NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S14-001
IT Standard: **Information Security Risk Management**	**Updated:** 11/23/2021
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

Security risk management is a critical component of any information security program. It helps ensure that risks to the confidentiality, integrity, and availability of an organization's systems and data are identified, analyzed, and monitored. Information security risk management activities must be integrated into State Entity (SE) processes to provide governance and ensure consistent responses to identified risks at all levels of the organization.

The security of New York State (NYS) and SE assets such as personal, private, sensitive information (PPSI) is essential. This Standard provides the minimum requirements for an SE's risk management program that frames, assesses, responds to, and monitors mitigation of organizational risk.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*[1], established January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy,

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

3.0 Scope

This standard applies to all "State Entities", defined as "State Government" entities as defined in Executive Order 117 or "State Agencies" as defined in Section 101 of the State Technology Law and NYS political subdivisions, and includes, but is not limited to, their employees, consultants, vendors, and contractors), that use or access any ITS Information Technology Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. While an SE may adopt a different standard, it must include the requirements set forth in this one.

4.0 Information Statement

4.1 Risk Management Process

Information security risk management is an organizational function that considers vulnerabilities, threat sources, identified risks, and security controls within an organization's environment. These factors help determine the resulting level of risk posed to SE information, systems, processes, and individuals that support SE business functions. Risk management and subsequent assessment activities can take many forms (e.g., formal risk assessment, audits, security reviews, configuration analysis, vulnerability scanning and testing), which all aim to identify and respond to risk in ways that improve an SE's overall security posture. An SE can never completely eliminate risk but can take steps to better manage risk.

There are four components of a risk management program: risk framing, risk assessment, risk response, and risk monitoring. Each of these components, briefly defined below, are outlined in further detail in subsequent sections.

- Risk Framing – establishes the context and common strategy for SE risk management activities.
- Risk Assessment – procedures for identifying, categorizing, and prioritizing risk to SE operations, assets, data, and more.
- Risk Response – approved response types to identified risks; and
- Risk Monitoring – ongoing maintenance activities associated with identified risks.

Information security risk management activities also occur at multiple layers within an organization, each providing different components to a consistent risk management program. For the purposes of this document, these layers, or "tiers," are separated as follows: Organization, Mission/Business Processes, and Information Systems. Table 1 defines and provides sample activities for each tier.

Table 1 – Organizational Risk Management Tiers

	Definition	Sample Activities
Tier 1: Organization level	Establishes the risk management program and provides context for risk-related activities at lower tiers. The organization tier activities often include SE executive staff and other relevant decision makers to provide strategic guidance to SE staff.	• Establish SE risk management function • Define SE risk tolerance • Prioritize mission/business functions
Tier 2: Mission/Business Process level	Focuses on the processes required to support mission/business functions defined at tier 1. Activities at tier 2 are informed by the strategic vision outlined at tier 1 and inform subsequent risk management processes at tier 3.	• Define and prioritize mission/business processes • Identify and classify data necessary for mission/business functions • Establish enterprise architecture in support of tier 1 strategic vision
Tier 3: Information System level	Risk management activities associated with a specific information system.	• Identifying and implementing security controls for the system • Managing secure system development life cycle (SSDLC) activities

Figure 1 demonstrates the interaction between the risk management program functions and organizational tiers. Risk framing primarily operates at the organizational tier, while risk assessments can occur at all tiers of the SE. Both risk response and risk monitoring primarily occur at tier 2 and 3. However, the SE risk management program may operate differently depending on the SE mission and other strategic goals.

