

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management

INFORMATION TECHNOLOGY RISK MANAGEMENT STANDARD SEC520-01

Virginia Information Technologies Agency (VITA)
January 2019

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 PPA 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 1.1	03/21/2019	<i>This administrative change was in section 3.2.2. Requirements to clarify business impact analysis requirements</i>

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 Solutions and Governance Directorate Review

~~Policy, Practices, and Enterprise Architecture (PPA)~~ (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 SEC520-01.1

Subject

Information Technology Risk Management Standard

Effective Date

February 12, 2014 January 1, 2019

Compliance Date

February 12, 2014 March 1, 2019

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. ~~This Standard is offered only as guidance to local government entities.~~

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)

~~Secretary of Technology~~

~~Reviews and approves statewide technical and data policies, standards and guidelines for information technology and related systems recommended by the CIO.~~

Chief Information Officer of the Commonwealth (CIO)

Develops and approves recommends to the Secretary of Technology 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.

Information Technology Advisory Council (ITAC)

Advises the CIO ~~and Secretary of Technology~~ on the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Executive Branch Agencies

Provide input and review during the development, adoption and update of

statewide 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 ITRM 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 SEC501-10)

TABLE OF CONTENTS

ITRM PUBLICATION VERSION CONTROL.....	i
PREFACE.....	ii
1. INTRODUCTION	1
Intent.....	1
2. RISK MANAGEMENT FRAMEWORK	2
2.1 Methodology.....	2
2.2 Framework Core.....	2
2.2.1 Framework Functions.....	4
2.3 Framework Profile.....	5
2.4 Risk Maturity.....	6
3. RISK MANAGEMENT REQUIREMENTS.....	6
3.1 Methodology.....	6
3.2 Business Impact Analysis.....	6
3.2.1 Overview.....	6
3.2.2 Requirements.....	6
3.3 IT System and Data Sensitivity Classification.....	9
3.3.1 Purpose.....	9
3.3.2 Requirements.....	10
3.4 Risk Assessment (RA).....	11
3.4.1 Purpose.....	11
3.4.2 Risk Assessment Planning.....	12
3.4.3 Performance of Risk Assessments.....	12
3.4.4 Reporting and Verification.....	13
3.4.5 Reporting IT Risk Assessment Results to VITA.....	13
3.5 Sensitive IT System Inventory and Definition.....	12
3.5.1 Purpose.....	12
3.5.2 Requirements.....	12
3.6 System Security Plan.....	14
3.7 Vulnerability Scanning.....	15
3.7.1 Purpose.....	15
3.7.2 Requirements.....	15
3.7.3 Reporting IT Vulnerability Scan Results to VITA.....	16
3.8 Intrusion Detection Systems (IDS).....	16
3.8.1 Purpose.....	16
3.8.2 Intrusion Detection System Reporting Requirements.....	17
Appendix A Risk Management Framework Core.....	18
Appendix B Threat, Vulnerability and Risk Definitions and Tables.....	32

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. SEC501)

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. 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).

2.1 Methodology

The Commonwealth Risk Management Framework provides a uniform approach to assessing 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 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:

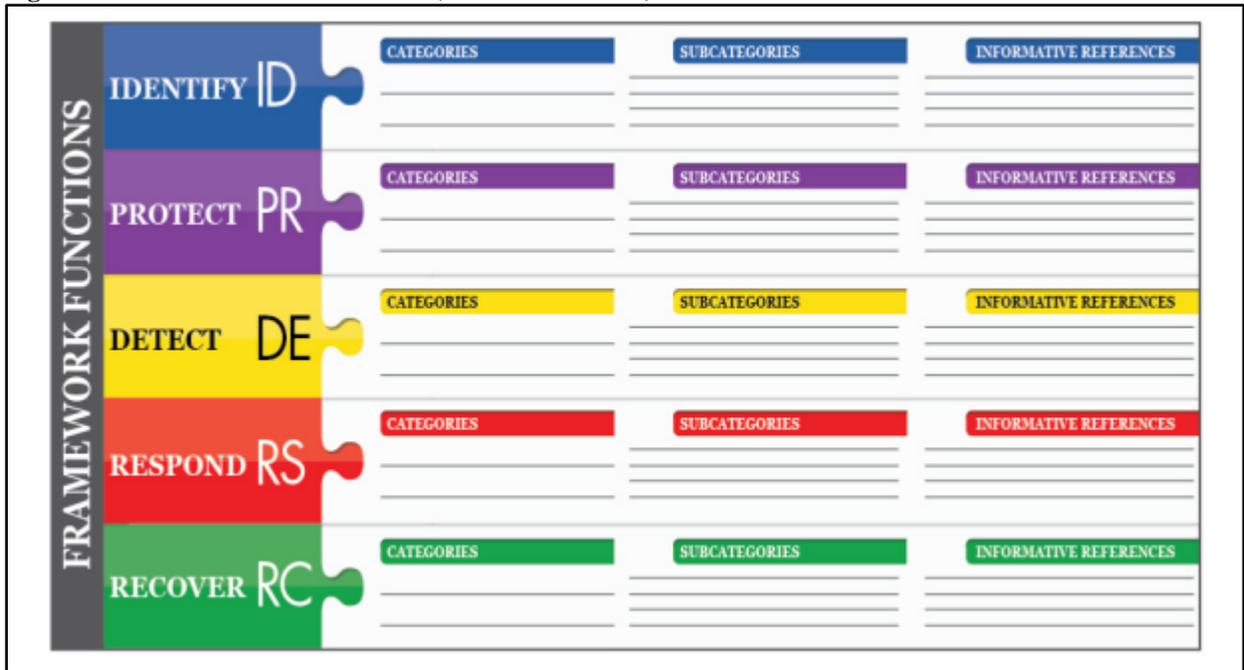
1. Describe current risk management posture;
2. Describe target risk management state;
3. Identify and prioritize opportunities for improvement within information security and risk management programs;
4. Assess progress toward the target risk state;
5. Report risk management metrics and activities.

2.2 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 501), Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 4), Control Objective for Information and Related Technology (COBIT), Security for Industrial Automation and Control Systems (ISA99.02.01), and Council on CyberSecurity (CCS) Top 20 Critical Controls (CSC).

2.2.1 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

2.3 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.

2.4 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 eGRC 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/>

3. RISK MANAGEMENT REQUIREMENTS

3.1 Methodology

The following risk management activities are elements of the COV ITRM SEC501 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.

3.2 Business Impact Analysis

3.2.1 Overview

Business Impact Analysis (BIA) defines a methodology for agencies to identify their organizational 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. Included within the BIA are elements that support subsequent risk functions such as data classification / sensitivity identification. The summation of these requirements provide one component as input to define, assess, and document Sensitive Systems.

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 a 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.

VDEM provides agency guidance on the development of Continuity Plans, and identification primary and mission essential functions.

3.2.2 Requirements

Each agency ISO shall submit the results of the review and revision of the agency BIA annually.

1. Require the participation of System Owners and Data Owners in the development of the agency's BIA.
2. Identify agency business processes/functions utilizing IT functions.
3. Identify mission essential functions (MEFs).

Note: VDEM defines Mission Essential Functions in "Guide to Identifying Mission Essential Functions (MEFs) and Conducting Business Process Analyses (BPAs)" and this definition is part of this requirement.

This states, "MEFs are functions that cannot be deferred during an emergency or disaster." ... "Mission essential functions (MEFs) are the limited set of department and agency level government functions that must be continued throughout, or resumed rapidly after, a disruption of normal operations."

