficient protections and controls, this situation should be monitored as an open risk. **Typical work products:** • list of requirements not included in agreements • risk register or other documented list of outstanding risks **Criteria for "Yes" Response:** • The acquirer documents and monitors as risks all resilience requirements not codified in formal agreements. **Criteria for "Incomplete" Response:** • The acquirer monitors some requirements not codified

		in agreements as risks, or the practice appears otherwise incomplete.
	6. Does the acquirer's risk monitoring include supplier performance issues and concerns? [RISK:SG5.SP2]	**Question intent:** To determine if the acquirer monitors supplier performance problems as outstanding risks. Failures of suppliers to support the resilience requirements of the critical service have the potential to create risks and disruptions. For that reason the acquirer should document and monitor these performance problems as part of its ongoing risk monitoring. Examples of supplier performance issues and concerns: • incidents affecting the critical service • process failures, for example failing to notify the acquirer of changes affecting the critical service • non-responsiveness to inquiries • non-available services **Typical work products:** • risk registers or other documented lists of outstanding risks • internal correspondence **Criteria for "Yes" Response:** • The acquirer includes performance problems and failures of suppliers to support resilience requirements as part of its documented, ongoing risk monitoring. **Criteria for "Incomplete" Response:** • The acquirer includes some supplier performance problems as part of its risk monitoring, or the practice appears otherwise incomplete.
	Goal 3 – Supplier performance is governed and managed. The purpose of this goal is to assess whether the acquirer manages the performance of suppliers in supporting the resilience of the critical service.	Guidance
	1. Does the acquirer monitor the performance of suppliers against resilience requirements? [EXD:SG4.SP1]	**Question intent:** To determine if the performance of suppliers is monitored against the resilience requirements of the critical service. The performance of suppliers should be monitored against the requirements of the critical service so that

		corrective actions can be taken as needed. Examples of supplier performance areas for monitoring: • timeliness of change notifications • responsiveness and participation in service continuity testing • availability of key services **Typical work products:** • internal correspondence • documented responsibilities in job descriptions • notes from service review meetings **Criteria for "Yes" Response:** • The acquirer monitors the performance of suppliers against the documented resilience requirements for the critical service. **Criteria for "Incomplete" Response:** • The acquirer monitors the performance of some suppliers that support the critical service, or the practice appears otherwise incomplete.
	2. Are issues with supplier performance documented and reported to appropriate stakeholders? [EXD:GG2.GP7]	**Question intent:** To determine if supplier performance issues (relevant to resilience requirements) are documented and reported to appropriate stakeholders. Stakeholders should be advised of performance issues so that they can use this information to help manage external dependencies. Typical stakeholders include • Risk managers • Procurement and vendor selection staff • Business or critical service owner **Typical work products:** • performance documentation • internal correspondence **Criteria for "Yes" Response:** • The acquirer documents and reports supplier performance issues to appropriate stakeholders. **Criteria for "Incomplete" Response:** • The acquirer reports performance issues involving some suppliers to stakeholders, or it only reports issues to some stakeholders, or the practice appears otherwise incomplete.

	3. Does the acquirer take corrective actions as necessary to address issues with supplier performance? [EXD:SG4.SP2]	**Question intent:** To determine if corrective actions are taken to address issues with supplier performance as it relates to resilience requirements. The intent of any corrective action is to minimize disruption to the critical service. **Typical work products:** • corrective action reports or documentation • supplier correspondence documenting corrective actions **Criteria for "Yes" Response:** • The acquirer takes corrective actions to address performance issues for every supplier that supports the critical service. **Criteria for "Incomplete" Response:** • The acquirer takes corrective actions to address performance issues for some suppliers that support the critical service, or the practice appears otherwise incomplete.
	4. Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]	**Question intent:** To evaluate if corrective actions are evaluated to ensure they are effective. **Typical work products:** • internal correspondence • service review reports **Criteria for "Yes" Response::** • The acquirer evaluates the corrective actions taken with all suppliers to ensure that issues are resolved. **Criteria for "Incomplete" Response::** • The acquirer evaluates corrective actions taken with some suppliers, it evaluates corrective actions inconsistently, or the practice appears otherwise incomplete.

	Goal 4 – Change and capacity management are applied to external dependencies. The purpose of this goal is to assess whether the acquirer coordinates change and capacity management with external entities that support the critical service.	Guidance
	1. Does the acquirer have a change management process to manage modifications to its own assets that support the critical service? [ADM:SG3.SP2] Information Technology Facilities People	**Question intent:** To determine if a change management process is used to manage modifications to assets that support the critical service. Change management is important in order to maintain assets in a condition that supports the resilience requirements of the critical service, and to avoid disruptions resulting from changes that were not foreseen or accounted for. A change management process typically addresses changes such as: • configuration changes (technology) • software and hardware changes • changes to the asset, including ownership, custodianship, and location • addition or elimination of assets • addition or elimination of controls **Typical work products:** • change requests • change implementation plan • blackout plan • change and configuration management board meeting minutes • change approvals • change tracking and status • change documentation, including test results **Criteria for "Yes" Response:** • A change management process is used to control changes to all assets in each category. **Criteria for "Incomplete" Response:** • A change management process is used to control changes to some assets in each category. **Additional guidance** Having an established process means that • There are specific steps or activities that acquirer staff must complete. • The process is supported by appropriate

		documentation. For example, there may be a documented list of internal staff that must be informed of certain changes. • The acquirer's staff is aware that the process exists and that they are expected to follow it.
	2. Are changes to assets that support the critical service (whether located at the acquirer or at suppliers) coordinated between the acquirer and suppliers? [ADM:GG2.GP7] Information Technology Facilities People	**Question intent:** To determine whether the acquirer and suppliers jointly manage changes to assets that support the critical service. Suppliers often own or have direct control of the assets that support the critical service. In other cases, the acquirer may own the assets but a supplier may have defined obligations affecting the assets (for example, maintenance agreements or other support obligations). Therefore, it is very important that the acquirer and relevant suppliers jointly coordinate changes to assets that support the critical service, as needed. **Typical work products:** • clauses in formal agreements that govern change management • integrated change documentation • notes from cross-organization participation in change and configuration management board meetings **Criteria for "Yes" Response:** • For each relevant supplier, a process is implemented that ensures the acquirer and supplier coordinate changes to assets that support the critical service. **Criteria for "Incomplete" Response:** • For some suppliers a process is implemented to coordinate changes, or the coordination of changes is inconsistent, or the practice is otherwise incomplete. **Additional guidance** Change procedures should ideally be part of a formal agreement that is established with a supplier. Defining and communicating change procedures ensures that changes to assets will be handled in a controlled manner, consistent with acquirer policy, standards, and guidelines. Examples of changes that may require joint coordination: • configuration (technology, software, information) • access rights • permissions

		• geographical location (people, technology, facilities) • protocols (technology) • software updates • process changes
	3. Is there a process to monitor contract renegotiations, updates, addendums, and similar changes to identify and manage any impacts to the critical service? [EXD:SG3.SP4]	**Question intent:** To determine if changes to formal agreements with suppliers are monitored for potential impacts to the critical service. Because relationships with suppliers are typically governed by formal agreements, it is important that the acquirer is aware of potential impacts to the critical service of changes to these agreements. Some examples of changes that may affect the resilience of critical services include: • additional or fewer requirements • changes in the contract remedies available • the addition or elimination of services provided • modifications to technology or communications Having an established process means that • There are specific steps or activities that acquirer staff must complete. • The process is supported by appropriate documentation. For example, there may be a documented list of formal agreement changes that are relevant to the process. • The acquirer's staff is aware that the process exists and that they are expected to follow it. **Typical work products:** • documented responsibilities in job descriptions • internal checklists • internal correspondence **Criteria for "Yes" Response:** • The acquirer monitors changes to formal agreements with suppliers to identify and manage impacts to the critical service. **Criteria for "Incomplete" Response:** • The acquirer monitors changes to some formal agreements, or it monitors these changes inconsistently, or the practice appears otherwise incomplete.

