RANSOMWARE READINESS ASSESSMENT

RRA Report

Disclaimer

The analysis, data, and reports in CSET® are provided “as is” for informational purposes only. The Cybersecurity & Infrastructure Security Agency (CISA) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report.

CISA does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by CISA.

The display of the CISA official seal or other CISA visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of CISA. The CISA seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by CISA or the United States Government. Use of the CISA seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against CISA policies governing usage of the seal.

The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the CSET Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the CSET Program Office.

Advisory

The Cyber Security Evaluation Tool (CSET®) is only one component of the overall cybersecurity picture and should be complemented with a robust cyber security program within the organization. A self-assessment with CSET® cannot reveal all types of security weaknesses, and should not be the sole means of determining an organization's security posture.

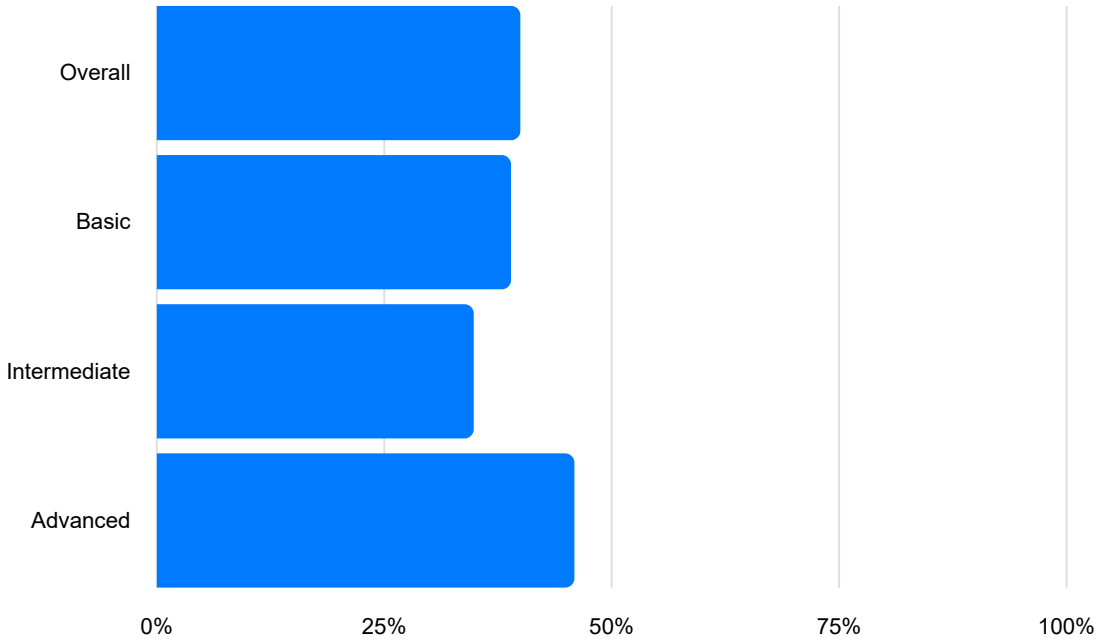
The tool will not provide a detailed architectural analysis of the network or a detailed network hardware/software configuration review. It is not a risk analysis tool so it will not generate a complex risk assessment. CSET® is not intended as a substitute for in-depth analysis of control system vulnerabilities as performed by trained professionals. Periodic onsite reviews and inspections must still be conducted using a holistic approach including facility walk-downs, interviews, and observation and examination of facility practices. Consideration should also be given to additional steps including scanning, penetration testing, and exercises on surrogate, training, or non-production systems, or systems where failures, unexpected faults, or other unexpected results will not compromise production or safety.

CSET® assessments cannot be completed effectively by any one individual. A cross-functional team consisting of representatives from operational, maintenance, information technology, business, and security areas is essential. The representatives must be subject matter experts with significant expertise in their respective areas. No one individual has the span of responsibility or knowledge to effectively answer all the questions.

Data and reports generated by the tool should be managed securely and marked, stored, and distributed in a manner appropriate to their sensitivity.