4. Identify dependent and supporting processes/functions, known as primary business functions (PBFs) which each mission essential function (MEF) depends. VDEM states, "Primary Business Functions (PBFs) are the specific supporting activities that an agency or institution of higher education must conduct in order to perform its MEFs."
5. For each business process/function, assess whether the MEF or PBF depends on an IT system. Each IT system that is required to perform a MEF or PBF shall be identified "Sensitive" relative to Availability. The impact due to loss of the IT system shall also be assessed based on Confidentiality and Integrity.
6. ~~Using the information collected which provides the impact of non performance of the process/function; each process/function assessed based on Confidentiality, Integrity and Availability (CIA) using the following criteria. Categories used in the development of the BIA and subsequently for the sensitivity determination of the IT system include:~~
 - Recovery Time Objective (RTO) based on agency and COV goals, objectives, and MEFs, as outlined in the agency Continuity Plan
 - Recovery Point Objectives (RPO) consistent with the agency Continuity Plan
 - Business Process Name
 - Business Owner
 - Date BIA completed
 - Business Purpose
 - Business process customer, including internal to the agency, external agency customers, federal entity customers, locality customers and private entity customers, for example vendors
 - ~~Description of the data used as input to the business function~~
 - ~~The source of the data used by the function, internal external or external and internal to the agency~~
 - ~~The destination of the data provided by the function, internal, external or external and internal to the agency~~
 - The IT systems required by the function
 - Identify Mission Essential Functions (MEFs)
 - Impact to Confidentiality

- Impact to Customer Service
- Impact to Finances
- Impact to Life
- Impact to Safety
- Legal Impact
- Regulatory Impact
- ~~Applications on which the business process is reliant~~

The following criteria are used to determine the **C**onfidentiality, **I**ntegrity and **A**vailability (CIA) of a business process/function.

Attribute	Criteria
Confidentiality	Impact to Confidentiality
Integrity	Impact to Customer Service, Impact to Finance, Legal Impact, Regulatory Impact
Availability	Impact to Finance, Impact to Customer Service, Impact to Life, Impact to Safety NOTE: Any business process that has been identified as mission essential must be considered to have high availability.

Each IT system that is necessary to perform a business process/function that requires confidentiality, integrity, or availability is considered a Sensitive System.

3.2.3 BIA / Business Process Reporting

The BIA (updated business process/functions as described above) shall be certified annually by the agency head and submitted to CSRМ. 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 (CSRМ) eGRC system.

3.3 IT System Inventory and Definition

3.3.1 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 changed 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.

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

3.4 IT System and Data Sensitivity Classification

3.4.1 Purpose

IT System and Data Sensitivity Classification requirements identify the steps necessary to classify all IT systems and data according to their sensitivity with respect to the following three criteria:

- Confidentiality, which addresses sensitivity to unauthorized disclosure;
- Integrity, which addresses sensitivity to unauthorized modification; and
- Availability, which addresses sensitivity to accessibility or outages.

Sensitive data is any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Data sensitivity is directly proportional to the materiality of a compromise or loss of the data with respect to these criteria. Agencies must classify each IT system by sensitivity according to the most sensitive data that the IT system collects, stores, processes, manages, or transmits. The following template assists in compiling the necessary information to classify agency data sensitivity. <https://www.vita.virginia.gov/it-governance/itrm-policies-standards/> (Data Set Template)

3.4.2 Requirement

Each agency ISO shall:

1. Identify all agency devices and assets by entering inventory into the CSRM eGRC application.
 - a. Agencies that are not a customer of VITA services, or which are considered an independent agency and have IT systems that are not part of the Configuration Management Database (CMDB), including those agencies with a signed CIO exception for exclusion, are required to add all agency devices and assets inventory into the CSRM eGRC application.
2. Identify or require that the Data Owner identify all type(s) of data handled by each agency IT system.
3. Determine or require that the Data Owner determine whether each type of data is subject to other regulatory requirements.

Example: Some IT systems may handle data subject to legal or business requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); IRS 1075; the Privacy Act of 1974; Payment Card Industry (PCI); the Rehabilitation Act of 1973, § 508, Federal National Security Standards, etc.

4. Determine or require that the Data Owner determine the potential damages to the agency of a compromise of confidentiality, integrity or availability of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.

Example: Data Owners may construct a table similar to the following table. Data Owners must classify sensitivity requirements of all types of data. The following table is only an illustration of one way to accomplish this.

