COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

INFORMATION TECHNOLOGY RISK MANAGEMENT STANDARD SEC520-05

Virginia Information Technologies Agency (VITA)
June 2024

ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this (or any applicable) ITRM publication, policy or standard. Questions or comments should be directed to the VITA *Enterprise* Architecture *(EA)* Division. EA will issue a Change Notice Alert, post it on the VITA Web site, and provide an e-mail announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties EA considers to be interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	02/12/2014	Base Document
v 00.1	12/08/2016	This administrative update is necessitated by changes in the Code of Virginia and organizational changes in VITA. No substantive changes were made to this document.
Revision 1	01/04/2019	Table of contents was updated to reflect changes in page numbers clarifying language added to: SEC 1 (Intent), 2.2 Framework Core, … A complete rewrite was performed with new requirements added: 2.4 Risk Maturity, 3.3.2 Requirements, 3.6.1 Purpose
Revision 2	05/05/2020	Quantitative Risk Analysis methodology added to standard. Updated language to 4.2 Business Impact Analysis, 4.3.2 IT System Inventory and Definition Requirements, 4.5.5 Reporting IT Risk Assessment Results, 4.7 Vulnerability Scanning, 4.7.2 Vulnerability Scanning Requirements, 4.7.3 Reporting IT Vulnerability Scan Results to VITA
Revision 2	10/01/2020	Vulnerability Scanning, 4.7.2
Revision 3	12/1/2021	Updated language to 2.0 Quantitative Risk changing the Center for Internet Security to 18 CIS Controls, 4.4 IT System and Data Sensitivity to match SEC530, 4.4.2, 2. to required data set template be attached to system security plan, 4.7.2 Vulnerability Scanning Requirements, and updated Appendix A, Risk Management Framework Core, to match new 18 CIS Controls.
Revision 4	4/1/2024	Update references from SEC501 and 525 to SEC530 throughout the document Reduced duplicate information between 530 and 520, withdrawing sections 4.4 and 4.7.2. Clarified risk assessment requirements and reporting requirements in 4.5. Update the tables in the appendix b to align more closely with CSRM terminology
Revision 5	*6/1/2024*	*Rewrote section 4.7.2 to clarify requirements from SEC 530.*

Identifying Changes in This Document

- See the latest entry in the table above
- Vertical lines in the left margin indicate that the paragraph has changes or additions.
- Specific changes in wording are noted using italics and underlines; with italics only indicating new/added language and italics that is underlined indicating language that has changed.

The following examples demonstrate how the reader may identify updates and changes:

Example with no change to text – The text is the same. The text is the same. The text is the same.

Example with revised text – This text is the same. *A wording change, update or clarification has been made in this text.*

Example of new section – *This section of text is new.*

Review Process

Enterprise Architecture (EA) Division provided the initial review of this publication.

Online Review

All Commonwealth agencies, stakeholders, and the public were encouraged to provide their comments through the Online Review and Comment Application (ORCA). All comments were evaluated and individuals that provided comments were notified of the action taken.

PREFACE

Publication Designation
COV ITRM Standard SEC520-05

Subject
Information Technology Risk Management Standard

Effective Date
June 7, 2024

Compliance Date
June 10, 2024

Scheduled VITA Review:
One (1) year from the effective date, then every two years thereafter.

Authority
Code of Virginia, §2.2-2009
(Additional Powers of the CIO relating to security)

Scope
This standard is applicable to all executive branch agencies, independent agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology databases or data communications in the Commonwealth. However, academic "instruction or research" systems are exempt from this Standard. This exemption, does not, however, relieve these academic "instruction or research" systems from meeting the requirements of any other State or Federal Law or Act to which they are subject.

Purpose
This standard delineates the methodology and requirements for creating an agency risk management program for IT systems that contain information as identified and prioritized in an Agency's Business Impact Analysis.

General Responsibilities
(*Italics indicate quote from the Code of Virginia requirements*)

Chief Information Officer of the Commonwealth (CIO)
Develops and *approves* statewide technical and data policies,
standards and guidelines for information technology and related systems.

Chief Information Security Officer
The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's information technology systems and data.

Virginia Information Technologies Agency (VITA)
At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts, reviewing procurement requests, agency IT projects, budget requests and strategic plans, and when developing and managing IT related services.

Executive Branch Agencies

Provide input and review during the development, adoption and update of commonwealth technical and data policies, standards and guidelines for information technology and related systems. Comply with the requirements established by COV policies and standards. Apply for exceptions to requirements when necessary.

Definitions
Definitions are found in the single comprehensive glossary that supports Commonwealth Information Technology Resource Management (ITRM) documents (COV IT Glossary).

Related ITRM Policies, Standards, and Guidelines
Commonwealth of Virginia Information Technology Security Policy (ITRM Policy *SEC519-*)
Commonwealth of Virginia Information Technology Security Standard (ITRM Standard SEC530)

TABLE OF CONTENTS

1. INTRODUCTION

Intent

The *Information Technology Risk Management Standard* (SEC520) establishes a risk management framework with minimum program activities applicable to Commonwealth of Virginia (COV) agencies (the term "agency" or "agencies" in this standard include commonwealth agencies, universities, commissions and boards as defined under Code of Virginia §2.2-2009 et. Seq). Risk management activities include, but are not limited to, regulatory requirements that an agency is subject to, information security best practices, and requirements defined in this Standard. These risk management activities will provide identification of sensitive system risks, their associated business impact, and a remediation/recommendation strategy that will help mitigate risks to agency information systems and data. The Risk Management Framework aligns with the methods set forth by the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

This Standard defines the minimum acceptable level of information risk management program activities and data objects required for COV agencies that are in Scope to this Standard. As used in this Standard, the term "sensitivity" encompasses the elements of confidentiality, integrity, and availability. (Ref. SEC530*)*

Each agency shall implement an effective risk management program to identify and mitigate security gaps that threaten information or IT systems. The risk management program evaluates an agency's environment by inspecting, verifying, and reviewing the extent of compliance with established security practices, processes, standards and procedures. The Information Technology Security Audit Standard (SEC502) requires that all audit results and corrective action plans be included in the agency risk management program and subsequently reported to VITA.