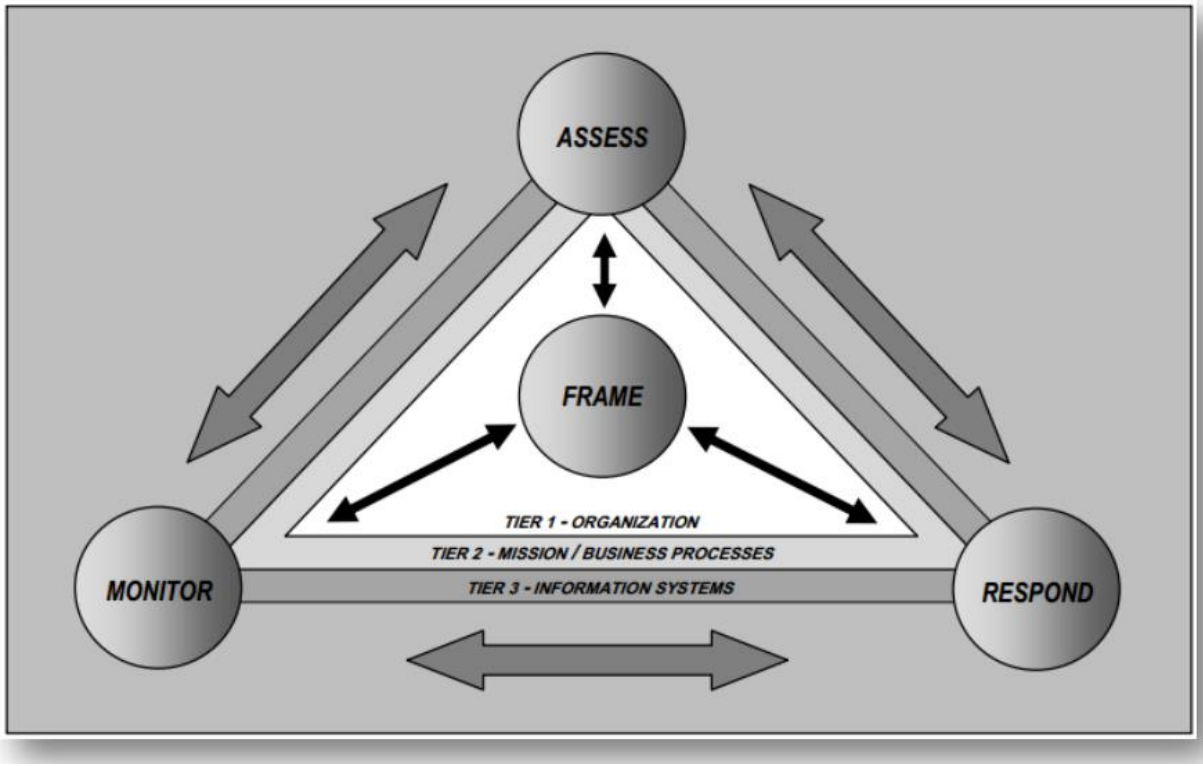

Figure 1. Risk Management Program and Organizational Tier Interaction (NIST Special Publication 800-39, page 32).

It is important to note that information security risk management is dynamic; actions at each organizational tier and risk management function will inform other activities. For example, changes to an SE business process may require changes to an associated information system, requiring a risk assessment. Newly identified risks would require new risk responses and would be incorporated into the SE's risk monitoring activities.

4.2 Risk Framing

Risk framing establishes the SE information security risk management strategy that governs subsequent activities (i.e., assessing, responding to, and monitoring risk). Risk framing activities generally happen at tier 1 as SE executive management will establish the overarching risk management strategy. Additionally, as required in the NYS-P03-002 Information Security Policy, SEs must designate an individual or team responsible for the risk management function. This function will support the development and implementation of the SE risk management program. There are two primary components of the risk framing function: risk tolerance and governance.

4.2.1 Risk Tolerance

Risk tolerance is the level of residual information security risk, including the environmental context that may influence a risk-based decision (e.g., regulatory requirements, SE mission, budget, etc.), that is acceptable for the organization. The SE risk tolerance governs risk response activities at all organizational tiers as it outlines what risks can be accepted. For example, an SE's risk tolerance will influence

the decision to use a new service based on the risk that it presents to the organization. Alternatively, the SE's risk tolerance will help to prioritize remediation activities across several existing SE systems.

The SE must define the organizational risk tolerance to support an effective risk management program. It is important to note that defining SE risk tolerance is an executive-level function and cannot be defined by Information Technology (IT) unless explicitly delegated by the SE. The SE is still responsible for risk management decisions even if risk tolerance determinations are transferred to an external entity.

SEs must establish organizational mechanisms for implementing the defined risk tolerance. For example, an SE may incorporate risk tolerance criteria into risk assessment and response activities or develop separate procedures to review identified risks and approve recommended risk responses in alignment with SE risk tolerance.

Where an identified risk affects multiple SEs, the strictest risk tolerance must apply. For example, where a risk identified in a system that processes high confidentiality data for one SE but low confidentiality data for another, the strictest response must be implemented, where possible. For risks that affect statewide infrastructure, the IT custodian must be included as a stakeholder.