	4. Does the acquirer monitor for organizational changes at external entities - for example buy-outs, financial problems, political or civil problems - that may affect the critical service? [MON:SG1.SP1]	**Question intent:** To determine if the acquirer monitors for organizational changes at suppliers for potential impacts to the critical service. Some examples of changes that may affect the critical service include: • changes to supplier financial stability • changes in political stability in regions where facilities are located • changes to staffing which may affect the quality of services • changes in the composition of the supplier's subcontractors or 'second-tier' suppliers • impending regulatory or compliance requirements that may affect the supplier's support to the acquirer **Typical work products:** • list of types of changes (financial, organizational) to be monitored • contracts with suppliers to provide business intelligence about the acquirer's supply chain • lists of information sources **Criteria for "Yes" Response:** • The acquirer monitors all suppliers for organizational changes that may impact the critical service. **Criteria for "Incomplete" Response:** • The acquirer monitors some suppliers for changes, or it monitors inconsistently, or the process otherwise appears incomplete.
	5. Does the acquirer manage the capacity of services and assets cooperatively with suppliers? [TM:SG5.SP3]	**Question intent:** To determine whether the acquirer and the suppliers that support the critical service jointly manage the capacity of the critical service and key assets that support it. When external entities support the critical service, the capacity of assets owned or managed by suppliers can affect the availability of the critical service. Therefore the acquirer should clearly define how it and the relevant suppliers will cooperatively manage the capacity of the critical service and supporting assets. **Typical work products:** • contract and formal agreement clauses concerning capacity management • meeting notes • memoranda of understanding **Criteria for "Yes" Response:**

		• For each supplier that supports the critical service, a process is implemented where the acquirer and the external entity cooperatively manage the capacity of the critical service and key assets. **Criteria for "Incomplete" Response:** • For some suppliers a process is implemented where capacity is jointly managed, or the practice appears otherwise incomplete.
	Goal 5 – Supplier transitions are managed The purpose of this goal is to assess whether the acquirer manages transitions of supplier formal agreements.	**Guidance**
	1. Has the acquirer identified criteria or conditions that would cause it to terminate supplier formal agreements? [EXD:SG4.SP2]	**Question intent:** To determine if the acquirer has documented criteria that would trigger the termination of formal agreements with suppliers that support the critical service. Transition - or exit - planning is an important part of managing dependencies on suppliers. Some examples of criteria that may cause the acquirer to terminate agreements include: • poor performance • strategic changes in the service supported • cost • in-sourcing Note: formal agreements or contracts typically contain clauses that describe the right to terminate the agreement. This question asks about a separate management practice: to identify what would trigger the acquirer to exercise its rights under the relevant contracts. By itself, the existence of a formal agreement does not satisfy this practice. **Typical work products:** • documented criteria **Criteria for "Yes" Response:** • The acquirer has identified criteria that would cause it to terminate formal agreements with each of the relevant suppliers that support the critical service. **Criteria for "Incomplete" Response:** • The acquirer has identified criteria that would cause it to terminate formal agreements with some suppliers, or the practice is otherwise incomplete.

	2. Has the acquirer planned the actions it will take to sustain the critical service if one or more supplier formal agreements are terminated (by either the acquirer or supplier)? [EXD:GG2.GP1]	**Question intent:** To determine if the acquirer has planned for the potential termination of agreements with one or more suppliers. These terminations may be driven by the acquirer, by the supplier, or by circumstances out of either party's control. For key suppliers which provide unique and essential services, the decision to transition to another sourcing strategy may require long lead times and careful planning to manage the risk. Lacking a plan for how to manage this transition could lead to significant impacts to the critical service(s). Examples of planning measures and mitigations: • maintaining contingency contracts with alternate suppliers • maintaining an in-house capability • identifying alternate suppliers • planning communciations and customer strategies to facilitate transition **Typical work products:** • a documented plan or set of steps that the acquirer will execute in the event supplier agreements are terminated **Criteria for "Yes" Response:** • The acquirer has planned and documented how it will manage supplier transitions in the event that formal agreements with suppliers are terminated. **Criteria for "Incomplete" Response:** • The acquirer has partially completed transition planning, or the planning only applies to some suppliers, or the practice appears otherwise incomplete.
	3. Does the acquirer use lessons learned from supplier transitions to refine its external dependency management processes? [EXD:GG3.GP2]	**Question intent:** To determine if the acquirer incorporates lessons learned from supplier transitions into its external dependencies management processes, particularly forming relationships with suppliers and managing performance. Learning from supplier transitions can help the acquirer to improve its external dependencies management processes and avoid similar problems in the future. **Typical work products:** • internal correspondence • checklists which require lessons learned to be

		identified and communicated upon termination of agreements **Criteria for "Yes" Response:** • The acquirer has a process so that lessons learned from supplier transitions are communicated to stakeholders to refine external dependencies management. **Criteria for "Incomplete" Response:** • The acquirer communicates lessons learned to some stakeholders, or it uses lessons learned from supplier transitions inconsistently, or the practice appears otherwise incomplete.
	Goal 6 – The acquirer manages the risks of infrastructure and governmental dependencies. The purpose of this goal is to assess whether the acquirer identifies and continuously manages the risks of dependence on infrastructure providers and governmental services.	**Guidance**
	1. Does the acquirer have a process to periodically review and update resilience requirements for infrastructure providers that support the critical service? [EXD:SG3.SP2]	**Question intent:** To determine if the acquirer has a process to periodically review and update resilience requirements for infrastructure providers that support the critical service. The acquirer's dependence on infrastructure providers may change in scope and importance based on business and service considerations, or on factors outside the acquirer's control. Therefore it is important that the acquirer has a process to periodically review and update resilience requirements for infrastructure providers. Periodically means that the acquirer has a documented time interval for the activity. Having an established process means that • There are specific steps or activities that acquirer staff must complete. • The process is supported by appropriate documentation. For example, there may be a documented schedule of meetings to identify requirements. • The acquirer's staff is aware that the process exists and that they are expected to follow it.

		Typical work products: • internal policy or command media documenting activity and period • notes from recurring meetings • internal correspondence • staff job descriptions assigning responsibility **Criteria for "Yes" Response:** • The acquirer periodically reviews and updates the resilience requirements for all infrastructure providers that support the critical service. **Criteria for "Incomplete" Response:** • The acquirer reviews and updates the resilience requirements for some infrastructure providers, or it reviews requirements inconsistently, or the practice appears otherwise incomplete.
	2. Has responsibility been assigned for monitoring the performance of infrastructure providers that support the critical service? [EXD:SG4.SP1]	**Question intent:** To determine if responsibility for monitoring the performance of infrastructure providers that support the critical service has been assigned. Assigning responsibility ensures that monitoring is performed on a timely and consistent basis. The acquirer should assign responsibility for monitoring the performance of each infrastructure provider that supports the critical service. The responsible staff should establish procedures that determine the frequency, protocol, and responsibility for monitoring the performance of a provider. **Typical work products:** • internal correspondence • assignment in staff job descriptions **Criteria for "Yes" Response:** • Responsibility for monitoring the performance of each infrastructure provider that supports the critical service has been assigned. **Criteria for "Incomplete" Response:** • Responsibility for monitoring the performance of some infrastructure providers has been assigned, or the practice appears otherwise incomplete.