Authority

Code of Virginia, §2.2-2009
(Additional Powers of the CIO relating to security)

Compliance

In the event that an agency does not comply with this ITRM IT Risk Management Standard, the CIO may exercise statutory authority to limit additional technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

2. QUANTITATIVE RISK ANALYSIS

The Commonwealth performs quantitative risk analysis (QA) to determine the potential financial impact of a commonwealth system compromise due to loss of availability, integrity or confidentiality. Reputational risk is represented by the number of citizens impacted by an event. This analysis estimates resources associated with the detection, response, and recovery activities associated with cyber security incidents within the Commonwealth executive branch, independent agencies and institutions of higher education.

The QA methodology leverages The 18 Center for Internet Security (CIS) Critical Security Controls, SEC530 and SEC530 controls to set the baseline establishing the acceptable level of agency cyber hygiene. This baseline establishes the potential risk incurred by an agency based on the inventory of controls in place and allows each application to be measured for impact of a loss event. Residual risk potentially incurred by the Commonwealth is identified by any missing controls. Each missing control increases the quantity of risk the agency experiences, and thus the likely cost of a loss event. The overall loss event cost is estimated based on industry trends and Commonwealth costs. Both direct and indirect costs are included in the total calculation of a loss event in order to determine a final cost of the event.

The QA methodology assists agencies in evaluating and forecasting risk based on security control modifications. With the QA methodology agencies are better able to define their organizational risk posture by the identified residual risk and further determine their appropriate risk appetite to best be able to maintain aggregate liability within the CSRM set agency target boundaries. CSRM sets risk boundaries which agencies cannot exceed without an approved CSRM exception.

2.1 Requirements

Each agency ISO shall:

1. Identify residual risk in the performance of issue management such as exceptions, remediation plans, Operational Risks and Issues (ORI) and are assessed with the QA methodology to determine residual risk.
2. IT Procurements use QA methodology to assess the level of liability.

3. RISK MANAGEMENT FRAMEWORK

This standard (SEC520) defines the Commonwealth Risk Management Framework (Framework) as it applies to agencies, universities, commissions, boards and other legal entities as defined in Code of Virginia, §2.2-2009 et. Seq. The Commonwealth Framework is consistent with the National Institute of Standards and Technology (NIST) Risk Management Framework for Information Systems and Organizations (NIST SP800-37 Rev2) and the Framework for Improving Critical Infrastructure Cybersecurity (CSF, Version 1.1 Dated: April 16, 2018).

3.1 Methodology

The Commonwealth Risk Management Framework provides a uniform approach to assessing, quantifying and managing information technology risk within the Commonwealth. The Framework assists by describing how the agency's risk management program supports the achievement of its objectives and is integrated into the agency's business processes. The framework provides measurable metrics to executive leadership within the Commonwealth in order to assess and quantify current IT risk levels as well as assist in the prioritization of actions for reducing risks to acceptable levels.

The Risk Management Framework provides a common method to:

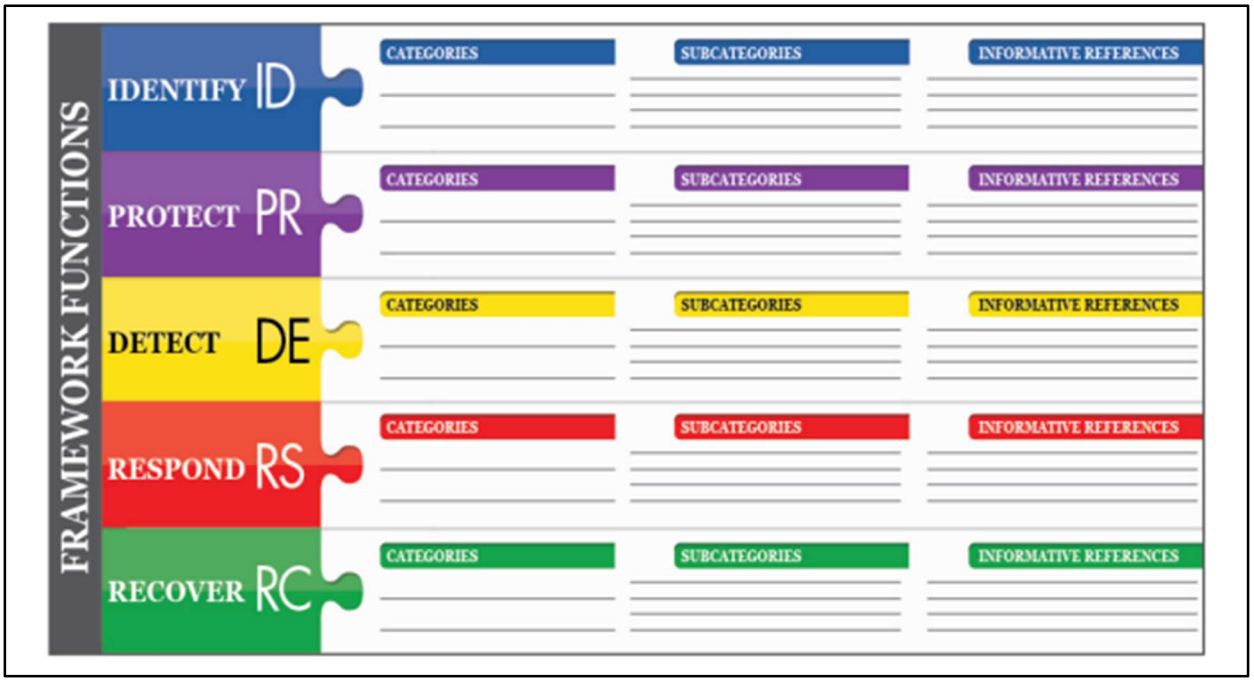
1. Describe current risk management posture;
2. Describe target risk management state;
3. Identify and prioritize opportunities for improvement within information security and risk management programs;
4. Assess progress toward the target risk state;
5. Quantify cybersecurity risk to determine potential financial impact to agency or Commonwealth;
6. Report risk management metrics and activities.