System ID:	Sensitivity Criteria		
Type of Data	Confidentiality	Integrity	Availability
HR Policies	Low	High	Moderate

Medical Records	High	High	High
Criminal Records	High	High	High

Table 1: Sample Sensitivity Analysis Results

- Classify the IT system as sensitive if any type of the data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability.

Recommendation: Agencies should classify IT systems as “sensitive” if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability. Documentation should be developed and maintained by the agency in cases where this determination is identified as “non-sensitive.”

- Review IT system and data classifications with the Agency Head (or designee) and obtain Agency Head or designee approval of these classifications.
- Verify and validate that all agency IT systems and data have been reviewed and classified as appropriate for sensitivity.
- Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users.
- Enter IT system and data sensitivity classification directly into the CSRM eGRC system. The agency (including those noted under Item 1.a above) shall ensure the information in eGRC is current and updated at least annually, or when substantive changes occur.
- Require that the agency prohibit posting any data classified as sensitive with respect to confidentiality on a public website, ftp server, drive share, bulletin board or any other publicly accessible media. Where an agency identifies a business case where this is a requirement, the agency shall submit to the CISO a written exception request approved by the Agency Head identifying the business case, risks, mitigating controls, and all residual risks. The CISO will determine whether the CoV exception should be granted and communicate to the agency.
- Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process defined in below and the Commonwealth SEC501 Standard.

3.5 Risk Assessment (RA)

3.5.1 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.

3.5.2 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.

3.5.3 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 controls from COV SEC501, COV SEC525, NIST Cybersecurity Framework as outlined in IT Risk Management Standard SEC520, or CIS Top 20 Critical Security Controls. 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 using the risk assessment/risk treatment template. (<https://www.vita.virginia.gov/it-governance/itrm-policies-standards/>).
- b. If the agency ISO completed the prior RA using a subset of the comprehensive controls, the subsequent scope shall incorporate both critical controls and those skipped in the prior year.

- c. Conduct and document an annual assessment to determine the continued validity of the RA. Send updates to the annual assessment to CISO.
- d. Risks identified in the risk assessment with a residual risk rating greater than a value of low create a risk finding.

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

- e. 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/>

3.5.4 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.

3.5.5 Reporting IT Risk Assessment Results (Findings)

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

1. A record of all *completed* IT Risk Assessments conducted by or on behalf of the Agency.
2. Agencies are required unless otherwise approved by the CISO to use the Risk Assessment Template found at: <https://www.vita.virginia.gov/it-governance/itrm-policies-standards/>
3. Each risk identified in the risk assessment template 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 501 control)

- f. Vulnerabilities
 - g. Threats
 - h. Risk Summary
 - i. Magnitude of impact (e.g. low, medium, high)
 - j. Controls in place (brief description)
4. For each risk identified with a residual risk greater than low, a Risk Treatment Plan 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 501, enterprise policy, operating instruction)
 - c. Control ID (e.g. AC-1)
 - d. Date risk identified
 - e. Risk summary
 - f. Risk rating (Low, Med-Low, Med, Med-High, High, Critical)
 - g. Status
 - h. Status Date
 - i. Planned resolution;
 - j. Resolution due date
5. An updated risk treatment plan must be submitted quarterly (at the end of the 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.

3 System Security Plan

3.6.1 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/>

3.7 Vulnerability Scanning

3.7.1 Purpose

Vulnerability scanning (also sometimes called vulnerability testing) assesses a network or an IT system to discover all potential weaknesses for an asset. A scanning tool is often used to determine what services the IT system is running and whether any unnecessary ports, operating system and applications, or back doors can be exploited because of a lack of patching or other flaw. **3.7.2 Requirements**