	3. Has responsibility been assigned for managing relationships with the providers of governmental services that support the critical service? [EXD:SG4.SP1, EXD:GG2.SP7]	**Question intent:** To determine if the acquirer has assigned responsibility for managing relationships with governmental service providers (agencies, departments, etc.) that support the critical service. Governmental services may support the critical service in a variety of ways, for example: fire and police services, maintenance and operation of transportation networks, or cyber threat information sharing. Examples of managing governmental service relationships include: • Managing and coordinating emergency preparedness exercises with local and state authorities • Exchanging information and being aware of transportation system closures • Liaising with federal law enforcement agencies • Being aware of local or regional events that may impact staff availability **Typical work products:** • internal correspondence • assignment of responsibility in staff job descriptions **Criteria for "Yes" Response:** • The acquirer has assigned responsibility for managing relationships with all of the governmental service providers that support the critical service **Criteria for "Incomplete" Response:** • The acquirer has assigned responsibility for managing relationships with some governmental service providers, the assignment of responsibility is not clear, or the practice appears otherwise incomplete.
	4. Are performance (or other) issues involving infrastructure providers and governmental services communicated to stakeholders for use in managing the dependency? [EXD:GG2.GP7]	**Question intent:** To determine if relevant stakeholders in the acquirer are alerted to issues or risks involving infrastructure and governmental services providers. When performance problems or other issues are identified at infrastructure and governmental services providers, key stakeholders in the acquirer should be alerted so that they can take required actions to manage any resulting risks. Specific stakeholders may range from operations personnel, including, for example, managers who may need to be informed about preparedness exercises or infrastructure interruptions, to executives who may need to interface with government leaders to resolve issues. Stakeholders should understand their roles and responsibilities in external dependencies management

		activities. **Typical work products:** • internal correspondence • documented list of stakeholders to inform **Criteria for "Yes" Response:** • The acquirer escalates issues involving infrastructure providers and governmental services to relevant internal stakeholders to manage any resulting risks. **Criteria for "Incomplete" Response:** • The acquirer escalates issues involving some infrastructure providers or governmental service providers, or it elevates issues to some stakeholders, or the practice appears otherwise incomplete.
	5. Does the acquirer's risk monitoring include performance (or other) issues involving infrastructure providers and government services? [RISK:SG5.SP2]	**Question intent:** To determine if the acquirer's risk management processes include the monitoring of infrastructure and governmental service issues. Performance problems involving infrastructure and governmental services providers (as related to resilience requirements) have the potential to create risks and disruptions to the critical service. For that reason the acquirer's risk management processes should include the monitoring of performance problems or other issues involving infrastructure and governmental services **Typical work products:** • internal correspondence communicating problems and issues • risk registers and other lists of outstanding risks **Criteria for "Yes" Response:** • The acquirer includes monitoring of infrastructure performance issues and governmental service issues as part of its ongoing risk monitoring and risk management. **Criteria for "Incomplete" Response:** • The acquirer includes some performance issues as part of its risk monitoring, or the practice appears otherwise incomplete.

	Goal 7 – External entity access to acquirer assets is managed. The purpose of this goal is to assess whether the acquirer manages access by external entities to acquirer assets that support the critical service. This includes both physical and logical access to the acquirer.	Guidance
	1. Are both local and remote access to acquirer assets that support the critical service granted based on the assets' protection requirements? [AM:SG1.SP1]	**Question intent:** To determine if access to acquirer assets that support the critical service is granted based on the requirements of the critical service. This question asks about access granted to both internal staff and to any external entity (i.e.: not only external entities that actually support the critical service). Access includes both internal and external (aka remote) access. Remote access may be conducted by internal staff or by external entities/suppliers. Access should be granted in accordance with the justification for the request and the protection requirements that have been established for the asset. Normally, asset owners are responsible for reviewing the request, justification, and protection requirements to decide whether to approve or deny access. The access provided should be commensurate to and not exceed the requestor's job responsibilities (least privilege principle). **Typical work products:** • access control lists and matrices (information and technology) • facility access rosters • access control logs or audit reports **Criteria for "Yes" Response:** • The acquirer has identified the protection requirements for assets that support the critical service and uses them as the basis to grant or deny access privileges to assets. **Criteria for "Incomplete" Response:** • The acquirer has identified the protection requirements for some assets, or it evaluates some access requests based on requirements, or the practice appears otherwise incomplete.

	2. Does the acquirer have a process to assess whether it appropriately modifies access privileges when an external entity has personnel changes such as terminations, promotions, or job changes? [AM:SG1.SP2]	**Question intent:** To determine if the acquirer has a process that ensures access privileges granted to external entities are adjusted when the external entity has personnel changes. One of the most important access management processes is the "move-adds-changes" (MAC) process for staff. This includes both logical access to information/systems and physical access to facility assets. Without a process and controls, access management can quickly deteriorate and risks can increase significantly. These processes can be even more complicated when staff at an external entity has access to acquirer assets. A key aspect of the MAC process is to ensure linkages are in place between relationship managers, the acquirer's relevant staff, and the staff responsible for personnel management at the external entity. **Typical work products:** • formal agreement clauses that describe the process and require adherence • internal correspondence • access control logs or audit reports **Criteria for "Yes" Response:** • The acquirer has established a process to appropriately manage changes to access privileges granted to external entity staff to acquirer assets that support the critical service. **Criteria for "Incomplete" Response:** • The acquirer has established a process to manage some changes to external entity staff access privileges, or it has instituted this process with some external entities, or the practice appears otherwise incomplete. **Additional guidance** Having an established process means that • There are specific steps or activities that acquirer staff must complete. • The process is supported by appropriate documentation. For example, there may be a documented list of relevant points of contact at suppliers. • The acquirer's staff is aware that the process exists and that they are expected to follow it.
	3. Does the acquirer periodically review	**Question intent:** To determine if the acquirer

	external entity access privileges – granted to external entity personnel or systems – to identify and correct inappropriate access privileges to acquirer assets? [AM:SG1.SP3] Information Technology Facilities	periodically reviews access privileges granted to **any** external entity, to identify inappropriate access privileges. Periodically means the acquirer has a documented time internal that governs execution of the activity. Access privileges include those granted to either external entity personnel or systems. Managing changes to access privileges granted to external entities is an ongoing activity. Excessive access privileges – granted either to internal staff or external entities - are a common factor contributing to breaches or other disruptions, breakdowns to change management, and non-compliance for firms in regulated industries. **Typical work products:** • internal policy or memoranda documenting period • internal correspondence correcting excessive privileges • changes to lists, access matrices (technology and information), and rosters • access control logs or audit reports **Criteria for "Yes" Response:** • The acquirer periodically reviews access privileges granted to all external entities, to acquirer assets in each category, to identify and correct inappropriate privileges. **Criteria for "Incomplete" Response:** • The acquirer has established a process to identify and correct inappropriate privileges granted to some entities to access acquirer assets, or it reviews access privileges inconsistently, or it only reviews access to some assets in each category, or the process appears otherwise incomplete.