4.2.2 Governance

Governance ensures that strategic and operational decisions align with the SE's defined risk tolerance to ensure that risk-based activities are monitored and evolve with the changing threat landscape. The SE must implement mechanisms to monitor risk management processes (e.g., establish and track approved risk assessment methodologies, risk responses, create risk management procedures) and regularly review performance, at least annually. This review serves two purposes:

1. Ensuring compliance with the information security risk management strategy (this includes relevant regulatory or business requirements) of the SE; and
2. Identifying potential changes required to the SE risk management strategy.

SE information security risk management activities should align with the processes used for other types of risk (e.g., financial, legal) to incorporate information security risk into existing strategic activities. SE information security risk management is only one type of risk that an SE must manage and should be prioritized as part of overarching strategic activities.

Information system vulnerability management must be included in risk management processes to ensure that they are reviewed and responded to appropriately. This is because significant vulnerabilities may change current strategic risk management decisions. For example, a newly identified vulnerability found in a business-critical

system may require an immediate fix. At the same time, another vulnerability may exist in components of several less critical systems. The SE must assess and prioritize responses to both vulnerabilities within the context of other risk management activities. Additional requirements for vulnerability management are found in the NYS-S15-002 Vulnerability Management Standard.

4.3 Assess Risk

Risk assessments identify, prioritize, and help an SE to estimate the level of risk associated with SE operations (i.e., mission, functions, image, and reputation), assets, individuals, external entities, etc. resulting from the operation and use of information systems and other sources.

The goal of a risk assessment is to identify:

- Threats (both internal and external) to the organization's operations, assets, individuals, or systems;
- Vulnerabilities, or weaknesses, that could impact the confidentiality, integrity, or availability of the assessed system, process, or other source;
- Impact, the level of harm (i.e., consequence), to the SE that may occur if a potential threat exploits a vulnerability; and
- Likelihood that the event will occur.

Risk assessment results incorporate the impact (degree of harm) and likelihood of the event. The following formula is used to assign a risk rating: risk = impact * likelihood. Qualitative (high, moderate, low) or quantitative ratings must be documented and assigned, with justification, for both impact and likelihood. Exhibit 1, Calculating Risk outlines this process in more detail.

SE risk assessments must include:

- Roles, responsibilities, and communication;
- Tools, techniques, and methodologies (e.g., quantitative, qualitative, or semi-quantitative) used to assess risk;
- Any assumptions or constraints;
- How threat information is obtained (i.e., sources and methods);
- How risk assessment information is collected; and
- The frequency of risk assessments.

Risk assessments can be conducted at any of the organizational tiers, each with different objectives and outputs. Tier 1 and 2 risk assessments should be performed, at a minimum, annually, per the NYS-P03-002 NYS Information Security Policy. Risk assessments conducted at one tier can inform threat, vulnerability, likelihood, and impact information used in assessments conducted at other tiers:

Tier 1 - SE Organizational Level Risk Assessments:

- Support organizational strategies, policies, guidance, and processes for managing risk;
- Focus on SE organizational operations, assets, and individuals;
- Can be based solely on the assumptions, constraints, risk tolerances, priorities, and trade-offs established in the risk framing step; and
- Consider the identification of mission-essential functions from Continuity of Operations Plans (COOP) prepared by the SE and relevant third parties when determining the contribution of Tier 2 risks.

Tier 2 - Mission/Business Process Level Risk Assessments:

- Conducted across multiple mission/business functions;
- Support control selection for mission/business processes, resiliency requirements, and the implementation of those requirements in the enterprise architecture;
- Inform decisions for how and when to use information systems for specific mission/business processes, including supporting mission/business processes in the event of a system compromise;
- Align with the development of Business Continuity Plans (BCP); and
- Focus on mission/business segments, with varying degrees of criticality and/or sensitivity to core organizational mission/business functions.

Tier 3 - Information System Level Risk Assessments:

- Conducted for each system and reviewed at each phase of the secure system development lifecycle (SSDLC) as outlined in the NYS-S13-001 Secure System Development Life Cycle Standard;
- Initial risk assessments (i.e., risk assessments performed for the first time, rather than updating prior risk assessments) should occur in the initial phase of system development, but can be performed at any phase in the system development life cycle;
- Evaluate anticipated vulnerabilities and conditions affecting the confidentiality, integrity, and availability in the planned environments of operation; and
- At a minimum, assessments must occur at system initiation, during system design, prior to transitioning the system to production, or after a significant change to the system.

