

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management

INFORMATION TECHNOLOGY RISK MANAGEMENT STANDARD

Virginia Information Technologies Agency (VITA)

ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to the VITA Policy, Practice and Architecture (PPA) *Division*. PPA 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 considers to be interested in the change.

Version	Date	Purpose of Revision
Original	02/12/2014	Base Document

Review Process

The Policy, Practice, and Architecture (PPA) 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 carefully evaluated and individuals that provided comments were notified of the action taken.

PREFACE

Publication Designation

COV ITRM Standard SEC520-00

Subject

Information Technology Risk Management Standard

Effective Date

February 12, 2014

Compliance Date

February 12, 2014

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 for creating an agency risk management program for sensitive 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 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 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.

Enterprise Solutions and Governance Directorate

In accordance with the Code of Virginia § 2.2-2010 the CIO has assigned the Enterprise Solutions and Governance Directorate the following duties: Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions.”

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 *SEC519-00*)
Commonwealth of Virginia Information Technology Security Standard (ITRM Standard SEC501).

TABLE OF CONTENTS

ITRM PUBLICATION VERSION CONTROL	ii
PREFACE	iv
1. INTRODUCTION	1
Intent	1
2. RISK MANAGEMENT FRAMEWORK	2
2.1 Methodology	2
2.2 Framework Core	2
2.2.1 <i>Framework Functions</i>	3
2.3 Framework Profile	4
2.4 Risk Maturity	4
3. RISK MANAGEMENT REQUIREMENTS	5
3.1 Methodology	5
3.2 Business Impact Analysis	5
3.2.1 <i>Overview</i>	5
3.2.2 <i>Requirements</i>	5
3.3 Risk Assessment (RA)	7
3.3.1 <i>Purpose</i>	7
3.3.2 <i>Risk Assessment Planning</i>	7
3.3.3 <i>Performance of Risk Assessments</i>	7
3.3.4 <i>Reporting and Verification</i>	8
3.3.5 <i>Reporting IT Risk Assessment Results to VITA</i>	8
3.4 Vulnerability Scanning	9
3.4.1 <i>Purpose</i>	9
3.4.2 <i>Requirements</i>	9
3.4.3 <i>Reporting IT Vulnerability Scan Results to VITA</i>	10
3.5 Intrusion Detection Systems (IDS)	10
3.5.1 <i>Purpose</i>	10
3.5.2 <i>Intrusion Detection System Reporting Requirements</i>	10
Appendix A Risk Management Framework Core	11
Appendix B Threat, Vulnerability and Risk Definitions and Tables	18

1. INTRODUCTION

Intent

The intent of this *Information Risk Management Standard* is to establish a risk management framework, setting a baseline for information risk management activities for agencies across the Commonwealth of Virginia (COV). These risk management activities include, but are not limited to, any regulatory requirements that an agency is subject to, information security best practices, and the 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) Framework for Improving Critical Infrastructure Cybersecurity.

This *Standard* defines the minimum acceptable level of information risk management program activities and data objects required to assess those 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, RA-2)

In order to identify and mitigate IT security gaps that threaten government information or IT systems, each agency must implement a risk management program. The risk management program audits an agency's environment by inspecting, verifying, and reviewing the extent of compliance with established security practices, processes, and procedures. Although security audits conducted as part of a risk management program may not independently satisfy all requirements listed in the Information Technology Security Audit Standard (SEC502), their results and related plans for corrective action and remediation activities are treated the same as audits conducted pursuant to SEC502.

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 information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

2. RISK MANAGEMENT FRAMEWORK

2.1 *Methodology*

The Commonwealth Risk Management Framework provides a uniform approach to assessing and managing information technology risk within the Commonwealth. This framework is designed to provide measurable metrics to executive leadership within the Commonwealth in order to understand current IT risk levels as well as assist in the prioritization of actions for reducing risks to acceptable risk tolerance 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 postures 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 references to risk management activities conducted within the Commonwealth.

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. 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.

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. Examples of categories include, but are not limited to Business Environment, Asset Management, Access Control, Protective Technology, Detection Processes, Response Planning, and Recovery Planning.