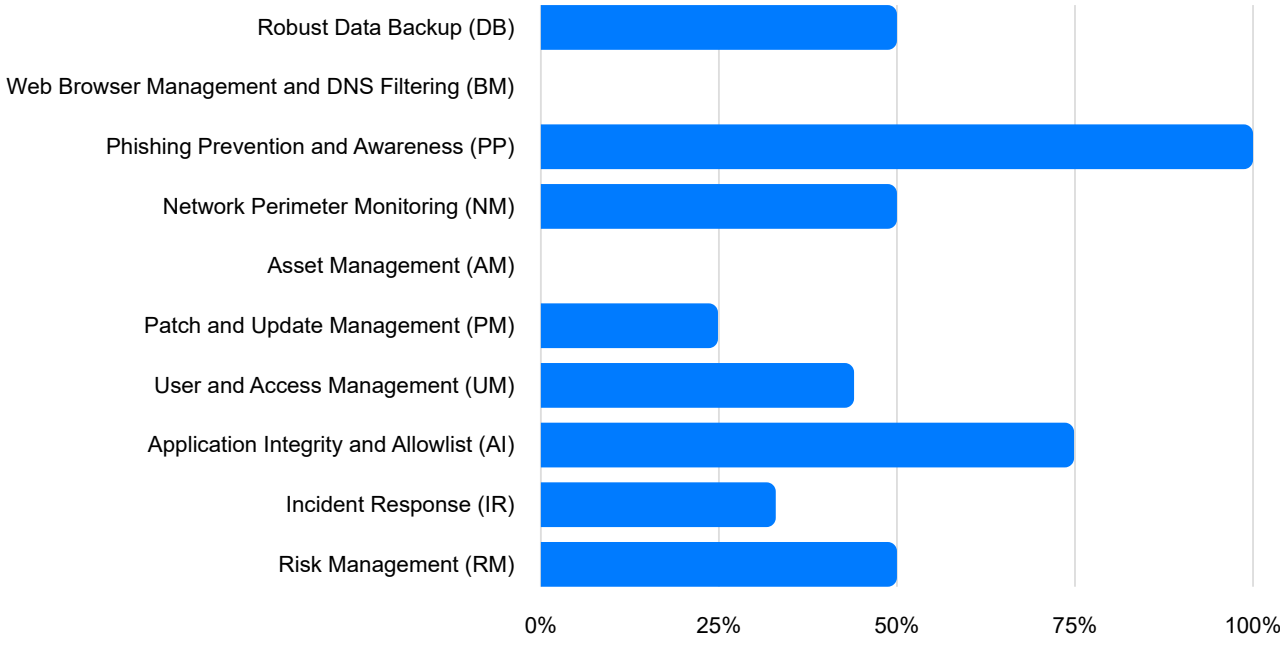
Percentage of Practices Performed

Overall Score	Basic	Intermediate	Advanced
40%	39%	35%	46%



Scores are calculated as the percentage of 'Yes' answers.

Percentage of Practices Performed by Goal

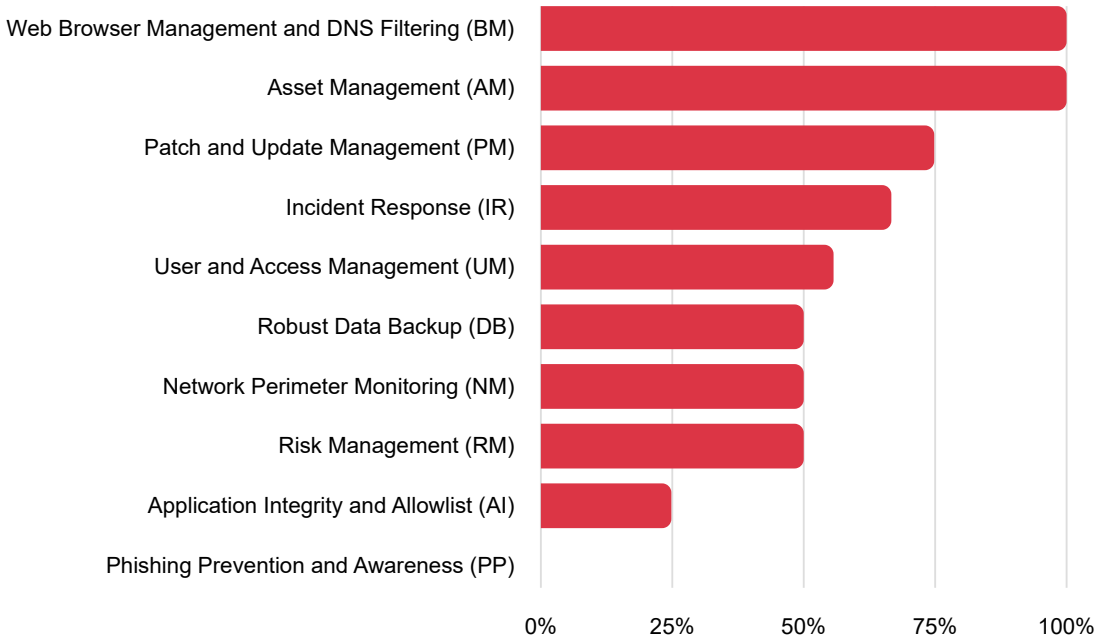


RRA Practices Scoring

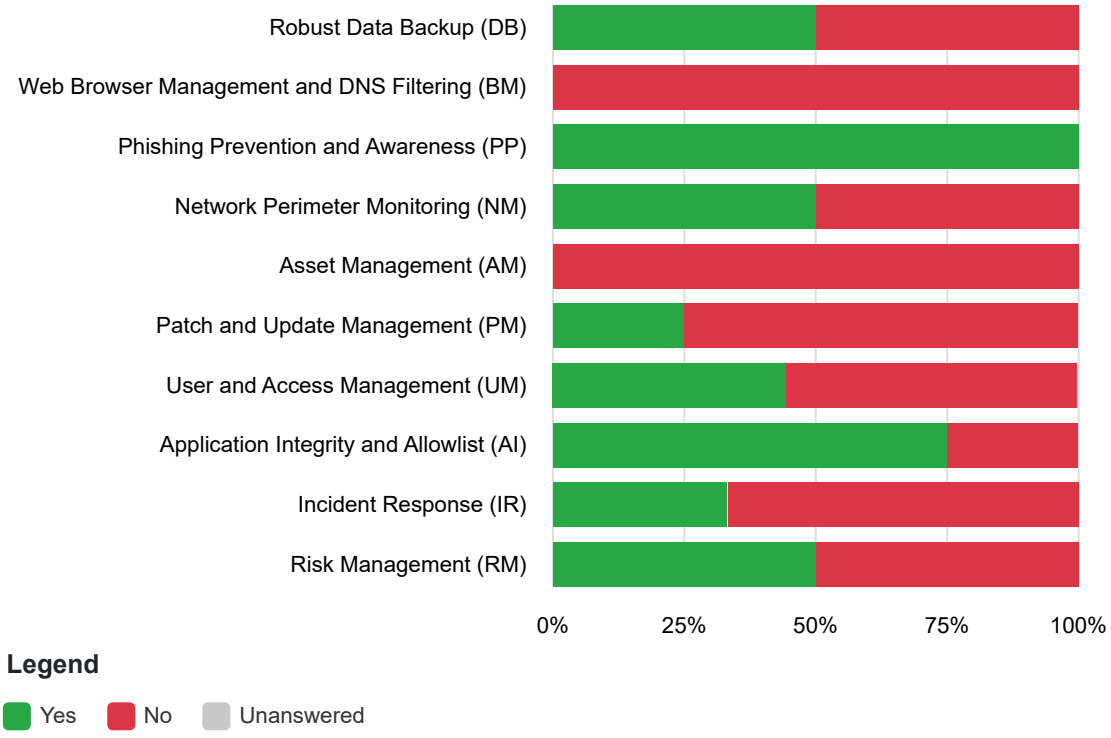
	Yes	No	Unanswered	Total Practices	Percent Complete
Robust Data Backup (DB)	1	1	0	2	50.0%
Web Browser Management and DNS Filtering (BM)	0	2	0	2	0.0%
Phishing Prevention and Awareness (PP)	3	0	0	3	100.0%
Network Perimeter Monitoring (NM)	2	2	0	4	50.0%
Asset Management (AM)	0	7	0	7	0.0%
Patch and Update Management (PM)	1	3	0	4	25.0%
User and Access Management (UM)	4	5	0	9	44.4%
Application Integrity and Allowlist (AI)	3	1	0	4	75.0%
Incident Response (IR)	3	6	0	9	33.3%
Risk Management (RM)	2	2	0	4	50.0%