1. Each agency shall perform the following at least once every 90 days and when new vulnerabilities potentially affecting the systems/applications are identified and reported. Vulnerability scans shall be performed to include:
 - a. Vulnerabilities in information systems,
 - b. Hosted applications,
 - c. Patch levels,
 - d. Functions, ports, protocols, and services that should be inaccessible to users and devices,
 - e. Improperly configured enforcement mechanisms which control the flow of information between designated sources and destinations,
 - f. Web based applications.
2. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - a. Enumerating platforms, software flaws, and improper configurations;
 - b. Formatting checklists and test procedures; and
 - c. Measuring vulnerability impact;
3. Analyze vulnerability scan reports and results from security control assessments;
4. Remediate legitimate vulnerabilities within 90 days in accordance with an agency assessment of risk; and
5. Share information obtained from the vulnerability scanning process and security control assessments with the appropriate agency defined personnel to help eliminate

similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

3.7.3 Reporting IT Vulnerability Scan Results to VITA

Agencies that use the VITA vulnerability scanning program and are full service customer agencies are not required to report scan results to VITA. This will be done on your behalf by VITA and the service provider.

Agencies that *do not* use the VITA vulnerability scanning program and are full service customers, will only need to report risks identified in vulnerability scans to the CISO and include the following information:

1. Date of Scan
2. Host Name
3. IP or DNS Entry
4. Vulnerability description
5. Severity level/Risk Rating (high, medium, low)
6. Common Vulnerability and Exposure (CVE) reference
7. Remediation action (e.g. what's needed ... disable port, etc.)
8. Results of follow-up scan after remediation action is taken

For agencies that participate in the VITA vulnerability scanning program:
The data owning agency shall:

1. Document and report vulnerabilities and risks identified in the vulnerability scans and related remedial actions to CSRM once every 90 days.

Note: If no vulnerabilities were identified in a vulnerability scan, agency must notify CISO that the vulnerability scan was conducted and there were no findings.

For agency OS/Network Level Scanning, full service partnership agencies do not require additional reporting as this is done internally.

For agency OS/Network Level Scanning for non-partnership agencies:
The data owning agencies shall:

1. Submit evidence of periodic OS/Network scanning to the CISO.
 2. Tenable Nessus, Rapid 7 Nexpose, Qualys Guard Vulnerability Management are examples of scanning tools which produce this information and reports.

3.8 Intrusion Detection Systems (IDS)

3.8.1 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.

3.8.2 *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
<p>IDENTIFY (ID)</p>	<p>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.</p>	<p>ID.AM-1: Physical devices and systems within the organization are inventoried</p>	<ul style="list-style-type: none"> • Q1: Are the agency assets that directly support this IT system inventoried? • Q2: Are the personnel with responsibility for these assets documented? 	<ul style="list-style-type: none"> • CCS 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 501 5.2, CM-8 • NIST SP 800-53 Rev. 4 CM-8
		<p>ID.AM-2: Software platforms and applications within the organization are inventoried</p>	<ul style="list-style-type: none"> • Q1: Are software license information and software version number documented, inventoried, and maintained? • Q2: Are agency applications documented and inventoried? 	<ul style="list-style-type: none"> • CCS 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 501 5.2, CM-8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2

Function	Category	Subcategory	RA Questions	Informative References
	<p>Risk Assessment (RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>ID.RA-1: Asset vulnerabilities are identified and documented</p>	<ul style="list-style-type: none"> • Q1: Is a process for identifying and analyzing vulnerabilities established and maintained? • 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? 	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 CM-8 • CCS CSC 4 • 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 501 6.2, CA-7, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	<p>PROTECT (PR)</p>	<p>Access Control (AC): Access to assets and associated facilities is limited to authorized users, processes,</p>	<p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p>	<ul style="list-style-type: none"> • Q1: Are user identities and credentials granted based on their role or approved level of access? • Q2: Are access requests

Function	Category	Subcategory	RA Questions	Informative References
	or devices, and to authorized activities and transactions.		<p>reviewed and approved by system or data owner based on user role?</p>	<p>4.3.3.5.1</p> <ul style="list-style-type: none"> • 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 • SEC501 8.1, AC-2, IA Family • NIST SP 800-53 Rev. 4 AC-2, IA Family
		<p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties</p>	<ul style="list-style-type: none"> • 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? 	<ul style="list-style-type: none"> • CCS CSC 12, 15 • 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 • SEC501 8.1, AC-2, AC-3, AC-5, AC-6