3.2 Framework Core

The Risk Management Framework Core consists of four elements: Functions, Categories, Subcategories, and Informative References. The Framework Core provides guidance to risk management activities conducted within the Commonwealth.

The Framework Core provides key personnel the ability to prioritize resources in order to reduce risks, defend against threats, and respond and recover from information security events that potentially impact public safety, confidential citizen data, finances, and/or the ability of Commonwealth agencies to perform their missions.

Figure 1: Framework Core Structure (Source NIST CSF)



Functions: The Risk Management Framework Core utilizes a methodology in which risk management activities comprise of five primary functions. These functions are: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. Organizing risk management activities according to these primary functions enables the information security and risk management community, as well as executive leadership, the ability to

better understand current risk and threat levels. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an agency's management of risk.

Categories: Categories are subdivisions of the primary core functions. Categories are closely tied to the processes that comprise the information security programs within the Commonwealth. The categories enable risks to be aggregated and reported upon so that material risks can be shared with senior management to support decision making. Examples of categories include, but are not limited to Asset Management, Access Control, Protective Technology, Detection Processes, Response Planning, and Recovery Planning.

Subcategories: Subcategories further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of subcategories include "Physical devices and systems within the organization are inventoried," "Data-at-rest is protected," and "Response Plan is executed during or after an event." Each subcategory is supported by one or more *Informative References*.

Informative References: Informative References are specific controls or sections from within standards, guidelines, and practices common across the Commonwealth and industry partner entities that illustrate specific methods or requirements to accomplish the activities described within the subcategories. Informative references may include controls from numerous private industry standards in order to facilitate communications and understanding between Government and private sector partners, specifically partners providing critical infrastructure services within the Commonwealth.

Examples of Government and industry standards include (but are not limited to) controls identified within this Risk Management Standard (SEC 520), the Commonwealth Information Security Standard (SEC 530), Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 5), Control Objective for Information and Related Technology (COBIT), Security for Industrial Automation and Control Systems (ISA/IEC 62443), and Center for Internet Security (CIS) Critical Security Controls (CIS Controls).

3.2.1 Framework Functions

The Risk Management Framework Functions are groups of information security and risk management activities that are grouped in a manner which focuses on five core functions. The five Framework Core Functions are Identify, Protect, Detect, Respond and Recover which are defined below. The assessment of each of the Functions can be performed concurrently and continuously to form an operational culture that addresses risk. See Appendix A for the entire Risk Management Framework Core inclusive of Functions, Categories, Subcategories and Informative References.

Identify: Develop the institutional understanding to manage the information security risks to the agency's IT systems, assets, data, and the business functions necessary to accomplish the Commonwealth agency missions.

> Activities include identification of the agency's business functions, the IT systems and assets that the business functions rely on, determine the impacts in the event that the business functions are compromised in relation to confidentiality, integrity, and/or availability, and determine the amount of time a business process could be nonfunctional. The Identify function includes the following categories Asset Management and Risk Assessment. The Identify function is the foundation for the effective implementation of the Risk Management Framework.

Protect: Develop and implement the appropriate safeguards, prioritized through the agency's risk management program to ensure the continued operation of the agency's business functions. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

The Protect function includes the following categories: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, and Protective Technology.

Detect: Develop and implement the appropriate activities to identify the occurrence of an information security event. The Detect Function enables timely discovery of cybersecurity events to limit or contain the impact of potential information security events.

The Detect function includes the following categories: Security Continuous Monitoring and Detection Processes.

Respond: Develop and implement the appropriate activities, prioritized through the organizations risk management process, to take action regarding a detected information security event. The Respond function supports the ability to contain the impact of a potential cybersecurity incident.

The Respond function includes the following category: Response Planning.

Recover: Develop and implement the appropriate activities, prioritized through the organizations risk management process, to take action regarding an identified cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

The Recover function includes the following category: Recovery Planning

3.3 Framework Profile

Framework Profiles are an agency's alignment of their requirements and objectives against the desired outcomes of the Framework Core functions. A Profile enables agencies to establish a roadmap for reducing risk while remaining aligned with agency and Commonwealth goals, considering legal/regulatory requirements and industry best practices, and recognizing risk management priorities. Profiles can be used to describe the current state or the desired target state of specific risk management activities. The current profile indicates the state of the information security program that are currently being achieved based on the assessment of the five core framework functions, their categories and subcategories. The framework profile results for Commonwealth agencies are included in the annual review to reflect the extent to which security standards and guidelines have been adopted by state agencies.