Suggested Areas for Improvement

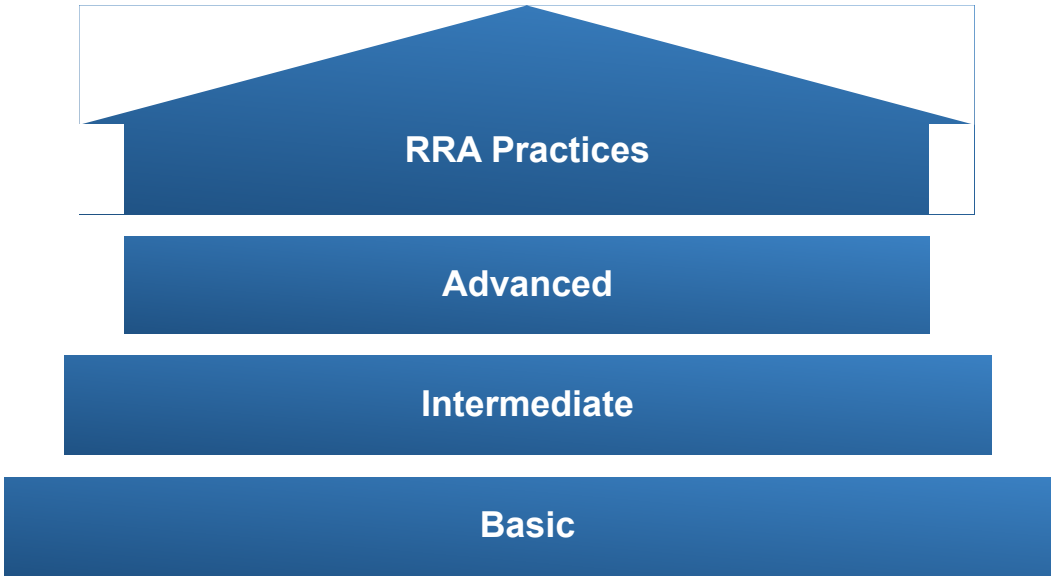
The goals in the assessment are ranked in order of deficiency with goals having fewer satisfied practices ranked higher in the chart. The bar chart reflects the percentage of practices for each goal that are answered 'No' or are left unanswered.