	4. Does the acquirer identify inappropriate access attempts (for example by periodically reviewing access logs) by external entity personnel or systems to acquirer assets? [IMC:SG2.SP1] Information Technology Facilities	**Question intent:** To determine if the acquirer identifies inappropriate access attempts originating from external entities. Monitoring of access activity can alert the acquirer to potential attempts to inappropriately access information, conduct probing or reconnaissance activity in acquirer networks, or otherwise disrupt the critical service. This question asks about inappropriate access attempts made on the acquirer's information, technology, and facilities that support the critical service. Techniques to identify inappropriate access range from log analysis to other solutions, for example SIEM (Security Incident and Event Management) systems. Depending on the technique used, activities to identify inappropriate access should be periodic, for example log analysis should be conducted based on a documented time interval to be a complete practice. **Typical work products:** • incident management plan that defines these occurrences as an incident • reports • SIEM alerts • log file analysis **Criteria for "Yes" Response:** • The acquirer has a process to identify inappropriate access attempts by external entities to the acquirer's assets, in each of the three asset types. **Criteria for "Incomplete" Response:** • The acquirer identifies inappropriate access attempts originating at some external entities, it conducts this activity to protect some assets in each category, or the practice appears otherwise incomplete.

Relationship Management and Governance – Other Observations

3 Service Protection and Sustainment

The purpose of the Service Protection and Sustainment Domain is to assess whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats. This includes integrating external entity considerations into the acquirer's activities to manage disruptions – typically incident management and service continuity, validating controls at external entities, and maintaining situational awareness activities directed at external dependencies.

	Goal 1 – Disruption planning includes external dependencies. The purpose of this goal is to assess whether the acquirer accounts for external dependencies as part of its incident management and service continuity processes.	
	1. Does the acquirer have an incident management plan to protect the critical service? [IMC SG1.SP1]	**Question intent**: To determine if the acquirer has an incident management plan to protect the critical service. The purpose of incident management is to establish processes to identify and analyze events, detect incidents, and determine an organizational response. Incident management is a core resilience activity to protect and sustain critical services. The incident management plan should address at a minimum • a plan for managing incidents, including the owner, escalation plan, and scope • the structure of the incident management process • the requirements and objectives of the incident management process • a description of how the acquirer will identify incidents, analyze them, and respond to them **Typical work products:** • documented incident management plan **Criteria for "Yes" Response:** • The acquirer has a documented incident management plan to protect the critical service.

		Criteria for "Incomplete" Response: • The acquirer has a partially documented plan, it has a documented plan but staff are unaware it exists, or the practice appears otherwise incomplete.
	2. Have incident declaration criteria that support the critical service been established and communicated to relevant external entities? [IMC:SG3.SP1, IMC:GG2.GP7]	**Question intent:** To determine if the acquirer's criteria for incidents that affect the critical service have been established and communicated to relevant suppliers and other external entities. Because it is very common for assets that support the critical service to be provided, maintained, or housed by external entities, it is important that relevant external entities be aware of the acquirer's criteria for incidents that affect the critical service. Organizations that do not establish and communicate these criteria can experience delays to become aware of – and respond to – incidents that affect the critical service. **Typical work products:** • documented incident declaration criteria • correspondence with external entities • documented results from joint exercises of the incident management plan **Criteria for "Yes" Response:** • The acquirer has established incident declaration criteria and communicated these to all of the relevant external entities that support the critical service. **Criteria for "Incomplete" Response:** • The acquirer has established incident declaration criteria and communicated them to some external entities, or the practice appears otherwise incomplete.
	3. Does the acquirer have a documented service continuity/business continuity plan to sustain the critical service? [SC:SG3.SP2]	**Question intent:** To determine whether the acquirer has a service continuity plan to sustain the critical service. The purpose of a service continuity plan and related activities is to ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other disruptive event. The development of service continuity plans is both a foundational and ongoing activity. Plans are developed at the time of service development and

		implementation, but are also updated on an ongoing basis as new risks are encountered and the operational environment changes. **Typical work products:** • service continuity plan **Criteria for "Yes" Response:** • The acquirer has a documented service continuity plan to sustain the critical service. **Criteria for "Incomplete" Response:** • The acquirer has a partially documented plan, there is a plan but staff at the acquirer seem generally unaware of it, or the practice appears otherwise incomplete.
	4. Do the acquirer's plans account for dependence on external entities? [EXD:SG2.SP2, SC:SG3.SP2]	**Question intent:** To determine if the acquirer has accounted for external dependencies as part of its incident management and service continuity planning. "Accounted for" means that the acquirer has analyzed each plan type to identify information relevant to external dependencies that should be included in the plan. This may include detailed planning relating to plan conflicts and external entities. Typically the names of the external entities that are essential to the critical service(s) and a contact list are included, at a minimum. **Typical work products:** • incident management and service continuity plan sections and information relevant to external dependencies • documentation of tasks that require interaction and handoffs between the acquirer and external entities • external entity contact information in plans • resolutions to plan conflicts **Criteria for "Yes" Response:** • The disruption management plan contains all of the relevant information pertaining to external entities that support the critical service. **Criteria for "Incomplete" Response:** • The disruption management plan contains some external entity information, or the acquirer has analyzed the plan but has not updated it with relevant information, or the practice appears otherwise incomplete.

	5. Do relevant external entities participate in the acquirer's planning activities? [IMC:GG2.GP7, SC:SG2.SP2]	**Question intent:** To determine if the acquirer includes the participation of external entities in its disruption management planning activities. Because external entities support the critical service, it is important that they participate in and contribute information to the acquirer's planning activities with respect to incident management and service continuity. Examples of planning considerations where external entity input may be required include: • Developing network connectivity procedures for alternate recovery sites • Identifying fire and emergency response times and first responder planned actions • Identifying supplier compliance or breach notification requirements which may affect acquirer incident response plans • Plan de-confliction, for example identifying supplier or governmental service responsibilities in the event of a regional disaster **Typical work products:** • correspondence • meeting notes • formal agreement clauses requiring supplier participation **Criteria for "Yes" Response:** • All relevant external entities that support the critical service participate in the acquirer's disruption management process. **Criteria for "Incomplete" Response:** • Some relevant external entities that support the critical service participate in the acquirer's disruption management and planning processes, or the practice appears otherwise incomplete.
	Goal 2 – Planning and controls are maintained and updated. The purpose of this goal is to assess whether the acquirer's controls and plans are continuously tested and updated with respect to external dependencies.	**Guidance**
	1. Are disruption management plans tested cooperatively with relevant suppliers? [SC:SG5.SP3,	**Question intent:** To determine if the acquirer exercises/tests its disruption management plans with relevant suppliers that support the critical