Comparison of Profiles (current state versus target state) may reveal gaps to be addressed with risk management objectives. An action plan to address these gaps, focused on a specific category or subcategory can enhance the agency's state of security to achieve the target risk profile. This risk-based approach allows agencies to prioritize risk measures and gauge resource requirements.

3.4 Risk Maturity and Profile Reporting

Risk Maturity provides context on how an organization views IT risk, security resources and processes in place to manage organizational IT risk. The result is a measurement of an organization's current risk

management program in relation to the desired implementation of risk management processes. Risk maturity results for COV agencies are included in the annual review of the extent to which security standards and guidelines adopted and implemented by the agency.

A. Agencies shall participate (annually) in the National Cyber Security Review (NCSR) questionnaire distributed through the MS-ISAC LogicManager system. The NCSR is an annual self-assessment survey that evaluates agency and COV cybersecurity maturity. The question set covers the core NIST Cybersecurity Framework components allowing agencies to measure progress against the NIST framework and peer agencies. The output metrics from the NCSR survey provides a risk maturity level assessment and progress toward enhanced cybersecurity and risk management programs.

B. When required, the CISO shall also prepare and distribute requirements and requests for information from the agencies. Agencies shall participate in such requests and provide the required information through the applicable format, most notably the eGRC system.

C. The Agency ISO shall perform a comprehensive review of agency cybersecurity policies according to §2.2-2009 (Section C) annually. The review shall assess the policy requirements based on continued compliance with current Commonwealth policies and standards. Deficiencies and gaps identified in the review shall be documented as findings and reported with corrective actions to the eGRC system. The reporting template for this is the Risk Treatment Plan template. https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

4. RISK MANAGEMENT REQUIREMENTS

4.1 Methodology

The following risk management activities are elements of the COV ITRM SEC530 Information Security Standard. Included in this standard is the Business Impact Analysis (BIA); IT System Inventory and Definition; IT System and Data Classification; Risk Assessment (RA); System Security Plan (SSP); Vulnerability Scanning; and Intrusion Detection System (IDS) Reporting.

4.2 Business Impact Analysis

4.2.1 Purpose

Business Impact Analysis (BIA) delineates the steps necessary for agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions.

> **Note:** The requirements below address only the IT and data aspects of a BIA and do not require agencies to develop a BIA separate from the BIA that could be used to develop an agency's Continuity Plan (previously referred to as Continuity of Operations Plan). Agencies should create a single BIA that meets both the requirements of this Standard and can be used to develop the agency Continuity Plan (previously referred to as Continuity of Operations Plan).

4.2.2 Requirements

Each agency should:

1. Require the participation of System Owners and Data Owners in the development of the agency's BIA.

2. Identify agency business functions.

3. Identify mission essential functions (MEFs).

Note: MEFs are functions that cannot be deferred during an emergency or disaster.

4. Identify dependent and supporting functions, known as primary business functions (PBFs), previously referred to as primary functions, on which each mission essential function (MEF) depends.

5. For each MEF and PBF, assess whether the function depends on an IT system to be recovered. Each IT system that is required to recover a MEF or PBF shall be considered sensitive relative to availability. For each such system, each agency shall:

    a. Document the required Recovery Time Objective (RTO), based on agency and COV goals, objectives, and MEFs, as outlined in the agency Continuity Plan.

    b. Document the Recovery Point Objectives (RPO) as outlined in the agency Continuity Plan.

    c. Identify the IT resources that support each MEF and PBF.

6. Use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification (Section 4), Risk Assessment (Section 6), Contingency Plan (Section CP-2) and System Security Plan (Section PL-2).

7. Conduct annual reviews of the agency BIAs, and conduct a full revision at least once every three years.

4.2.3 BIA / Business Process Reporting

The BIA (updated business process/functions as described above) shall be certified annually by the agency head and submitted to CSRM. The agency ISO shall submit the updated information in either of the following methods.

a. The BIA template provided to capture the required information. https://www.vita.virginia.gov/it-governance/itrm-policies-standards/ , or

b. Entered directly into the Commonwealth Security and Risk Management (CSRM) eGRC system.

4.3 IT System Inventory and Definition

4.3.1 Purpose

The agency shall develop and maintain a current IT System Inventory that includes appropriate detail to assess the business function and utilization of the system for operational and risk management needs. The IT System Inventory and Definition requirements identify the steps in listing and marking the

boundaries of sensitive IT systems in order to provide cost-effective, risk-based security protection for the agency and the Commonwealth enterprise.

This inventory shall be developed to include three primary elements of IT Systems and be maintained by the agency for reporting at least annually (more frequently as changes necessitate) to VITA in the eGRC system. The agency should develop and maintain the comprehensive IT System inventory to include (but not be limited to) devices (servers, workstations, etc.); data sets (databases, etc.) and applications/software that are the responsibility of the reporting agency.

4.3.2 Requirements

Each agency ISO, Designee or designated System Owner(s) shall ensure:

1. Document each IT system owned by the agency, including its ownership, network configuration, data flow and boundaries, facility sites sensitive relative to availability, number of concurrent users, and update the documentation as changes occur.

   Note: Data and homogeneous systems, belonging to a single agency, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.

   Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner for the purposes of this Standard, upon request, the CIO of the Commonwealth will determine the System Owner.