Risk assessments must be maintained as part of the SE's risk monitoring program (e.g., changes in organizational information systems and environments may trigger a risk assessment review). Additional benefits include:

- Current risk assessments ensure timely, relevant information that enables SE leadership to make informed, real-time risk management decisions;

- Reduced cost of future assessments and support of ongoing risk monitoring activities; and
- Reduces assessment scope. Incremental risk assessments consider only new information and differential risk assessments consider how changes affect the overall risk determination.

4.4 Risk Response

Once a risk has been assessed, the SE must determine and implement the appropriate course of action. Options include:

1. **Risk Acceptance** – This is a documented decision not to act on a specific risk at the time of assessment. Acceptance is not negligence or "inaction" and can be appropriate if the risk falls within the SE's defined risk tolerance. A risk acceptance response must be reviewed periodically as part of requirements outlined in the risk monitoring section below. For example, choosing to accept the risk of an earthquake, based on the high cost of preventative controls and the low likelihood of occurrence of an earthquake in a given area.
2. **Risk Avoidance** – These are specific actions taken to eliminate the activities or technologies that are the basis for the risk. This is appropriate when the identified risk exceeds the SE's risk tolerance, even after controls have been applied (i.e., residual risk). For example, choosing not to connect to an unsecure network.
3. **Risk Mitigation/Reduction** – These are specific actions taken to eliminate or reduce risk to an acceptable level. This is the most common approach and is appropriate where controls can reduce the identified risk. For example, a firewall is installed to reduce the risk of network intrusion.
4. **Risk Transfer/Sharing** – These are specific actions taken to shift responsibility for the risk, in whole or in part, to a third party. This may be appropriate when it is more cost effective to transfer the risk, or when a third party is better suited to manage the risk. For example, the purchase of an insurance policy, by which a specified risk of loss is passed from the policyholder to the insurer.

Regardless of the chosen risk response, all NYS Information Security Policies and Standards must be considered. If the chosen response does not meet any one or more NYS Information Security Polices or Standards, the SE must submit an exception request to the Chief Information Security Office (CISO) as outlined in the NYS-P13-001 NYS Information Security Exception Policy.

4.5 Risk Monitoring

The SE must monitor and review, at least annually, the effectiveness of its risk response measures and maintain situational awareness regarding security and privacy by performing ongoing risk monitoring activities.

4.5.1 Risk monitoring activities include, but are not limited to:

1. Implementation of a process to alert the SE of significant changes in the factors used to assess its risk (e.g., assets, threats, controls, regulations, policies, risk tolerance). These changes/factors indicate that a new or updated assessment is needed.
2. Documenting and tracking identified risks and risk response efforts. Efforts must be tracked through a risk repository (e.g., Plan of Actions and Milestones (POAM)), which must be updated on a regular basis, at least annually, as defined by the system owner or SE.
3. Performing ongoing risk assessments when changes to the system, organization, compliance requirements, etc. are identified. A new risk assessment may be required following a security incident.

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all ITS policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, State Entities shall request an exception through the Chief Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this standard, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S14-001
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This standard shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
01/17/2014	Original Standard Release	Thomas Smith, Chief Information Security Officer
01/16/2015	Standard Review – no changes	Deborah A. Snyder, Deputy Chief Information Security Officer
02/21/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
09/11/2018	Scheduled review – minor changes to Authority, Scope, and title of office	Deborah A. Snyder, Deputy Chief Information Security Officer
12/15/2020	Added aspects of risk management aligned with NIST SP 800-30, NIST SP 800-37, and NIST SP 800-39	Karen Sorady, Chief Information Security Officer
11/23/2021	Scheduled review – minor changes to Authority, Scope	Karen Sorady, Chief Information Security Officer

9.0 Related Documents

NIST SP 800-30, Guide for Conducting Risk Assessments

NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems

NIST SP 800-39, Managing Information Security Risk

NYS-P03-002 Information Security Policy

NYS-P13-001 Information Security Exception Policy

NYS-S13-001 Secure System Development Life Cycle Standard

NYS-S15-002 Vulnerability Management Standard

Exhibit 1 – Calculating Risk

The level of risk presented by a specific scenario is calculated through a combination of the level of harm (impact) and likelihood of that event occurring. Impact and likelihood ratings must be documented with written justification when conducting a risk assessment.

Table 1 defines qualitative and semi-quantitative values (0-100 or 1-10 scales) to facilitate likelihood determinations as part of a risk assessment.