	IMC:GG2.GP7] Incident management Business continuity	service. In enterprises where critical services depend on the performance and resilience of external entities, it is essential that disruption plans are periodically tested with the cooperation and participation of those external entities. It is important to conduct exercises in a manner that simulates real events, during which various components and organizations may need to communicate, work together, and understand their roles and responsibilities to resolve an incident. Note, this practice does not require that testing or exercises be done with all external entities at the same time. **Typical work products:** • correspondence • testing plans including objectives and responsibilities for suppliers • post-exercise reports and reviews **Criteria for "Yes" Response:** • The acquirer exercises/tests disruption management plans with relevant suppliers that support the critical service. **Criteria for "Incomplete" Response:** • The acquirer tests disruption management plans with some suppliers, or the practice appears otherwise incomplete.
	2. Do changes in external entity relationships trigger a review of disruption management plans? [IMC:GG2.GP8, SC:SG7.SP1]	**Question intent:** To determine if the acquirer reviews disruption management plans (service continuity and incident management plans) based on changes to external entity relationships. Examples of changes that may trigger a plan review include • supplier relationships change, resulting in a single point of failure • a supplier agreement is terminated • changes in the composition of sub-contractors • external entity assets move to a different legal jurisdiction that may affect reporting or other requirements **Typical work products:** • list of external entity agreements, changes to which trigger plan review • staff responsibilities in job descriptions • internal correspondence or policy detailing

		changes that are relevant to disruption management plans **Criteria for "Yes" Response:** • The acquirer reviews disruption management plans when external entity relationships change in order to identify necessary plan changes. **Criteria for "Incomplete" Response:** • The acquirer reviews plans based on changes involving some external entities, it reviews plans inconsistently, or the practice appears otherwise incomplete.
	3. Are controls at suppliers that support the critical service periodically validated or tested to ensure they meet control objectives? [CTRL:SG4.SP1, EXD:SG4.SP1]	**Question intent:** To determine if the acquirer periodically tests or conducts reviews of controls at external entities to ensure that they continue to meet control objectives. Suppliers are often responsible for maintaining controls to protect assets that are important to the critical service, or for which the acquirer is directly responsible. Therefore, it is important that the acquirer periodically tests or validates that relevant suppliers are maintaining controls that meet the acquirer's control objectives. This activity may be conducted in a variety of ways including by: • Engaging third party auditors or reviews • Evaluating reporting from the supplier that documents the supplier's internal testing • Establishing criteria and schedules for testing controls (using penetration testing or other methods) **Typical work products:** • documented controls testing policies, standards, and procedures • reporting on controls testing at external entities • audits of controls testing at external entities **Criteria for "Yes" Response:** • For all suppliers that support the critical service, the acquirer tests, reviews, or validates controls at external entities to ensure they continue to meet control objectives, based on a documented period. **Criteria for "Incomplete" Response:** • The acquirer tests or validates controls at some suppliers, or it tests controls inconsistently or occasionally, or the practice appears otherwise

		incomplete.
	4. Does the acquirer have a documented list of triggering events or changes that require testing of controls at suppliers that support the critical service?[CTRL:SG4.SP1, EXD:SG4.SP1]	**Question intent:** To determine if the acquirer has documented criteria, issues, or changes that trigger tests/reviews of controls at suppliers to ensure that they continue to meet the acquirer's control objectives. In addition to testing or validating controls at external entities periodically, acquirers should identify and document events or changes that trigger testing or validation. This practice is intended to guard against the possibility that the acquirer may miss important changes to the control environment at the external entity until the next scheduled test or validation. Example triggering events include • changes in the external entities' technical environment, for example, new servers or other hardware • changes in the composition of sub-contractors (the supplier's external dependencies) • receiving threat or vulnerability information that may affect a supplier • the occurrence of incidents or "near-miss" incidents **Typical work products:** • documented list of triggering events • external entity controls testing policies, standards, and procedures **Criteria for "Yes" Response:** • For all relevant suppliers that support the critical service, the acquirer has a documented list of events that will trigger the testing or validation of suppler controls to ensure they continue to meet control objectives. **Criteria for "Incomplete" Response:** • The acquirer has a documented list of triggering events that apply to some suppliers, or the acquirer's list is partial, or the practice appears otherwise incomplete.

	Goal 3 – Situational awareness extends to external dependencies. The purpose of this goal is to assess whether the acquirer's situational awareness activities – for example collecting threat information - include external dependencies.	Guidance
	1. Has the acquirer assigned responsibility internally for monitoring sources of threat information? [MON:SG1.SP2]	**Question intent:** To determine if the responsibility for monitoring sources of threat information has been assigned. Effective threat monitoring requires the assignment of responsibility to specific staff. Threat monitoring is a process of data collection and distribution with the purpose of providing timely, accurate, complete, and relevant information about the acquirer's threat environment. Example sources of threat information include • vendors' notifications • industry groups (Sector Information Sharing and Analysis centers, Internet Storm Center, Nextgov Threat watch) • international sources (multinational vendors, CERT-EU) • weather alerts (NOAA) • law enforcement (FBI InfraGard, IC3) • DHS (ICS-CERT, NCICC) **Typical work products:** • staff responsibility listed in job descriptions • internal memoranda **Criteria for "Yes" Response:** • The acquirer has identified sources of information about threats that may affect the critical service and has assigned responsibility for monitoring these sources. **Criteria for "Incomplete" Response:** • The acquirer has assigned responsibility for monitoring some sources of threat information, a staff member monitors threat information inconsistently or not based on any formal assignment of responsibility, or the practice appears otherwise incomplete.

	2. Has the acquirer implemented threat monitoring procedures, including how threats are received and responded to? [MON:SG2.SP2]	**Question intent:** To determine if the acquirer has implemented procedures for monitoring threat information. Effective threat monitoring requires people, procedures, and technology that need to be deployed and managed to meet monitoring requirements. Procedures ensure the timeliness, consistency, and accuracy of threat information and the distribution of this information to relevant stakeholders. Threat monitoring procedures may address • source identification • monitoring frequency • threat identification • threat validation and analysis • threat and threat actor trend analysis • threat communication **Typical work products:** • Written procedures **Criteria for "Yes" Response:** • The acquirer has developed and implemented procedures for all threat monitoring activities. **Criteria for "Incomplete" Response:** • The acquirer has implemented procedures for some threat monitoring activities, procedures are under development, or the practice appears otherwise incomplete.

	3. Does the acquirer participate in or take advantage of industry consortia (i.e., InfraGard, Coordinating Councils, Council of Supply Chain Management) to detect threats to the acquirer and external entities? [MON:SG2.SP1, MON:GG2.GP7] Suppliers Infrastructure providers	**Question intent:** To determine if the acquirer has identified external entities that support the critical service, that it should include as part of its threat monitoring activities for the purpose of detecting threats to these external entities. Acquirers may choose to include threats to external entities as part of their threat monitoring activities in cases where, for example, a supplier lacks its own threat monitoring program. An acquirer may decide that sustaining the critical service requires a more complete understanding of threats to critical infrastructure than it receives through its relationships with the specific infrastructure providers. **Typical work products:** • Internal correspondence and meeting notes • list of entities to include as part of threat monitoring **Criteria for "Yes" Response:** • The acquirer has analyzed its external dependencies to identify external entities that it should include as part of its threat monitoring, and it monitors threats against these entities. **Criteria for "Incomplete" Response:** • The acquirer has identified some external entities it should include as part of its threat monitoring, or it monitors threats to external entities inconsistently, or the practice appear otherwise incomplete.
	4. Do the acquirer and relevant external entities exchange information about threats to the critical service? [MON:SG2.SP4, MON:GG2.GP7]	**Question intent:** To determine if the acquirer exchanges threat information with relevant external entities that support the critical service. Example activities include • threat or situational awareness reporting jointly developed or distributed to the acquirer and external entity stakeholders • shared information repository or system where the acquirer and external entity can share information on threats • threat monitoring and response teams comprising representatives from the acquirer and the external entity **Typical work products:** • correspondence