   Note: A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.

2. Multiple records which identify an individual in a system are counted as one unique individual record.

   Note: For a loss event, the QA methodology views records at risk as information that identifies the unique individual whose information has been compromised. By doing so, this limits the record at risk to just one unique individual regardless of how many records contain the individuals' information.

3. Maintain or require that its service provider maintain updated specifications, software versions, network diagrams, etc. on assets that support the agency system.

4.4 IT System and Data Sensitivity Classification

Withdrawn, incorporated into SEC530 Section 4. IT System and Data Classification. (https://www.vita.virginia.gov/policy--governance/policies-standards--guidelines/)

4.5 Risk Assessment (RA)

4.5.1 Purpose

Risk Assessment (RA) requirements delineate the steps agencies must take for each IT system classified as sensitive to:

- Identify potential threats to the confidentiality, integrity, and availability of an IT system and the environment in which it operates;
- Determine the likelihood that threats will materialize;
- Identify and evaluate vulnerabilities; and
- Determine the impact if one or more vulnerabilities are exploited by a potential threat.

4.5.2 Risk Assessment Planning

Annually, each Agency shall develop a risk assessment plan, and as necessary, update an existing one for the IT systems for which it is the System or Data Owner. The risk assessment plan shall be risk-based (to include the BIA, sensitivity classifications, etc.). Each Agency Head shall submit the Agency risk assessment plan (or approval of the risk assessment plan) to the CISO, annually.

Agencies are required to submit their plans using the Risk Assessment Plan Template found at: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/ unless an alternative is approved by the CISO.

The Risk Assessment Plan Template includes the following fields:

- Agency Information,
- Contact Information,
- The system full name and abbreviation,
- The planned assessor,
- The date the last risk assessment was conducted for the system, and
- Scheduled risk assessment completion date.

Note: Scheduled assessment completion date is the planned date of the completion of the future risk assessment covering a three-year period from the submission date.

4.5.3 Performance of Risk Assessments

For each IT system classified as sensitive, the data-owning agency shall:

a. Conduct and document a Risk Assessment (RA) of the IT system as needed, but not less than once every three years. Determine and document the most appropriate methodology for assessing the controls based on agency risk and maturity. The RA shall use, at a minimum, all controls from COV SEC530. Examples of risk assessment control questions provided in **Appendix A**. The agency ISO is responsible for documenting the methodology, assessment, results and corrective actions (risk treatment) to the CISO.

b. Conduct and document an annual *review of the assessment* to determine the continued validity of the RA. Send updates to the annual assessment to CISO *with agency head approval*.

c. Risks identified in the risk assessment with a *severity* greater than a value of low create a risk finding.

***Note:** Residual risks are calculated based on the data from the risk assessment.

d. For each risk finding, a risk treatment plan shall be created using the Risk Treatment Plan template. https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

4.5.4 Reporting and Verification

a. Implementation

Until completion of all risk treatment plans, the responsible Agency Head or designee shall document and report, at least quarterly, progress toward the completion of the risk treatment plan to the CISO using the Risk Treatment Plan Template. https://www.vita.virginia.gov/it-governance/itrm-policies-standards/
The quarterly risk treatment (sometimes referred to as a corrective action plan update) update will report progress toward implementing outstanding risk treatments.

b. Verification

Upon completion of the risk treatment(s), the responsible Agency Head or designee shall verify and document implementation of the control (or corrective actions) required to mitigate the risk finding.

4.5.5 Reporting IT Risk Assessment Results (Findings)

The Agency Head or designee shall submit to the CISO the following information:

1. All completed IT Risk Assessments conducted by or on behalf of the Agency which shall include the following:

a. Summary of the assessment,
b. Name of assessor
c. IT System Name,
d. Start Date of Assessment,
e. End Date of Assessment,
f. Scope of assessment indicating the controls used, and
g. Risks identified during the assessment

2. Each risk identified in the risk assessment must contain:

a. IT System Name
b. Risk ID
c. Sensitivity rating (e.g. Confidentiality, Integrity and availability)
d. Date of risk assessment
e. Risk vulnerability family (e.g. SEC 530 control)
f. Vulnerabilities

g. Threats
h. Risk summary
i. Magnitude of impact (e.g. Low, Medium, High, Critical)
j. Controls in place (brief description)

3. For each risk identified with a severity greater than low, a Risk Treatment Plan, found at: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/,shall be submitted to the CISO within 30 days of the final risk assessment report, and the risk treatment plan shall include (at a minimum):

   a. IT System affected
   b. Authoritative source (e.g. SEC 530, enterprise policy, operating instruction)
   c. Control ID (e.g. SEC530 AC-01 Access Control Policy & Procedures)
   d. Date risk identified
   e. Risk summary
   f. Magnitude of impact (e.g. Low, Medium, High, Critical)
   g. Status
   h. Status Date
   i. Planned resolution
   j. Resolution due date

4. An updated risk treatment plan must be submitted quarterly (at the end of each quarter), until all risks have been remediated. All Risk Treatment Plans and quarterly updates submitted must have evidence of agency head approval. Agencies must use the Risk Treatment Plan Template or enter the quarterly updates in the CSRM eGRC application.

4.6 System Security Plan

4.6.1 Purpose

Security plans relate security requirements to a set of security controls and control enhancements for sensitive systems. Security plans also describe, at a high level, how the security controls and Control Enhancements for Sensitive Systems meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements.

1. Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of:

   a. All existing IT and planned IT security controls for the IT system, including a schedule for implementing planned controls;

   b. How these controls provide adequate mitigation of risks to which the IT system is subject.

2. Submit the IT System Security Plan to the Agency Head or designated ISO for approval.

3. Plan, document, and implement additional security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

4. All final approved System Security Plans for existing or newly activated IT systems are required to be submitted to CSRM using the System Security Plan online template provided to capture information. https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

4.7 Vulnerability Scanning

4.7.1 Purpose

Vulnerability scanning is the process of assessing computer hardware and software via automated tools designed for detecting vulnerabilities. Scanning requires authenticated administrative scans of networking appliances and equipment, servers and end-user workstations, and communications egress and end points. Scanning tools should detect potential weaknesses including security misconfiguration, software with missing patches or updates, injection flaws, data leakage, and all common well-known vulnerabilities. Periodic review and timely remediation of the vulnerabilities are a critical component of a strong risk management program. *This section expands upon the requirements present in SEC 530 (https://www.vita.virginia.gov/policy--governance/policies-standards--guidelines/)*

4.7.2 Requirements

The organization shall:

a. *Fix vulnerabilities within 30 days of a fix becoming available that are either:*
    1. *Rated as critical or high (CVSS V3 Score of 7-10) according to the National Vulnerability Database (NVD).*
    2. *Otherwise identified by CSRM*

b. *Remediate all other vulnerabilities within 90 days of a fix becoming available.*

c. *Acquire an approved security exception for the vulnerability should it not be remediated within the timeframes identified. Mitigating controls will be expected as part of this process.*

4.7.3 Reporting IT Vulnerability Scan Results to VITA

The organization shall:

a. Provide a copy of the vulnerability scan results

    NOTE: Agencies that use the VITA vulnerability scanning program and acquire services or system components from VITA are only required to provide corrective action plans for identified vulnerabilities. Vulnerability report results will be provided on an agency's behalf by VITA and service providers.

b. Document and submit corrective action plans for vulnerabilities and risks identified to the CISO quarterly using the risk treatment plan template and include the following:

An export from the vulnerability scanning tool (i.e. Nessus, Rapid 7, Accunetix, etc.) with the following information, at a minimum, must be submitted with the initial agency corrective action plan. The following information must be included in the corrective action plan submitted to Commonwealth Security for each system scanned:

1. Date of Scan,
2. Host Name,
3. IP,
4. DNS Entry (N/A if not available),
5. Vulnerability description,
6. Severity level/Risk Rating (high, medium, low),
7. Common Vulnerability and Exposure (CVE) reference,
8. Remediation action (e.g. what's needed … disable port, etc.),
9. Results of follow-up scan after remediation action is taken.

Note: If no vulnerabilities were identified in a vulnerability scan, agency should include N/A for fields requesting vulnerability information.

4.8 Intrusion Detection Systems (IDS)

4.8.1 Purpose

Intrusion Detection Systems are used to monitor incoming and outgoing network traffic for possible hostile attacks originating from outside the agency and, also system misuse or attacks originating from inside the agency. These systems can be either signature based or behavior based. These systems can provide valuable intelligence on:

- Severity of the attacks
- Type of attacks
- Origin of the attacks
- Protocols/services and ports being attacked

Using this information can allow agencies to take action to protect systems against these attacks.

4.8.2 Intrusion Detection System Reporting Requirements

Agencies shall provide Intrusion Detection System Reports to the CISO at the end of each quarter. IDS reports should provide the following information:

1. Name of Agency
2. Date Range for the Report (example: Jan 1st 2013 – March 31st, 2013)
3. Total number of attacks per month (example: Jan 2013 = 1,000,000, Feb 2013=1,500,000, March 2013= 1,250,000)
4. Top 10 high attacks & number of attacks seen (example: SSH Brute Force, total: 100 attacks)
5. Top 10 Source IPs
6. Top 10 Destination IPs
7. Top 10 countries of origin of attacks with percentages per month (example: Jan 2018: US – 80%, China =4%, Russia = 3%, Canada = 3%, U.K. = 3%, India=2%, Brazil=2%, Germany=2%, Ireland=2%, Sweden=2%)
8. Top 10 types of attacks (example: Denial of Service, Privilege Escalation)
9. Top 10 inbound attacks by protocol/service/port (http/www/80)
10. Top 10 outbound attacks by protocol/service/port (http/www/80)

Appendix A Risk Management Framework Core

Function	Category	Subcategory	RA Questions	Informative References
IDENTIFY (ID)	**Asset Management (AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **Q1: Are the agency assets that directly support this IT system Inventoried?** • **Q2: Are the personnel with responsibility for these assets documented?**	• **CIS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **SEC 530** 5.2, CM-8 • **NIST SP 800-53 Rev. 5** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **Q1: Are software license information and software version number documented, inventoried, and maintained?** • **Q2: Are agency applications documented and inventoried?**	• **CIS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **SEC 530** 5.2, CM-8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 5** CM-8
	Risk Assessment (RA): The organization	**ID.RA-1:** Asset vulnerabilities are	• **Q1: Is a process for identifying and analyzing vulnerabilities established and maintained?**	• **CIS CSC** 7

Function	Category	Subcategory	RA Questions	Informative References
	understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	identified and documented	• **Q2: Are vulnerability scans being performed in accordance to applicable policies, standards, and regulations?** • **Q3: Is logging enabled to record information about identified vulnerabilities and their resolution, in accordance with applicable policies, standards, and regulations?**	• **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **SEC 530** 6.2, CA-7, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • **NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
PROTECT (PR)	**Access Control (AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **Q1: Are user identities and credentials granted based on their role or approved level of access?** • **Q2: Are access requests reviewed and approved by system or data owner based on user role?**	• **CIS CSC** 6 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **SEC530** 8.1, AC-2, IA Family