Subcategories: Subcategories consist of high-level outcomes within a category, but are not intended to be a comprehensive set of the entities information security policies or procedures. Examples of subcategories: "Dependencies and critical functions for delivery of critical services are established", "Sensitive data is encrypted in transit", "Asset vulnerabilities are identified and documented", and "Access Permissions are managed".

Informative References: Informative References are specific controls or sections from within standards, guidelines, and procedures common across Commonwealth and industry partner entities that illustrate specific methods or requirements to accomplish the activities 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 may include 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 grouped in a manner that focuses on five core functions. The five Framework Core Functions are defined below. The Functions can be performed concurrently and continuously to form an operational culture that addresses risk. See Appendix A for the complete Framework Core listing.

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

Activities include identification of the organizations 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 function could be unavailable. The Identify function includes the following categories Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy. 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 organizations risk management program to ensure the continued operation of the organizations business functions.

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 includes the following categories: Anomalies and Events, Security Continuous Monitoring, and Detection Processes. The Detect function enables timely response and the potential to limit or contain the impact of potential information security events.

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 includes the following categories: Response Planning, Analysis, Mitigation, and Improvements.

Recover: Develop and implement the appropriate activities, prioritized through the organizations risk management process, to take action regarding a detected information security event.

The Recover function includes the following categories: Recovery Planning, Improvements, and Communications.

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

2.3 Framework Profile

Framework 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 outcomes that are currently being achieved based on the assessment of the five core framework functions. The framework profile results are included in the annual review of the extent to which security standards and guidelines have been adopted by state agencies.

2.4 Risk Maturity

Risk Maturity provides context on how an organization views IT risk and the 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. The risk maturity results are included in the annual review of the extent to which security standards and guidelines have been adopted by state agencies.

3. RISK MANAGEMENT REQUIREMENTS

3.1 Methodology

The following risk management activities are part of the COV ITRM SEC501 Information Security Standard Risk Management Framework. Included in this framework is the Business Impact Analysis (BIA); Risk Assessment (RA); Vulnerability Scanning; and Intrusion Detection System (IDS) Reporting.

3.2 Business Impact Analysis

3.2.1 Overview

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. Included within the BIA are data classification and data sensitivity identification activities. The summation of these requirements can provide the input to document a Sensitive Systems Inventory.

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).

3.2.2 Requirements

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

1. Identify agency business functions utilizing IT functions.
2. Identify mission essential functions (MEFs).

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

3. 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.
4. For each business function, assess whether the MEF or PBF depends on the recovery of an IT system. Each IT system that is required to recover a MEF or

PBF shall be considered sensitive relative to availability. In addition, the impact on confidentiality and integrity should be assessed.

5. Using the information collected which provides the impact of non-performance of the function; each function should be evaluated for confidentiality, integrity and availability (CIA). Some of the categories that may be used to evaluate the impact are listed below:
 - a. Confidentiality – Impact on customer service, public perception/trust, impact on sensitive data
 - b. Integrity – Impact on finance, legality, regulation, customer service, public perception/trust
 - c. Availability – Impact on life, safety, customer service, public perception/trust, finance, recovery time objective, recovery point objective
 - d. Combine the individual CIA evaluations for each function to create a prioritized listing of agency functions.
6. Reporting Requirements
 - a. An online template will be provided to capture the required information. The following data will be needed to fill out the template
 - b. Document the required Recovery Time Objective (RTO) based on agency and COV goals, objectives, and MEFs, as outlined in the agency Continuity Plan.
 - c. Document the Recovery Point Objectives (RPO) as outlined in the agency Continuity Plan.
 - d. Document the following additional BIA data objects:
 - Business Function Name.
 - Business Function Owner.
 - Date BIA completed.
 - Person Completing the BIA.
 - Primary Objective of the Business Function.
 - Business function internal customers, Commonwealth Agency customers, government entity customers, public customers and other types of 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 internal agency IT systems required by the function.
 - The external agency IT systems required by the function.
 - Identify Mission Essential Functions (MEFs).
 - Indicate whether the business function uses sensitive data.