		• distribution list for threat information • recurring meetings to exchange threat information **Criteria for "Yes" Response:** • The acquirer exchanges threat information with all relevant external entities that support the critical service. **Criteria for "Incomplete" Response:** • The acquirer exchanges threat information with some relevant external entities that support the critical service, or the practice appears otherwise incomplete.
	5. Does the acquirer participate in or take advantage of industry consortia (i.e., InfraGard, Coordinating Councils, Council of Supply Chain Management) to detect threats to the acquirer and external entities? [MON:SG2.SP1, MON:GG2.GP7]	**Question intent:** To determine if the acquirer participates in groups or activities that help it detect or identify threats to the critical service. Example activities and groups include • industry or sector incident/cyber exercises • InfraGard • Sector Coordinating Councils • ISACs • participation in industry groups such as the Council of Supply Chain Management **Typical work products:** • notes and correspondence relating to threat information • shared threat reports • correspondence from senior leadership affirming participation or membership of relevant groups **Criteria for "Yes" Response:** • The acquirer participates in activities or groups to help identify relevant threats to the critical service, and the information learned influences activities to protect and sustain the critical service. **Criteria for "Incomplete" Response:** • The acquirer participates occasionally or inconsistently in groups to detect and identify threats to the acquirer or its suppliers, or it participates but the information learned does not discernibly influence activities to protect the critical service, or the practice appears otherwise incomplete.
	6. Are threats to external entities reported to internal stakeholders for	**Question intent:** To determine if threats to external entities that are detected by the acquirer

	use in managing the dependency? [MON:SG1.SP3, MON:SG2.SP4]	are reported to internal stakeholders. Internal stakeholders should be advised of threats to external entities that are relevant to the acquirer's critical service. Internal stakeholders may use this information for a variety of purposes: • to consider external entities' susceptibility to threats when entering into new agreements • to change external entity selection criteria • to refine or adjust incident or intrusion detection systems to detect attacks involving external entities • to evaluate the external entity's reactions and risk mitigation as part of performance management • to consider the existence of the threat when making risk management decisions Threat information communications must be delivered on an as-needed basis, according to established requirements. Because threat information communications can be diverse, a broad array of procedures, practices, technology, and infrastructure to support those requirements may need to be developed and implemented. The infrastructure to support various communication methods (physical and technical) and channels must be developed and implemented. Through these actions, timely, relevant, consistent, high-quality, and purposeful communications can be delivered proactively or during an event, incident, or crisis. **Typical work products:** • list of stakeholders to receive threat information • threat reports **Criteria for "Yes" Response:** • The acquirer reports to internal stakeholders all threats to relevant external entities that support the critical service. **Criteria for "Incomplete" Response:** • The acquirer reports threats to some internal stakeholders, or it reports threat information inconsistently, or the practice appears otherwise incomplete.

Service Protection and Sustainment – Other Observations

4 Maturity Indicator Level

The maturity indicator level questions below apply to all of the domains in this assessment; Relationship Formation, Relationship Management and Governance, and Service Protection and Sustainment. Achievement of the maturity indicator levels means that external dependencies management is more likely to be effective, consistent, and retained during times of disruption or acquirer change.		
MIL2-Planned	Performance at MIL2 – Planned means that external dependencies management is not only performed but also supported throughout the lifecycle of external dependencies by sufficient planning, stakeholder involvement, and standards and guidelines.	
	1. Is there a documented plan for performing external dependencies management?	**Question Intent:** To determine if a plan for performing external dependencies management exists. The plan defines external dependencies management within the organization and prescribes how external dependencies management activities will be performed. In practice, many of the required actions to manage external dependencies may be documented in other plans or documents (for example vendor selection and contracting procedures, or service continuity plans that involve third parties). The purpose of the EDM plan is not to duplicate or repeat material, but rather to establish and clarify the roles and responsibilities of staff and activities across the acquirer, to ensure that practices, activities, and documentation relevant to other security and resilience activities support EDM. The plan typically includes • who performs EDM activities • key EDM activities • when and how often EDM activities are performed • identification of EDM stakeholders • standards and funding information **Typical work products:** • written plan including change log

		• plan status information such as implementation level or known open issues **Criteria for "Yes" Response:** • There is a documented plan for performing external dependencies management. **Criteria for "Incomplete" Response:** • A plan is in development, or is partially documented, or is otherwise incomplete. Because organizational operations, priorities, and requirements may change frequently, plans require periodic review and update to remain effective, as determined by the organization.
	2. Is there a documented policy for external dependencies management?	**Question Intent:** To determine if a policy for performing external dependencies management activities exists. A policy is a written communication from the organization's senior management to employees that establishes the organizational expectations for planning and performing the external dependencies management activities and communicates these expectations to the organization. The policy will typically address • responsibility, authority, ownership, and the requirement to perform external dependencies management activities • the identification of procedures, standards, and guidelines • how adherence to or potential violations of the policy is measured, and potential exceptions are documented • compliance with legal, regulatory, contractual, and government obligations **Typical work products:** • written policy • correspondence from leadership referencing policy **Criteria for "Yes" Response:** • The organization has a documented policy for performing external dependencies management. **Criteria for "Incomplete" Response:** • A policy is in development, is partially

		documented, does not apply to the critical service, or is otherwise incomplete. If the policy has not been periodically reviewed or updated, as determined by the organization, it may also be appropriate to consider it incomplete.
	3. Does the plan or policy identify and describe external dependencies management processes?	**Question Intent:** To determine if the plan or policy identifies, references, or describes external dependencies management activities. Activity descriptions document the series of actions or specific steps that are necessary to perform external dependencies management activities in a repeatable, predictable manner. Examples may include: • the activity to form supplier relationships, for example the steps ("gates") and approval authorities required for new relationships • the activity to identify external dependencies • The activities to modify formal agreements with external entities **Typical work products:** • explanations of external dependencies management activities • activity requirements • activity linkages and interdependencies **Criteria for "Yes" Response:** • Plans or policies include (or reference) documented descriptions of external dependencies management activities. **Criteria for "Incomplete" Response:** • Activity documentation is in development, only partially relevant to the critical service, or is otherwise incomplete.
	4. Have internal and external stakeholders for external dependencies management activities been identified and made aware of their roles?	**Question Intent:** To determine if stakeholders for external dependencies management activities have been identified and made aware of their roles. Stakeholders of the external dependencies management activity may be a person or organization that has a vested interest in the organization or its activities. Their input and engagement is essential to establishing, managing and improving external dependencies

		management activities. **Typical work products:** • Stakeholder lists and related information • Stakeholder engagement communications • Stakeholder input and feedback tracking **Criteria for "Yes" Response:** • All stakeholders for the external dependencies management activities have been identified in the written plan and made aware of their roles. **Criteria for "Incomplete" Response:** Some stakeholders have been identified and made aware of their roles, or stakeholders are identified but have not been made aware of their roles, or the activity is otherwise incomplete.
	5. Have external dependencies management standards, guidelines, and roles been identified and implemented?	**Question Intent:** To determine if standards and guidelines for performing external dependencies management activities have been identified and implemented. Standards and guidelines can help provide support for establishing more consistent and predictable activities. They can also provide assistance with organization-specific details for individuals who may be less familiar with EDM and operational risk management practices. EDM standards and guidelines may address • criteria for prioritizing external dependencies • templates that define the correct information needed to identify, track and manage external dependencies in databases or information repositories • the guidelines and standards required to make risk statements with impact valuation • agreement templates, including enterprise specifications that apply to external entities • time standards for becoming aware of contractor personnel changes that require deleting or modifying access to the acquirer • standard RFPs, including applicable SLAs • criteria for selecting external entities • performance-monitoring report standards and templates • corrective-action report standards and examples