Function	Category	Subcategory	RA Questions	Informative References
				• **NIST SP 800-53 Rev. 5** AC-2, IA Family
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• **Q1: Are user access permissions managed based on principle of least privilege and separation of duties?** • **Q2: Are user access permissions reviewed on a regular basis with a process to correct inconsistencies?** • **Q3: Are users identified who are granted read/write access to information based on integrity?**	• **CIS CSC** 6 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • **SEC530** 8.1, AC-2, AC-3, AC-5, AC-6 • **NIST SP 800-53 Rev. 5** AC-2, AC-3, AC-5, AC-6, AC-16
	Awareness and Training (AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies,	**PR.AT-1:** All users are informed and trained	• **Q1: Are all users trained on the confidentiality, integrity and availability of agency data?** • **Q2: Have staff (and contractors) been trained on their cyber security responsibilities as an agency employee?** • **Q3: Is security awareness training provided to all personnel on an annual schedule?** • **Q4: Have skill gaps been identified in personnel with assigned security roles and responsibilities?** • **Q5: Have training need been identified to address skill gaps in personnel with assigned security roles and responsibilities?**	• **CIS CSC** 14 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2 • **SEC530** 8.2, AT-2 • **NIST SP 800-53 Rev. 5** AT-2, PM-13

Function	Category	Subcategory	RA Questions	Informative References
	procedures, and agreements.		• **Q6: Are security awareness activities provided to all personnel?** • **Q7: Are security awareness activities scheduled, resources, and tracked? (i.e.: newsletters, posters, presentations, training courses)** • **Q8: Have personnel with assigned incident response duties been trained in communicating threat information?**	
		PR.AT-2: Privileged users understand roles & responsibilities	• **Q1: Is role based training provided to personnel with assigned security roles and responsibilities?**	• **CIS CSC** 14 • **COBIT 5** APO07.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **SEC530** 8.2, AT-3 • **NIST SP 800-53 Rev. 5** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• **Q1: Are third party stakeholders (suppliers, customers, partners) required to complete security awareness training, to include policies and procedures?**	• **CIS CSC** 15 • **COBIT 5** APO07.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **SEC530** 8.2, PS-7, SA-9 • **NIST SP 800-53 Rev. 5** PS-7, SA-9

Function	Category	Subcategory	RA Questions	Informative References
		PR.AT-4: Senior executives understand roles & responsibilities	• **Q1: have senior executives been trained in their assigned security roles and responsibilities?**	• **CIS CSC** 14 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **SEC530** 8.2, AT-3 • **NIST SP 800-53 Rev. 5** AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	• **Q1: Have physical security personnel received role based security awareness training?** • **Q2: Has responsibility for monitoring sources of threat information been assigned to specific roles? (physical security, technology administrators, asset owners)** • **Q3: Have threat monitoring procedures been implemented with specific staff assigned duties?** • **Q4: Have specific roles been assigned the authority and accountability for communicating threat information?** • **Q5: Have all personnel been trained in situational awareness and made aware of their role in reporting threats?**	• **CIS CSC** 4, 14 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **SEC530** 8.2, AT-3 • **NIST SP 800-53 Rev. 5** AT-3, PM-13
	Data Security (DS): Information and records (data) are managed consistent with the	**PR.DS-1:** Data-at-rest is protected	• **Q1: Have controls been implemented to protect data-at-rest? (encryption, access controls)**	• **CIS CSC** 3, 4 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06

Function	Category	Subcategory	RA Questions	Informative References
	organization's risk strategy to protect the confidentiality, integrity, and availability of information.			• **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **SEC530** SC-28 • **NIST SP 800-53 Rev. 5** SC-28
		PR.DS-2: Data-in-transit is protected	• **Q1: Have controls been implemented to protect data-in-transit? (encryption, randomized communication patterns)**	• **CIS CSC** 3, 4 • **COBIT 5** APO01.06, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **SEC530** SC-8 • **NIST SP 800-53 Rev. 5** SC-8
		PR.DS-4: Adequate capacity to ensure availability is maintained	• **Q1: Is capacity management and planning performed for assets? (measurement of current demand, test for anticipated demand, and gathering usage trends to predict expansion needs)**	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1 • **SEC 530** AU-4, CP-2 • **NIST SP 800-53 Rev. 5** AU-4, CP-2, SC-5
				• **CIS CSC** 4, 12

Function	Category	Subcategory	RA Questions	Informative References
	Information Protection Processes and Procedures (IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	• **Q1: Is configuration management performed on agency assets?** • **Q2: Are all modifications to agency assets analyzed and reviewed to determine their potential impact to agency services?** • **Q3: Do agency assets have configuration baselines? (software and application code, operating systems, hardware, firewall rulesets, routers and other network equipment)** • **Q4: Is approval obtained for proposed changes to configuration baselines?**	• **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **SEC 530** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 • **NIST SP 800-53 Rev. 5** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	• **Q1: Is a System Development Life cycle implemented to manage all agency systems?**	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • **SEC 530** SA-3, SA-8, SA-10, SA-11 • **NIST SP 800-53 Rev. 5** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
				• **CIS CSC** 8