Function	Category	Subcategory	RA Questions	Informative References
				<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
	<p>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, procedures, and agreements.</p>	<p>PR.AT-1: All users are informed and trained</p>	<ul style="list-style-type: none"> • 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? • 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? 	<ul style="list-style-type: none"> • CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • SEC501 8.2, AT-2 • NIST SP 800-53 Rev. 4 AT-2, PM-13
		<p>PR.AT-2: Privileged users understand</p>		<ul style="list-style-type: none"> • CCS CSC 9 • COBIT 5 APO07.02,

Function	Category	Subcategory	RA Questions	Informative References
		roles & responsibilities	<ul style="list-style-type: none"> • Q1: Is role based training provided to personnel with assigned security roles and responsibilities? 	DSS06.03 <ul style="list-style-type: none"> • 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 • SEC501 8.2, AT-3 • NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	<ul style="list-style-type: none"> • Q1: Are third party stakeholders (suppliers, customers, partners) required to complete security awareness training, to include policies and procedures? 	<ul style="list-style-type: none"> • CCS CSC 9 • 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 • SEC501 8.2, PS-7, SA-9 • NIST SP 800-53 Rev. 4 PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	<ul style="list-style-type: none"> • Q1: have senior executives been trained in their assigned security roles and responsibilities? 	<ul style="list-style-type: none"> • CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2

Function	Category	Subcategory	RA Questions	Informative References
				<ul style="list-style-type: none"> • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, • SEC501 8.2, AT-3 • NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	<ul style="list-style-type: none"> • 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? 	<ul style="list-style-type: none"> • CCS CSC 9 • 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, • SEC501 8.2, AT-3 • NIST SP 800-53 Rev. 4 AT-3, PM-13
	Data Security (DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality,	PR.DS-1: Data-at-rest is protected	<ul style="list-style-type: none"> • Q1: Have controls been implemented to protect data-at-rest? (encryption, access controls) 	<ul style="list-style-type: none"> • CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013

Function	Category	Subcategory	RA Questions	Informative References
	integrity, and availability of information.			A.8.2.3 • SEC501 SC-28 • NIST SP 800-53 Rev. 4 SC-28
		PR.DS-2: Data-in-transit is protected	• Q1: Have controls been implemented to protect data-in-transit? (encryption, randomized communication patterns)	• CCS CSC 17 • 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 • SEC501 SC-8 • NIST SP 800-53 Rev. 4 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 501 AU-4, CP-2 • NIST SP 800-53 Rev. 4

Function	Category	Subcategory	RA Questions	Informative References
	<p>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.</p>	<p>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained</p>	<ul style="list-style-type: none"> • 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? 	<p>AU-4, CP-2, SC-5</p> <ul style="list-style-type: none"> • CCS CSC 3, 10 • 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 501 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		<p>PR.IP-2: A System Development Life Cycle to manage systems is implemented</p>	<ul style="list-style-type: none"> • Q1: Is a System Development Life cycle implemented to manage all agency systems? 	<ul style="list-style-type: none"> • COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.3 • ISO/IEC 27001:2013

Function	Category	Subcategory	RA Questions	Informative References
				A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • SEC 501 SA-3, SA-8, SA-10, SA-11 • NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
	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 SEC501 policy?	• CCS CSC 14 • 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 501 AU Family • NIST SP 800-53 Rev. 4 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,	• COBIT 5 DSS05.02

Function	Category	Subcategory	RA Questions	Informative References
			<p>ports, protocols, services, etc.?</p>	<ul style="list-style-type: none"> • 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, 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 501 AC-3, CM-7 • NIST SP 800-53 Rev. 4 AC-3, CM-7
		<p>PR.PT-4: Communications and control networks are protected</p>	<ul style="list-style-type: none"> • Q1: Have controls been implemented to protect communication and control networks? (control documents usage restrictions, 	<ul style="list-style-type: none"> • CCS CSC 7 • COBIT 5 DSS05.02, APO13.01