		Typical work products: • Written standards that establish expectations for performance • Guidelines which are used to ensure the performance of EDM activities meets standards and are predictable, measurable, and repeatable **Criteria for "Yes" Response:** • The organization has implemented documented standards and guidelines for performing external dependencies management activities. **Criteria for "Incomplete" Response:** • Some standards and guidelines have been implemented.
MIL3-Managed	Performance at MIL3 – Managed means that external dependencies management is performed, planned and supported throughout the lifecycle of external dependencies by sufficient oversight and resources.	
	1. Is there management oversight of the performance of external dependencies management?	**Question Intent:** To determine if management oversight exists. The intent of the practice is to ensure oversight is being performed on the performance of all external dependencies management activities. Oversight may include regular meetings, written or oral status updates, auditing or spot checks **Typical work products:** • assignment of responsibility in job descriptions • organizational communications and memoranda • inclusion of activity tasks in staff performance management goals and objectives, with measured of progress against these goals **Criteria for "Yes" Response:** • Management oversight of all the day-to-day external dependencies management activities is being performed. **Criteria for "Incomplete" Response:** • Management oversight covers some aspects of external dependencies management activities, or there is coverage for some areas, or the activity is otherwise incomplete.
	2. Are the acquirer's external dependencies management	**Question Intent:** To determine if the organization identifies and manages risks to the performance of

	processes periodically reviewed to identify and manage risks to these processes?	external dependencies management activities. This practice refers to identifying risks to the performance of EDM, and is distinct from managing the risks of entering into specific supplier or vendor relationships. Examples of risks to an EDM activity include: • the risk that insufficient standards or activity definition will result in an incorrect prioritization of dependencies • the risk of variability or inaccuracies in risk statements or valuations relating to external dependencies • imprecise supplier selection criteria and the risk of improper supplier influence on acquirer staff • the risk that centrally (corporate) managed relationships with infrastructure or governmental service providers may not adequately account for the critical service's resilience requirements • Inadequate linkage/communication between Change Management and EDM activities. **Typical work products:** • documented EDM activity review procedures • reports and communications about specific EDM activity risks **Criteria for "Yes" Response:** • Risks to the performance of all planned external dependencies management activities are identified, analyzed, disposed of, monitored, and controlled. **Criteria for "Incomplete" Response:** • Risks to the performance of some EDM activities are reviewed and identified, or risks to the performance of EDM activities are sporadically reviewed, or the activity is otherwise incomplete.
	3. Have qualified staff been assigned to perform external dependencies management activities as planned?	**Question Intent:** To determine if qualified staff have been assigned to external dependencies management activities. The intent of this question is to evaluate the qualifications of the staff, not the completeness of the plan. Qualified means that staff are appropriately skilled to perform external dependencies management activities, and have been assigned responsibility and given authority for performing those activities.

		Examples of qualified staff include personnel responsible for • evaluating and selecting external entities • negotiating agreements with external entities • 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 required • technical skills to evaluate technology provided by suppliers for vulnerabilities **Typical work products:** • documented skills required for EDM activities • staffing and succession plans for EDM activities **Criteria for "Yes" Response:** • Enough sufficiently skilled staff have been assigned to perform planned external dependencies management activities. **Criteria for "Incomplete" Response:** • Some staff have the skills necessary to perform their roles, or the practice is otherwise incomplete.

	4. Is there adequate funding to perform external dependencies management activities as planned?	**Question Intent:** To determine if adequate funding is provided. The intent of the question is to evaluate the completeness of the funding, not the completeness of the plan. **Typical work products:** • budgets to support the external dependency plan **Criteria for "Yes" Response:** • Adequate funding has been provided to perform all planned external dependencies management activities. **Criteria for "Incomplete" Response:** • The planned activities have only been partially funded, or some areas in the organization are not considered in the funding, or the activity is otherwise incomplete.
MIL4-Measured	Performance at MIL4 – Measured means that external dependencies management is performed, planned, managed, and supported throughout the lifecycle of external dependencies by controls, monitoring, and effectiveness measures.	
	1. Are external dependencies management activities periodically reviewed and measured to ensure they are effective and producing intended results?	**Question Intent:** To ensure the external dependencies management activities remain effective and produce intended results by conducting periodic review and measurement. **An example of a measurement is the percentage of external entities that have undergone some form of assessment, risk assessment, or audit.** **Other examples of measurements include the count or percentage of external entities in the following categories:** • by number or type of unforeseen or disruptive agreement changes • by performance problems • by problems relating to responsiveness or timeliness involving EDM practices, for example participation in service continuity planning or

		change management boards • located in less suitable geographic or political regions (for example characterized by political instability or physical security problems) • count of suppliers with which the acquirer has open litigation involving the critical service • by supplier adherence or compliance with independent standards • number of supplier relationships terminated for performance failures **Typical work products:** • documented list of measures for external dependencies management • list of identified weaknesses • exception reports – areas out of compliance with activity standards **Criteria for "Yes" Response:** • All external dependencies management activities are periodically (as defined by the organization) reviewed and measured, and the results evaluated. **Criteria for "Incomplete" Response:** • The organization has not established a frequency for review of external dependencies management activities, or review and measurement addresses some of the external dependencies management activities, or external dependencies management activities are reviewed but not measured, or the activity is otherwise incomplete.
	2. Are external dependencies management activities periodically reviewed to ensure they are adhering to the plan?	**Question Intent:** To periodically determine if external dependencies management activities are being performed as planned. Examples of possible periodic (as defined by the organization) plan review items: • percentage of external dependencies without designated organizational owners • count of supplier relationships formed outside the external dependencies management activity • percentage of external dependencies records or database entries with old or incomplete information **Typical work products:** • designation of responsibility for periodic reviews • exception reporting

		• stakeholder communication regarding reviews of external dependencies management activities **Criteria for "Yes" Response:** • All external dependencies management activities are periodically (as defined by the organization) reviewed to ensure that these activities are performed as planned. **Criteria for "Incomplete" Response:** • The organization has not established a frequency for reviews, or some external dependencies management activities are reviewed, or the activity is otherwise incomplete. • If MIL 2.Q1 is Incomplete (can't be a yes if there is no/incomplete Plan)
	3. Is higher level management aware of issues related to the performance of external dependencies management?	**Question Intent:** To determine if the performance of external dependencies management is communicated to higher-level managers to provide visibility and facilitate the resolution of issues. Higher-level managers include those in the organization above the immediate level of management responsible for the external dependencies management activity. Communications are expected to be performed periodically (as defined by the organization) and may be event-driven when escalation is needed. **Typical work products:** • reviews of status of external dependencies management activities • reporting of issues identified in activity and plan reviews • documented reporting of risks associated with external dependencies management activities • recommendations for improvement **Criteria for "Yes" Response:** • Higher-level management is made aware of issues related to the performance of external dependencies management. **Criteria for "Incomplete" Response:** • The organization has not established a frequency for communication to higher-level management, or communications address some issues, or some stakeholders are not included in the communications, or the activity is otherwise incomplete.