Function	Category	Subcategory	RA Questions	Informative References
	Protective Technology (PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **Q1: Has audit logging been implemented with records documented and reviewed according to SEC530/SEC530 policy?**	• **COBIT 5** APO11.04 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **SEC 530** AU Family • **NIST SP 800-53 Rev. 5** AU Family
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	• **Q1: Are agency systems and assets configured to provide only essential capabilities and prohibit or restrict the use of unnecessary functions, ports, protocols, services, etc.?**	• **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13,

Function	Category	Subcategory	RA Questions	Informative References
				SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **SEC 530** AC-3, CM-7 • **NIST SP 800-53 Rev. 5** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	• **Q1: Have controls been implemented to protect communication and control networks? (control documents usage restrictions, configuration/connection requirements, and implementation guidance for remote access, wireless access)**	• **CIS CSC** 13 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **SEC 530** AC-4, AC-17, AC-18, CP-8, SC-7 • **NIST SP 800-53 Rev. 5** AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Security Continuous Monitoring (CM):** The information system and assets are monitored at	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **Q1: Are events detected and reported appropriately (to include cybersecurity events related to personnel activity,**	• **CIS CSC** 13 • **COBIT 5** DSS05.07

Function	Category	Subcategory	RA Questions	Informative References
	discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.		**network activity, the physical environment, and information)?**	• **ISA 62443-3-3:2013** SR 6.2 • **SEC 530** AC-2, CA-7, CM-3, SC-7, SI-4 • **NIST SP 800-53 Rev. 5** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-4: Malicious code is detected	• **Q1: Does the agency use a standard set of tools and/or methods to detect malicious code in information systems entry and exit points to detect and eradicate malicious code?**	• **CIS CSC** 10, 13 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1 • **SEC 530** SI-3 • **NIST SP 800-53 Rev. 5** SI-3
	Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	• **Q1: Does the agency have a documented incident management plan? (plan should address identification, analysis, and response to an incident)** • **Q2: Are roles and responsibilities from the incident management plan included in personnel job descriptions?** • **Q3: Have personnel been assigned to the roles and**	• **CIS CSC** 17 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1

Function	Category	Subcategory	RA Questions	Informative References
			responsibilities detailed in the incident management plan?	• **ISO/IEC 27001:2013** A.6.1.1 • **SEC 530** CA-7 • **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-14
RESPOND (RS)	**Response Planning (RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• **Q1: Are responses to declared incidents developed and implemented according to pre-defined procedures?**	• **COBIT 5** BAI01.10 • **CIS CSC** 17 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **SEC 530** CP-2, CP-10, IR-4, IR-8 • **NIST SP 800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	• **Q1: Have conditions been identified which will trigger the execution of the agency continuity plan?** • **Q2: Has the agency continuity plan been tested for this IT system?** • **Q3: Has related continuity plan training for this IT system been provided to designated personnel?**	• **CIS CSC** 17 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5 • **SEC 530** CP-10, IR-4, IR-8 • **NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8

Appendix B Threat, Vulnerability and Risk Definitions and Tables

Purpose:

The following definitions and tables are for organizational reference while performing the risk management functions within this standard.

Threat - any circumstance or event (human, physical, or environmental) with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and or denial of service by exploiting vulnerability and it may halt or disrupt any of the agency's critical business functions. When assessing the various threats it is important to consider what destruction a threat can cause. If the threat will cause minimal damage, its priority will be placed at a much lower level than one with severe consequences.

Vulnerability - a weakness in a process or technical control that exposes data or it's supporting systems to loss or harm. Vulnerabilities could exist in numerous areas including architectural design, business processes, hardware, software, system configurations, and poor internal controls. When assessing how susceptible an IT system is to exploitation, it is also necessary to consider how likely it is that a threat will occur.

Risk - the potential that an event may cause a material negative impact to an asset and is the overlap of a threat and vulnerability. Vulnerability with no associated threat will not result in a risk to the agency. All identified risks to sensitive processes and data, IT systems, and the performance of the agency's essential business functions were included in this assessment. Where applicable, the agency identified those instances where it accepts any residual risk.

Magnitude of Impact – the level of harm that an exploited vulnerability could cause the agency or Commonwealth.

Table 1. Magnitude of Impact

Rating	Impact Definition
Critical	Direct high impact such as mission essential functions unavailable and/or complete data breach of sensitive information.
High	Direct minimal impact such as a temporary suspension of services or the loss of a subset of information.
Moderate	Indirect high impact.
Low	Indirect minimal impact.

Effectiveness of Controls – the effectiveness of the agency's controls in reducing its risk.

Table 2. Probability of Occurrence

Rating	Probability of Occurrence
Critical	There are no other controls in place that mitigate the risk and existing threats capable of exploiting the gap.
High	Few, if any, Internal controls are in place to reduce the risk.
Moderate	Internal controls reduce the threat; however, additional controls should be implemented to further mitigate the risk where feasible.
Low	There are sufficient controls in place to substantially reduce the risk posed.

Severity – the impact of a threat based on the Probability of Occurrence and its expected Magnitude of Impact.

Table 3. Severity

Probability of Occurrence	Magnitude of Impact			
	Low	Moderate	High	Critical
Critical	High	High	Critical	Critical
High	Moderate	High	High	Critical
Moderate	Low	Moderate	High	High
Low	Low	Low	Moderate	High

TEMPLATES

Agencies are required, unless otherwise approved by the CISO, to use the templates found at:
https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

GLOSSARY OF SECURITY DEFINITIONS

As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page at:
https://www.vita.virginia.gov/it-governance/itrm-policies-standards/