Function	Category	Subcategory	RA Questions	Informative References
<p>DETECT (DE)</p>	<p>Security Continuous Monitoring (CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.</p>		<p>configuration/connection requirements, and implementation guidance for remote access, wireless access)</p>	<ul style="list-style-type: none"> • 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 501 AC-4, AC-17, AC-18, CP-8, SC-7 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
		<p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p> <p>DE.CM-4: Malicious</p>	<ul style="list-style-type: none"> • Q1: Are events detected and reported appropriately (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information)? 	<ul style="list-style-type: none"> • CCS CSC 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • SEC 501 AC-2, CA-7, CM-3, SC-7, SI-4 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 • CCS CSC 5

Function	Category	Subcategory	RA Questions	Informative References
		code is detected	<ul style="list-style-type: none"> • 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? 	<ul style="list-style-type: none"> • 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 501 SI-3 • NIST SP 800-53 Rev. 4 SI-3
	<p>Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.</p>	<p>DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability</p>	<ul style="list-style-type: none"> • 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 responsibilities detailed in the incident management plan? 	<ul style="list-style-type: none"> • CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1

Function	Category	Subcategory	RA Questions	Informative References
				<ul style="list-style-type: none"> • ISO/IEC 27001:2013 A.6.1.1 • SEC 501 CA-7 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
RESPOND (RS)	<p>Response Planning (RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.</p>	<p>RS.RP-1: Response plan is executed during or after an event</p>	<ul style="list-style-type: none"> • Q1: Are responses to declared incidents developed and implemented according to pre-defined procedures? 	<ul style="list-style-type: none"> • COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • SEC 501 CP-2, CP-10, IR-4, IR-8 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
RECOVER (RC)	<p>Recovery Planning (RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.</p>	<p>RC.RP-1: Recovery plan is executed during or after an event</p>	<ul style="list-style-type: none"> • 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? 	<ul style="list-style-type: none"> • CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • SEC 501 CP-10, IR-4, IR-8 • NIST SP 800-53 Rev. 4

Function	Category	Subcategory	RA Questions	Informative References
				CP-10, IR-4, IR-8

1

2 **Appendix B Threat, Vulnerability and Risk Definitions and Tables**

3

4 **Purpose:**

5

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

8

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

16

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

22

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

29

30 **Magnitude of Impact** - the level of harm that an exploited vulnerability could cause
31 the agency or Commonwealth.

32

33

34

Table 1. Magnitude of Impact

Rating	Impact Definition
Critical	Direct high impact and high likelihood of occurrence.
High	Direct minimal impact and high likelihood of occurrence OR direct high impact and minimal likelihood of occurrence.
Moderate	Indirect high impact and minimal likelihood of occurrence.
Low	Indirect minimal impact and minimal likelihood of occurrence

35

36

37 **Effectiveness of Controls** - the effectiveness of the agency’s controls in reducing its
 38 risk.

39
 40
 41

Table 2. Effectiveness of Controls

Rating	Control Impact Rating
High	Internal controls are sufficient to substantially reduce the risk to an acceptable level.
Moderate	Internal controls reduce the threat; however, additional controls should be implemented to further mitigate the risk where feasible.
Low	Few, if any, internal controls are in place to reduce the risk in any meaningful way. Additional controls should be implemented to mitigate the risk.

42
 43
 44
 45
 46
 47
 48
 49

Probability of Threat Occurrence - the likelihood of a threat exploiting a vulnerability based on the effectiveness of the internal control and its expected Magnitude of Impact.

Table 3. Probability of Threat Occurrence

Effectiveness of Controls	Magnitude of Impact			
	Low	Moderate	High	Critical
High	Low	Low	Moderate	High
Moderate	Low	Moderate	High	High
Low	Moderate	High	High	High

50
 51
 52
 53
 54
 55
 56
 57
 58
 59
 60
 61
 62
 63
 64
 65
 66
 67

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/>