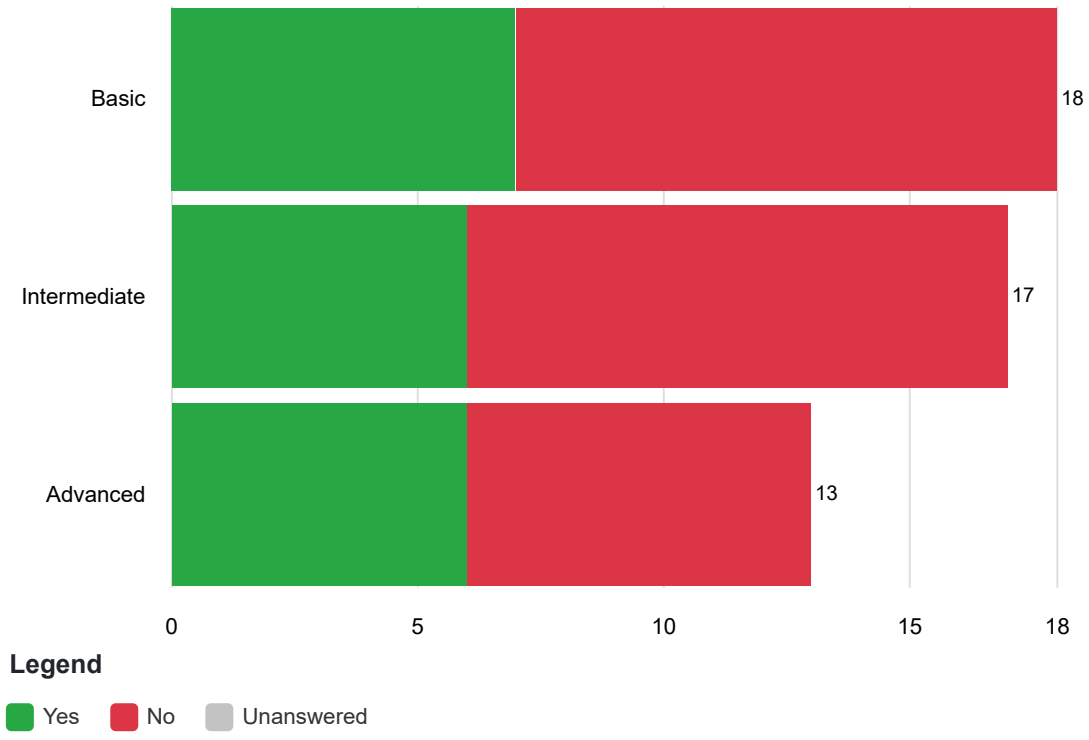
Goal Completion Summary



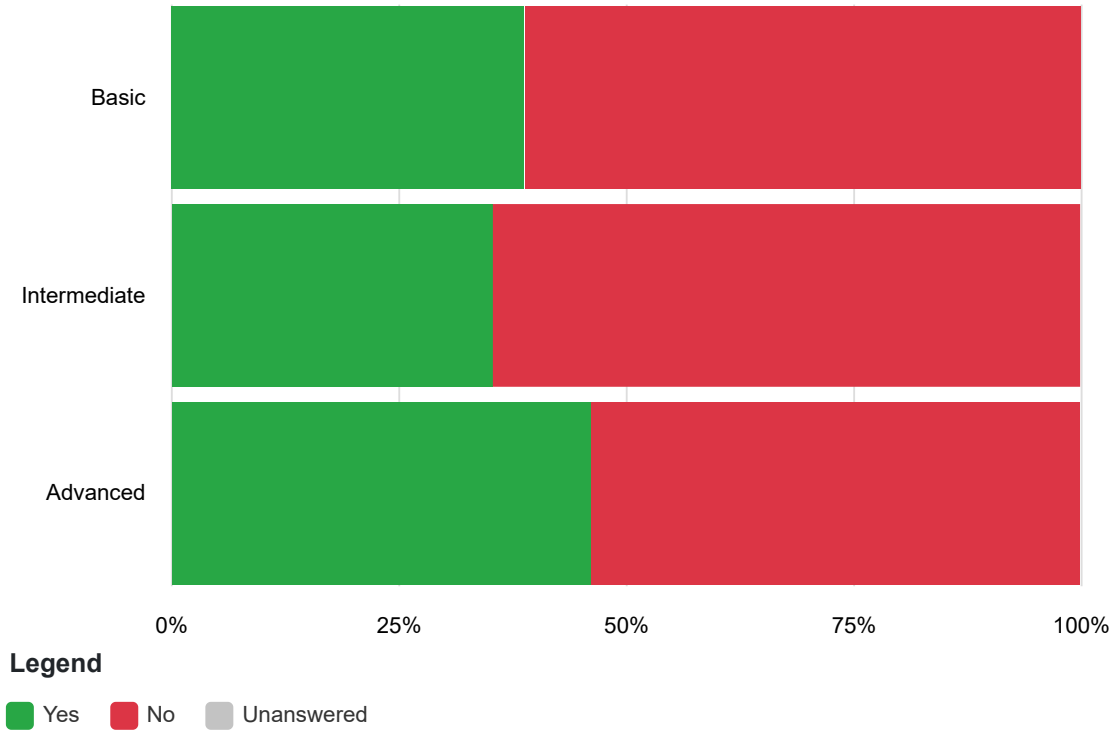
RRA Assessment Tiers



Practices Answered Per Tier



Practices Distribution Per Tier



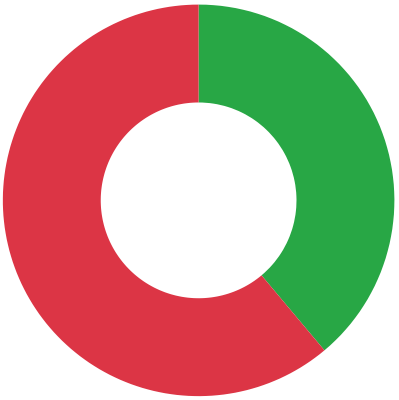
RRA Performance Summary

The RRA Performance Summary charts illustrate the distribution percentage of each response type overall and across all tiers.

Overall

- 40% Yes
- 60% No
- 0% Unanswered

Basic

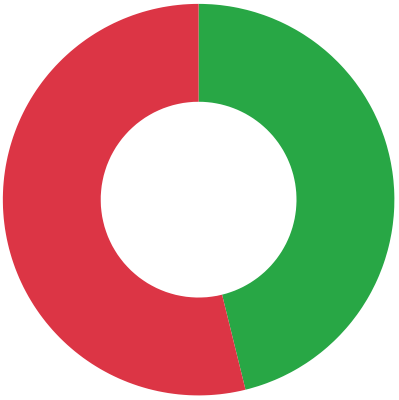


- 39% Yes
- 61% No
- 0% Unanswered

Intermediate

- 35% Yes
- 65% No
- 0% Unanswered

Advanced



- 46% Yes
- 54% No
- 0% Unanswered

RRA Practice List with Corresponding References

Red-shaded rows indicate practices that have been answered as 'No' or left unanswered.

Identifier	Practice	References
DB:B.Q01	Are important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-1, CP-2, CP-9, CP-10 NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle. CIS Control 11 - Data Recovery: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state. Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain, and Test Backup Files, National Cybersecurity Center of Excellence (NCCoE), 2020.

		CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process.
DB:B.Q02	Are data backups tested annually?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-1, CP-2, CP-9, CP-10 NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle. CIS Control 11 - Data Recovery: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state. Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain, and Test Backup Files, National Cybersecurity Center of Excellence (NCCoE), 2020. CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for

		organizations seeking help in establishing an asset management process. NIST Special Publication 800-81-2, Secure Domain Name System (DNS) Deployment Guide: The Domain Name System (DNS) is a distributed computing system that enables access to Internet resources by user-friendly domain names rather than IP addresses, by translating domain names to IP addresses and back. This document provides: deployment guidelines for securing DNS within an enterprise; guidance on maintaining data integrity and performing source authentication; guidelines for configuring DNS deployments to prevent many denial-of-service attacks that exploit vulnerabilities in various DNS components.
BM:B.Q01	Is malicious web content being blocked using DNS filtering via methods like DNS resolvers and DNS firewalls?	CIS Control 9 - Email and Web Browser Protections: Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement. Selecting a Protective DNS Service: National Security Agency, 2021. DNS protection – GCA Quad 9: Quad9 protects users from accessing known malicious websites, leveraging threat intelligence from multiple industry leaders. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. SC-7, SC-20, SC-21, SC-22, AC-4
BM:B.Q02	Are web browser security settings managed?	Steps to Secure Web Browsing, National Security Agency 2018: Identifies three mitigations in commonly-

		used web browsers that will ward off nearly all publicly known attacks. CIS Control 9 - Email and Web Browser Protections: Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. SC-7, SC-20, SC-21, SC-22, AC-4 Securing Your Web Browser, CISA: updated 2015.
PP:B.Q01	Are annual tabletop exercises that include phishing response scenarios conducted?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. AT-2, AT-3, CP-4, IR-3 NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities : This publication seeks to assist organizations in designing, developing, conducting, and evaluating a test, training, and exercise (TT&E) program and events in an effort to aid personnel in preparing for adverse situations involving IT.

		NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations. NIST SP 800-177 Revision 1, Trustworthy Email : This document gives recommendations and guidelines for enhancing trust in email. The primary audience includes enterprise email administrators, information security specialists and network managers. CISA and MS-ISAC Ransomware Guide : This guide provides best practices and recommendations for developing cyber incident response policies and procedures.
PP:B.Q02	Are users trained to recognize cyber threats like phishing?	Cyber Readiness Institute's Ransomware Playbook: How to prepare for, respond to, and recover from a ransomware attack. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. AT-2, AT-3
PP:B.Q03	Is email filtered to protect against malicious content?	NIST SP 800-177 Revision 1, Trustworthy Email : This document gives recommendations and guidelines for enhancing trust in email. The primary audience

		includes enterprise email administrators, information security specialists and network managers. CISA and MS-ISAC Ransomware Guide: This guide provides best practices and recommendations for developing cyber incident response policies and procedures. Cyber Readiness Institute's Ransomware Playbook: How to prepare for, respond to, and recover from a ransomware attack.
NM:B.Q01	Is perimeter network traffic monitored?	NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: The purpose of this guideline is to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate. CIS Control 13: Network Monitoring and Defense: Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base. CIS Control 12, Network Infrastructure Management: Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

		NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. SI-4 CRR Supplemental Resource Guide Volume 2, Controls Management Version 1.1: This guide is intended for organizations seeking help in establishing a controls management process. To outline this process, this document will use an approach common to many controls management standards and guidelines. The process areas described include: creating the controls management plan; defining the controls; analyzing and deploying the controls; assessing the controls.
NM:I.Q02	Is internal network traffic monitored?	NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: The purpose of this guideline is to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate.

		CIS Control 13: Network Monitoring and Defense : Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base. CIS Control 12, Network Infrastructure Management : Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. SI-4 CRR Supplemental Resource Guide Volume 2, Controls Management Version 1.1: This guide is intended for organizations seeking help in establishing a controls management process. To outline this process, this document will use an approach common to many controls management standards and guidelines. The process areas described include: creating the controls management plan; defining the controls; analyzing and deploying the controls; assessing the controls.
NM:I.Q03	Are networks segmented to protect	NIST Special Publication 800-125B, Secure Virtual Network Configuration for Virtual Machine (VM)

mission critical assets?	Protection: The virtual network configuration areas discussed in this document are network segmentation, network path redundancy, traffic control using firewalls, and VM traffic monitoring. This document analyzes the configuration options under these areas and presents a corresponding set of recommendations for secure virtual network configuration for VM protection.
	CIS Control 13: Network Monitoring and Defense: Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
	CIS Control 12, Network Infrastructure Management: Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.
	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. SI-4
	CRR Supplemental Resource Guide Volume 2, Controls Management Version 1.1: This guide is intended for organizations seeking help in establishing a controls management process. To outline this process, this document will use an approach common to many controls management standards and guidelines. The process areas described include: creating the controls management plan; defining the controls; analyzing and deploying the controls; assessing the controls.

NM:A.Q04	Has the organization established a baseline of network traffic and is it used to identify anomalous activity?	CIS Control 13: Network Monitoring and Defense: Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base. CIS Control 12, Network Infrastructure Management: Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. SI-4 CRR Supplemental Resource Guide Volume 2, Controls Management Version 1.1 : This guide is intended for organizations seeking help in establishing a controls management process. To outline this process, this document will use an approach common to many controls management standards and guidelines. The process areas described include: creating the controls management plan; defining the controls; analyzing and deploying the controls; assessing the controls. CRR Supplemental Resource Guide Volume 4, Vulnerability Management Version 1.1: This guide is intended for organizations seeking help in establishing a vulnerability management process. The process areas described include: developing a vulnerability analysis and resolution strategy; developing a vulnerability management plan; developing a vulnerability discovery capability; assessing the vulnerability management activities; managing exposure.

AM:B.Q01	Have the organization's hardware and software assets been inventoried and is the inventory managed?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-8
		NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: The purpose of this guideline is to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate. CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process. CIS Control 1: Inventory and Control of Enterprise Assets: Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying

		unauthorized and unmanaged assets to remove or remediate.
AM:B.Q02	Has the organization removed all unsupported hardware and software from its operating environment?	CIS Version 7, Implementation Guide for Industrial Control Systems: In this document, CIS provides guidance on how to apply the security best practices found in CIS Controls Version 7 to Industrial Control System environments. For each top-level CIS Control, there is a brief discussion of how to interpret and apply the CIS Control in such environments, along with any unique considerations or differences from common IT environments. CIS Control 1: Inventory and Control of Enterprise Assets: Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate. CIS Control 2: Inventory and Control of Software Assets: Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile

		attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. SA-22, PL-2, SA-3
AM:I.Q03	Does the organization detect rogue hardware and alert key stakeholders?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. IR-6 NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: The purpose of this guideline is to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate. CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process. CIS Control 1: Inventory and Control of Enterprise Assets: Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the

		enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.
AM:A.Q04	Does the organization quarantine and/or remove all rogue hardware?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-8 NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: The purpose of this guideline is to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate. CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process. CIS Control 1: Inventory and Control of Enterprise Assets: Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the

		enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.
AM:B.Q05	Are documented and approved secure configurations used to manage the organization's hardware and software assets?	NIST SP 800-70 Rev. 4, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers: A security configuration checklist is a document that contains instructions or procedures for configuring an information technology (IT) product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected. To facilitate development of checklists and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). This publication explains how to use the NCP to find and retrieve checklists, and it also describes the policies, procedures, and general requirements for participation in the NCP. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-2, CM-3, CM-6, CM-8 (2), CM-9 NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems: The focus of this document is on implementation of the information system security aspects of configuration management, and as such the term security-focused configuration management (SecCM) is used to emphasize the concentration on information security. The goal of SecCM activities is to manage and monitor

		the configurations of information systems to achieve adequate security and minimize organizational risk while supporting the desired business functionality and services. CRR Supplemental Resource Guide Volume 3, Configuration and Change Management Version 1.1: This guide is intended for organizations seeking help in establishing a configuration and change management process and for organizations seeking to improve their existing configuration and change management process. CIS Control 4: Secure Configuration of Enterprise Assets and Software: Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
AM:I.Q06	Are standard baseline images used to control hardware and software configurations?	NIST SP 800-70 Rev. 4, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers: A security configuration checklist is a document that contains instructions or procedures for configuring an information technology (IT) product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected. To facilitate development of checklists and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). This publication explains how to use the NCP to find and retrieve checklists, and it also describes the policies, procedures, and general requirements for participation in the NCP. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy

		controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-2, CM-3, CM-6, CM-8 (2), CM-9 NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems: The focus of this document is on implementation of the information system security aspects of configuration management, and as such the term security-focused configuration management (SecCM) is used to emphasize the concentration on information security. The goal of SecCM activities is to manage and monitor the configurations of information systems to achieve adequate security and minimize organizational risk while supporting the desired business functionality and services. CRR Supplemental Resource Guide Volume 3, Configuration and Change Management Version 1.1: This guide is intended for organizations seeking help in establishing a configuration and change management process and for organizations seeking to improve their existing configuration and change management process. CIS Control 4: Secure Configuration of Enterprise Assets and Software: Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
AM:A.Q07	Does the organization manage system configurations using security hardening guides?	NIST SP 800-70 Rev. 4, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers: A security configuration checklist is a document that contains instructions or procedures for configuring an information technology (IT) product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack

surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected. To facilitate development of checklists and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). This publication explains how to use the NCP to find and retrieve checklists, and it also describes the policies, procedures, and general requirements for participation in the NCP.

NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-6

NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems: The focus of this document is on implementation of the information system security aspects of configuration management, and as such the term security-focused configuration management (SecCM) is used to emphasize the concentration on information security. The goal of SecCM activities is to manage and monitor the configurations of information systems to achieve adequate security and minimize organizational risk while supporting the desired business functionality and services.

CRR Supplemental Resource Guide Volume 3, Configuration and Change Management Version 1.1: This guide is intended for organizations seeking help in establishing a configuration and change management process and for organizations seeking to improve their existing configuration and change management process.

		CIS Control 4: Secure Configuration of Enterprise Assets and Software: Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
PM:B.Q01	Is all public-facing software patched for vulnerabilities within 15 days for vulnerabilities rated as “Critical” and 30 days for vulnerabilities rated as “High”?	CIS Control 7, Continuous Vulnerability Management : Offers tips to help organizations maintain continuous vulnerability management to avoid compromised computer systems. CISA Binding Operational Directive 19-02: Ensures effective and timely remediation of critical and high vulnerabilities identified through Cyber Hygiene scanning. CISA Security Tip (ST04-006) Understanding Patches and Software Updates: Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features. NIST National Vulnerability Database: The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics. NIST Special Publication 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies: Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the

		challenges inherent in performing patch management. CIS Control 7, Continuous Vulnerability Management : Offers tips to help organizations maintain continuous vulnerability management to avoid compromised computer systems. CISA Binding Operational Directive 19-02: Ensures effective and timely remediation of critical and high vulnerabilities identified through Cyber Hygiene scanning. CISA Security Tip (ST04-006) Understanding Patches and Software Updates: Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features.
PM:B.Q02	Are all internal-facing software and firewalls patched for vulnerabilities within 30 days for both vulnerabilities rated as “Critical” and for vulnerabilities rated as “High”?	NIST National Vulnerability Database: The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics. NIST Special Publication 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies: Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management.
PM:I.Q03	Are all software and firewalls patched for vulnerabilities within	CIS Control 7: Offers tips to help organizations maintain continuous vulnerability management to avoid compromised computer systems.

	15 days for vulnerabilities rated as “Critical” and 30 days for vulnerabilities rated as “High”?	CISA Binding Operational Directive 19-02: Ensures effective and timely remediation of critical and high vulnerabilities identified through Cyber Hygiene scanning. CISA Security Tip (ST04-006) Understanding Patches and Software Updates: Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features. NIST National Vulnerability Database: The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics. NIST Special Publication 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies: Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management.
PM:A.Q04	Are all software and firewalls patched for vulnerabilities within 3 days for vulnerabilities rated as “Critical” and 7 days for vulnerabilities rated as “High”?	CIS Control 7: Offers tips to help organizations maintain continuous vulnerability management to avoid compromised computer systems. CISA Binding Operational Directive 19-02: Ensures effective and timely remediation of critical and high vulnerabilities identified through Cyber Hygiene scanning.