MIL5-Defined	Performance at MIL5 – Defined means that external dependencies management is performed, planned, managed, measured, and defined across the enterprise.	
	1. Has the acquirer identified, described, and disseminated standardized external dependency management activities that apply across the enterprise?	**Question Intent:** To determine if the acquirer enterprise has identified, described, and disseminated standardized activities that define external dependencies management. Standardized activities provide a predictable level of consistency for external dependencies management activities across the enterprise. This activity involves: • selecting - from the activities used by business units, divisions, or industry peers - the EDM activities that best meet the needs of the enterprise • ensuring that the enterprise's business, policy, and activity objectives are appropriately addressed in these standard, defined activities • documenting the defined activity • revising the description of the standard, defined activity as necessary **Typical work products:** • documented definitions of standard activities across the enterprise • reporting on external dependencies management activity identification and description activities **Criteria for "Yes" Response:** • The acquirer enterprise has identified, documented, and disseminated standardized EDM activities across the enterprise. **Criteria for "Incomplete" Response:** • Some standard activities have been defined, documented, and disseminated across the enterprise.
	2. Has the acquirer provided individual operating units with guidelines to help them tailor standard enterprise activities to fit their unique operating circumstances?	**Question Intent:** To determine if the organization has provided operating units with guidelines to help them tailor standard activities to fit their unique operating circumstances. The purpose of tailoring guidelines is to help individual operating units derive practices that best suit their unique operating circumstances and requirements – while allowing enterprise

		management to realize predictability, confidence, and efficiencies in the external dependencies management capability of dispersed business units. **Typical work products:** • guidelines for tailoring external dependencies management activities • list of areas which have tailored the enterprise activity definitions **Criteria for "Yes" Response:** • The organization has provided operating units with guidelines to help them tailor standard external dependencies management activities to fit their unique operating circumstances. **Criteria for "Incomplete" Response:** • Guidelines for tailoring standard external dependency activities are under development or are otherwise incomplete.
	3. Are improvements or changes to external dependency management documented and shared across the organization?	**Question Intent:** To determine if improvements or changes to the external dependencies management activity are documented and shared across the organization. Documentation of lessons learned during the execution and reviews of the external dependencies management activity may be used to propose improvements to the activity. Sharing lessons learned enables organization-wide activity improvements and organization-wide learning. **Typical work products:** • activity metrics and measurements • direct feedback from stakeholders • lessons learned in post-event review of incidents and disruptions in continuity • lessons learned from periodic reviews of external dependencies management activities that can be applied to improve the external dependencies management activity • risk evaluation techniques and tools found to be effective in managing the activity **Criteria for "Yes" Response:** • Improvements to external dependencies management activities are documented and shared across the organization. **Criteria for "Incomplete" Response:**

		• Improvements to external dependencies management activities are inconsistently documented, or not consistently shared across the organization, or are otherwise incomplete.

Glossary

The following definitions are used in the EDM Assessment:

Acquirer – an acquirer that depends on external entities (vendors, infrastructure providers, public services, other business units in some cases) to fulfil its mission or business objectives. Acquirer refers to the assessed or subject acquirer.

Assets – People, Information, Technology, and Facilities that are used to provide the critical service being assessed. Several questions in the EDM Assessment refer to acquirer or external assets. These terms have the following meanings:

> **Acquirer assets** – assets (people, information, technology, facilities) which the acquirer is primarily responsible for in terms of the assets' viability, productivity, and resilience.
>
> **External assets** – assets (people, information, technology, facilities) for which external entities are primarily responsible in terms of the assets' viability, productivity, and resilience.

Cooperative – describes activities or processes that are jointly performed by the acquirer and one or more external entities.

Disruption management – activities to manage and mitigate the impact of events that may negatively affect the requirements for the critical service. These usually involves activities such as incident management, problem management, service/business continuity, or crisis planning.

External dependency - a condition in which the production and requirements of one or more products or services provided by the acquirer depend on the actions of an external entity. This is usually because the external entity is a supplier of goods or services to the acquirer; it has access to, ownership of, control of, responsibility for, or some other defined obligation relating to an asset used to provide the critical service.

Related terms:

> **Relationship:** the existence of a connection, association or some level of external dependency.
>
> **Formal agreement:** a written agreement that creates obligations between the acquirer and an external entity. Formal agreements can provide clarity on terms, requirements and responsibilities. Formal agreements are not required for an external dependency or relationship to exist.

External entity – an acquirer that is separate from the assessed acquirer or business unit. While these are frequently separate legal entities, they may also be separate business units, affiliates or divisions within a large enterprise.

External entity types. The following are the definitions used in the EDM Assessment.

Supplier - an external entity that:

1. supplies one or more of the following to the acquirer:
    a. information and communications technology (ICT)
    b. services supported by ICT
    c. services that support the acquirer's operation or sustainment of ICT, and
2. with which the acquirer has some ability to negotiate the terms and conditions of formal agreements that govern the acquirer-supplier relationship.

Suppliers may also be known subcontractors, vendors, separate divisions or affiliates of a large enterprise, or third parties.

Governmental services – a service provided to people, acquirers, or other entities in a political subdivision (nation, state, or locality), usually provided by a governmental department or agency. These services frequently involve security; for example fire, police, and emergency response.

Industry consortia – voluntary groups of private industry or public stakeholders working cooperatively to minimize cybersecurity and external dependency risk. This activity frequently involves exchanging information about risks and threats.

Infrastructure providers – a type of supplier that supplies goods or services to a region, economy, infrastructure sector, or political subdivision, and with which the acquirer normally has no commercially practical ability to negotiate the terms and conditions of agreements. Contracts with public infrastructure providers are generally "take it or leave it".[1] Examples include natural gas, water, power, or transportation.

Trusted supplier (ICT) – an external entity that supplies information and communications technology to the acquirer, which the acquirer has justifiable reason to believe, meets appropriate standards for the use intended. One way for the supplier to achieve this is by demonstrating compliance with standards set forth by an acknowledged authority to ensure the integrity of the technology purchased. The authority may be the original manufacturer or an appropriate governing acquirer (for example: The Open Group or similar standard).

Using a trusted ICT supplier cannot provide complete protection against vulnerabilities, malicious tampering, or counterfeit ICT; however, it does indicate the presence of management controls against this specific risk.

[1] The key difference between a vendor and an infrastructure provider, from thew perspective of External Dependencies Management, is that acquirers normally have a very limited ability to negotiate the terms of the relationship with infrastructure providers. Note that this is a relative standard. In other words, large acquirers that do have the ability to negotiate terms with infrastructure providers may wish to treat these external entities as suppliers for the purpose of an assessment. Because the EDM Assessment is intended for critical infrastructure acquirers of different sizes, this is intended to be a flexible definition.

External process – describes processes performed using primarily external assets.

Internal process – describes processes performed using primarily acquirer assets.

Plan – a document that describes the actions required of acquirer staff to satisfy the acquirer's requirements in a particular work area or activity. Plan in the EDM Assessment refers to the existence of written documentation. Plans may exist in more than one specific document or acquirer repository.

Stakeholder – a person or acquirer that has a vested interest in the acquirer or its activities.

Supply chain – the material and informational interchanges in the logistical process stretching from acquisition of raw materials to delivery of finished products to the end user. All vendors, service providers and customers are links in the supply chain.[2]

[2] Source: Council of Supply Chain Management Professionals, 2013 Glossary.