Table 1 – Likelihood Ratings

Adapted from NIST Special Publication 800-30 Tables G-2 through G-4

Qualitative Values	Semi-Quantitative Values		Likelihood Description
Very High	96-100	10	• Adversary is almost certain to initiate the threat event. • The threat event is almost certain to have adverse impacts. • Errors, accidents, or acts of nature may occur more than 100 times per year.
High	80-95	8	• Adversary is highly likely to initiate the threat event. • The threat event is highly likely to have adverse impacts. • Errors, accidents, or acts of nature may occur 10-100 times per year.
Moderate	21-79	5	• Adversary is somewhat likely to initiate the threat event. • The threat event is somewhat likely to have adverse impacts. • Errors, accidents, or acts of nature may occur 1-10 times per year.
Low	5-20	2	• Adversary is unlikely to initiate the threat event. • The threat event is unlikely to have adverse impacts. • Errors, accidents, or acts of nature may occur less than once per year but more than once per ten years.
Very Low	0-4	0	• Adversary is highly unlikely to initiate the threat event. • The threat event is highly unlikely to have adverse impacts. • Errors, accidents, or acts of nature may occur less than once per ten years.

Table 2 defines qualitative and semi-quantitative values to facilitate impact determinations as part of a risk assessment.

Table 2 – Impact Ratings

Adapted from NIST Special Publication 800-30 Table H-3

Qualitative Values	Semi-Quantitative Values		Impact Description
Very High	96-100	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on SE operations, assets, individuals, other organizations, or NYS.
High	80-95	8	The threat event could be expected to have a severe or catastrophic adverse effect on SE operations, assets, individuals, other organizations, or NYS. This may include: 1. Severe degradation or loss of mission capability to an extent and duration that the organization cannot perform one or more primary functions; 2. Major damage to organizational assets; 3. Major financial loss; or 4. Severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a serious adverse effect on SE operations, assets, individuals, other organizations, or NYS. This may include: 1. Significant degradation or loss of mission capability to an extent and duration that the organization can perform one or more primary functions, but the effectiveness is significantly reduced; 2. Significant damage to organizational assets; 3. Significant financial loss; or 4. Significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a limited adverse effect on SE operations, assets, individuals, other organizations, or NYS. This may include:

			1. Degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness is noticeably reduced; 2. Minor damage to organizational assets; 3. Minor financial loss; or 4. Minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a negligible adverse effect on SE operations, assets, individuals, other organizations, or NYS.

Final Risk Calculations

Once impact and likelihood ratings have been assigned, a final risk rating can be determined. Table 3 outlines the final risk rating for a specific scenario based on the impact and likelihood of the event.

Table 3 – Risk Rating Calculations

Adapted from NIST Special Publication 800-30 Table I-2

Likelihood	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

The following Tables provide a description of the Level of Risks in an assessment and the inputs of risk based on the organizational Tier.

Table 4 – Level of Risk

Adapted from NIST Special Publication 800-30 Table I-3

Qualitative Values	Semi-Quantitative Values		Risk Description
Very High	96-100	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on SE operations, assets, individuals, other organizations, or NYS.
High	80-95	8	The threat event could be expected to have a severe or catastrophic adverse effect on SE operations, assets, individuals, other organizations, or NYS.
Moderate	21-79	5	The threat event could be expected to have a serious adverse effect on SE operations, assets, individuals, other organizations, or NYS.
Low	5-20	2	The threat event could be expected to have a limited adverse effect on SE operations, assets, individuals, other organizations, or NYS.
Very Low	0-4	0	The threat event could be expected to have a negligible adverse effect on SE operations, assets, individuals, other organizations, or NYS.

Table 5 – Input Risk

Adapted from NIST Special Publication 800-30 Table I-3

Adapted from NIST Special Publication 800-30 Table I-1

Description	Provided to		
	Tier 1	Tier 2	Tier 3
From Tier 1 (Organization level) • Sources of risk and uncertainty information identified for organization-wide use (e.g., specific information that may be useful in determining likelihoods such as adversary capabilities, intent, and targeting objectives). • Guidance on organization-wide levels of risk (including uncertainty) needing no further consideration.	No	Yes	Yes *If not provided by Tier 2*

• Criteria for uncertainty determinations. • List of high-risk events from previous risk assessments. • Assessment scale for assessing the level of risk as a combination of likelihood and impact, annotated by the organization, if necessary. (Table 3) • Assessment scale for assessing level of risk, annotated by the organization, if necessary. (Table 4)			
From Tier 2: (Mission/business process level) • Risk-related information and guidance specific to Tier 2 (e.g., risk and uncertainty information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies).	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) • Risk-related information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation).	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*