		CISA Security Tip (ST04-006) Understanding Patches and Software Updates: Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features. NIST National Vulnerability Database: The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics. NIST Special Publication 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies: Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management.
UM:B.Q01	Are strong and unique passwords implemented throughout the entire organization?	Back to basics: Multi-factor authentication (MFA): NIST Applied Cybersecurity Division, updated 2021. CISA Creating and Managing Strong Passwords: identifies six actions that users can take to create and manage strong passwords. Cyber Readiness Institute: The Cyber Readiness Program is a practical, step by-step guide to help small and medium-sized enterprises become cyber ready. Completing the Program will make your organization safer, more secure, and stronger in the face of cyber threats. The Program also provides customizable policy templates focused on human

		behavior that address phishing, patching, passwords/authentication, and USB use. CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process. Global Cyber Alliance Small Business Toolkit: provides tips and actions to keep your accounts safer by moving beyond simple passwords. Back to basics: Multi-factor authentication (MFA): NIST Applied Cybersecurity Division, updated 2021. NIST SP 1800-17, Cybersecurity Practice Guide: Multifactor Authentication for E-Commerce: This new Cybersecurity Practice Guide demonstrates how online retailers can implement open, standards-based technologies to enable Universal Second Factor (U2F) authentication by consumers at the time of purchase when risk thresholds are exceeded. The example implementations outlined in the guide encourage online retailers to adopt effective MFA implementations by using standard components and custom applications that are composed of open-source and commercially available components.
UM:I.Q02	Is two-factor authentication implemented for all privileged (e.g. system administrators) and remote users?	NSA Transition to Multi Factor Authentication: Outlines how to use Multi-factor Authentication to defend against an array of authentication attacks. CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process. Global Cyber Alliance Small Business Toolkit: Provides tips and actions to keep your accounts safer by moving beyond simple passwords.

		Back to basics: Multi-factor authentication (MFA): NIST Applied Cybersecurity Division, updated 2021.
UM:A.Q03	Is two-factor authentication implemented for all users?	NIST SP 1800-17, Cybersecurity Practice Guide: Multifactor Authentication for E-Commerce:This new Cybersecurity Practice Guide demonstrates how online retailers can implement open, standards-based technologies to enable Universal Second Factor (U2F) authentication by consumers at the time of purchase when risk thresholds are exceeded. The example implementations outlined in the guide encourage online retailers to adopt effective MFA implementations by using standard components and custom applications that are composed of open-source and commercially available components. NSA Transition to Multi Factor Authentication: Outlines how to use Multi-factor Authentication to defend against an array of authentication attacks. CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process. Cyber Readiness Institute's Ransomware Playbook: How to prepare for, respond to, and recover from a ransomware attack.
UM:B.Q04	Is the principle of least privilege enforced through policies and procedures?	CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process.
		Least Privilege, National Security Administration, IA Guidance Security Tips, 2017.
		Top Ten Cybersecurity Mitigation Strategies, National Security Administration, IA Guidance Security Tips, 2018.

		Defend Privileges and Accounts, National Security Administration, IA Guidance Security Tips, 2019.
		NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-5
		CRR Supplemental Resource Guide Volume 1, Asset Management Version 1.1 : This guide is intended for organizations seeking help in establishing an asset management process.
		Least Privilege, National Security Administration, IA Guidance Security Tips, 2017.
UM:I.Q05	Is least privilege enforced through technical (technology based) restrictions?	Top Ten Cybersecurity Mitigation Strategies, National Security Administration, IA Guidance Security Tips, 2018.
		Defend Privileges and Accounts, National Security Administration, IA Guidance Security Tips, 2019.
		NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-5
UM:I.Q06	Are audit logs maintained for all privileged (e.g.	NIST SP 800-92, Guide to Computer Security Log Management: This publication seeks to assist organizations in understanding the need for sound

system administrator) accounts?	computer security log management. It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in this publication covers several topics, including establishing log management infrastructures, and developing and performing robust log management processes throughout an organization.
	NIST SP 800-61 rev. 2, Computer Security Incident Handling Guide: This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.
	CIS Controls Version 8: The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.
	NIST SP 800-115, Technical Guide to Information Security Testing and Assessment: The purpose of this document is to assist organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies. The guide provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures.

		NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. AU-2, AU-3, AC-2 (7), AC-6 (9)
UM:A.Q07	Is role-based security training conducted?	NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide: This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. CIS Controls Version 8: The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment : The purpose of this document is to assist organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies. The guide provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures.

		NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. AT-3, PM-13
UM:I.Q08	Is rogue hardware being detected?	CIS Controls Version 8: The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment : The purpose of this document is to assist organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies. The guide provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-8

		NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide: This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.
UM:A.Q09	Are users who attempt to install rogue hardware counseled against installing rogue hardware?	CIS Controls Version 8: The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. AT-3 NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide: This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.
AI:B.Q01	Is there a list of known bad software (a “Blocklist”), and is	NIST SP 800-167 : Allowlisting: For more information on allowlists, this publication is intended to assist organizations in understanding the basics of application

	the software on that list being blocked?	allowlisting. It also explains planning and implementation for allowlisting technologies throughout the security deployment lifecycle. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-7(5) CIS Controls Version 8 : The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.
AI:I.Q02	Has the organization documented a list of known approved software (an “Allowlist”)?	NIST SP 800-167 : Allowlisting: For more information on allowlists, this publication is intended to assist organizations in understanding the basics of application allowlisting. It also explains planning and implementation for allowlisting technologies throughout the security deployment lifecycle. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-7 (5) CIS Controls Version 8 : The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.

		NIST SP 800-167 : Allowlisting: For more information on allowlists, this publication is intended to assist organizations in understanding the basics of application allowlisting. It also explains planning and implementation for allowlisting technologies throughout the security deployment lifecycle.
AI:I.Q03	Is the Allowlist organized by software publisher, and is that list used to allow only approved software to run on organizational systems?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-7 (5) CIS Controls Version 8 : The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.
AI:A.Q04	Has the organization documented a list of known approved software (an Allowlist) organized by software publisher and version number, and is that list used to allow only approved software to run on organizational systems?	NIST SP 800-167 : Allowlisting: For more information on allowlists, this publication is intended to assist organizations in understanding the basics of application allowlisting. It also explains planning and implementation for allowlisting technologies throughout the security deployment lifecycle. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-7(5)

		CIS Controls Version 8 : The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.
IR:B.Q01	Has the organization developed an incident response plan?	CISA and MS-ISAC Ransomware Guide : This guide provides best practices and recommendations for developing cyber incident response policies and procedures. CRR Supplemental Resource Guide Volume 5, Incident Management Version 1.1 : This guide is intended for organizations seeking help in establishing an incident management process and for organizations seeking to improve their existing incident management process. NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide: This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: this document provides guidance to evaluate information systems and to determine contingency planning requirements and priorities NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a

		diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. IR-8
IR:I.Q02	Are cybersecurity incidents reported and escalated to the appropriate stakeholders?	CISA and MS-ISAC Ransomware Guide : This guide provides best practices and recommendations for developing cyber incident response policies and procedures. CRR Supplemental Resource Guide Volume 5, Incident Management Version 1.1 : This guide is intended for organizations seeking help in establishing an incident management process and for organizations seeking to improve their existing incident management process. NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide: This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: this document provides guidance to evaluate information systems and to determine contingency planning requirements and priorities NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural

		failures, foreign intelligence entities, and privacy risks. IR-6 CISA and MS-ISAC Ransomware Guide : This guide provides best practices and recommendations for developing cyber incident response policies and procedures. CRR Supplemental Resource Guide Volume 5, Incident Management Version 1.1 : This guide is intended for organizations seeking help in establishing an incident management process and for organizations seeking to improve their existing incident management process.
IR:I.Q03	Have disaster recovery procedures been developed?	NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide: This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: this document provides guidance to evaluate information systems and to determine contingency planning requirements and priorities NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. IR-1, CP-1, CP-2

		CRR Supplemental Resource Guide Volume 5, Incident Management Version 1.1 : This guide is intended for organizations seeking help in establishing an incident management process and for organizations seeking to improve their existing incident management process.
IR:B.Q04	Does the organization conduct annual incident response tabletop exercises that include ransomware response scenarios?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-4, IR-3 CRR Supplemental Resource Guide Volume 5, Incident Management Version 1.1 : This guide is intended for organizations seeking help in establishing an incident management process and for organizations seeking to improve their existing incident management process.
IR:I.Q05	Are incident response tabletop exercises performed at least twice a year?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-4, IR-3
IR:I.Q06	Is a physical incident response exercise performed at least once a year?	CRR Supplemental Resource Guide Volume 5, Incident Management Version 1.1 : This guide is intended for organizations seeking help in establishing an incident management process and for organizations seeking to improve their existing incident management process.

		NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-4, IR-3, IR-4 CRR Supplemental Resource Guide Volume 5, Incident Management Version 1.1: This guide is intended for organizations seeking help in establishing an incident management process and for organizations seeking to improve their existing incident management process.
IR:A.Q07	Are physical incident response exercises performed at least twice a year?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-4, IR-3, IR-4
IR:I.Q08	Has the organization implemented redundant systems where appropriate for the purpose of resiliency?	NIST SP 800-160, Volume 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach: This publication can be viewed as a handbook for achieving identified cyber resiliency outcomes based on a systems engineering perspective on system life cycle processes in conjunction with risk management processes, allowing the experience and expertise of the organization to help determine what is correct for its purpose. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy

		controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-2, CP-7, CP-6, CP-8, CP-9, CP-10, MA-6
IR:A.Q09	Have redundant and resilient systems and data been implemented throughout the organization?	NIST Special Publication 800-160, Volume 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach: This publication can be viewed as a handbook for achieving identified cyber resiliency outcomes based on a systems engineering perspective on system life cycle processes in conjunction with risk management processes, allowing the experience and expertise of the organization to help determine what is correct for its purpose. NIST Special Publication SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6, SI-17
RM:I.Q01	Does the organization perform business impact assessments?	CRR Supplemental Resource Guide Volume 6, Service Continuity Management Version 1.1 : this publication provides guidance regarding service continuity planning as an important aspect of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made. See also Appendix A, Business Impact Analysis Template.

		CRR Supplemental Resource Guide Volume 7, Risk Management Version 1.1: this publication focuses on the processes by which an organization identifies, analyzes, and mitigates risks to affect the probability of their realization and/or the impact of a disruption. NIST Special Publication SP 800-184, Guide for Cybersecurity Event Recovery : this publication provides guidance regarding the planning, playbook developing, testing, and improvement of recovery planning. NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: this document provides guidance to evaluate information systems and to determine contingency planning requirements and priorities. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-2
RM:A.Q02	Has the organization defined organizational risk criteria and tolerances?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. PM-9, RA-3

		NIST SP 800-39 Managing Information Security Risk, Organization, Mission, and Information System View : The purpose of Special Publication 800-39 is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. CRR Supplemental Resource Guide Volume 7, Risk Management Version 1.1 : this publication focuses on the processes by which an organization identifies, analyzes, and mitigates risks to affect the probability of their realization and/or the impact of a disruption. CRR Supplemental Resource Guide Volume 6, Service Continuity Management Version 1.1 : this publication provides guidance regarding service continuity planning as an important aspect of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made.
RM:A.Q03	Does the organization consider risk inheritance and exposure between its various interconnected systems?	NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy : This publication describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. CRR Supplemental Resource Guide Volume 7, Risk Management Version 1.1: this publication focuses on the processes by which an organization identifies, analyzes, and mitigates risks to affect the probability of their realization and/or the impact of a disruption.

		CISA Security Tip (ST18-007) : Questions Every CEO Should Ask About Cyber Risks NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks, PM-9, CA-3. CRR Supplemental Resource Guide Volume 7, Risk Management Version 1.1 : This publication focuses on the processes by which an organization identifies, analyzes, and mitigates risks to affect the probability of their realization and/or the impact of a disruption.
RM:A.Q04	Does the organization apply quantitative risk analysis to remediation activities?	CISA Security Tip (ST18-007) : Questions Every CEO Should Ask About Cyber Risks NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations : The purpose of Special Publication 800-39 is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. See PM-9.