3.3 Risk Assessment (RA)

3.3.1 Purpose

Risk Assessment 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 loss impact if one or more vulnerabilities are exploited by a potential threat.

3.3.2 Risk Assessment Planning

Annually, each Agency shall develop a risk assessment plan or review and as necessary, update an existing one for the IT systems for which it is the Data Owner. The risk assessment plan shall be based on the Business Impact Analysis (BIA) and data sensitivity classification performed by the Agency. Each Agency Head shall submit the Agency risk assessment plan to the CISO, annually.

The risk assessment plan must include the following:

- The agency name, agency abbreviation and agency number,
- The contact information of individual submitting the plan,
- The date of submission,
- The system full name and abbreviation,
- The planned assessor,
- The date the last risk assessment was conducted for the system,
- Scheduled 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.

Agencies are required, unless otherwise approved by the CISO, to use the Risk Assessment Plan Template found at:

<http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs>.

3.3.3 Performance of Risk Assessments

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

1. Conduct and document a RA of the IT system as needed, but not less than once every three years. Document and report updates to CISO using the risk assessment template.
2. Conduct and document an annual assessment to determine the continued validity of the RA. Send updates to the annual assessment to CISO.

3. 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.

4. For each risk finding, a risk treatment plan shall be created using the Risk Treatment Plan template.

3.3.4 Reporting and Verification

A. Implementation

Until completion of all risk treatment plans, the responsible Agency Head or designee shall receive reports, at least quarterly, on progress toward the implementation of the risk treatment plan. The quarterly risk update will report progress toward implementing outstanding risk treatments.

B. Verification

Upon completion of the risk treatments, the responsible Agency Head or designee shall arrange for a follow-up review to verify implementation of the specified corrective actions.

3.3.5 Reporting IT Risk Assessment Results to VITA

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:
<http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs>
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, moderate, high, critical)
 - j. Controls in place (brief description)
4. For each risk identified, a Risk Treatment Plan must be submitted to the CISO and the plan shall include the:
 - 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. The Risk treatment plan for completed risk assessments must be submitted within 30 days of issuing the final risk assessment report. An updated risk treatment plan must be submitted quarterly (at the end of the quarter), until all resolutions are completed. All Risk Treatment Plans and quarterly updates submitted must have evidence of agency head approval.

3.4 Vulnerability Scanning

3.4.1 Purpose

Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. Vulnerability scanning tools and techniques should promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;
- Formatting and making transparent, checklists and test procedures; and
- Measuring vulnerability impact.

3.4.2 Requirements

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

1. Conduct a vulnerability scan of the information system and hosted applications at least once every 90-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported.
2. 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.

****Note:** If VITA is an agency's service provider for performing the required vulnerability scans on an agency's behalf, those results are automatically reported to the CISO on the agency's behalf.

3.4.3 Reporting IT Vulnerability Scan Results to VITA

Risks identified in Vulnerability scans must be reported to the CISO using the Risk Assessment and Risk Treatment Plan templates 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

3.5 Intrusion Detection Systems (IDS)

3.5.1 Purpose

Intrusion Detection Systems are used to monitor incoming and outgoing network traffic for signs of attacks. 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.

3.5.2 Intrusion Detection System Reporting Requirements

Agencies shall provide Intrusion Detection System Reports to VITA 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. Total number of high attacks per month
5. Total number of medium attacks per month
6. Total number of low attacks per month
7. Top 10 high attacks & number of attacks seen (example: SSH Brute Force, total: 100 attacks)
8. Top 10 Source IPs
9. Top 10 Destination IPs
10. Top 10 countries of origin of attacks with percentages per month (example: Jan 2013: US – 80%, China =4%, Russia = 3%, Canada = 3%, U.K. = 3%, India=2%, Brazil=2%, Germany=2%, Ireland=2%, Sweden=2%)
11. Top 10 types of attacks (example: Denial of Service, Privilege Escalation)
12. Top 10 inbound attacks by protocol/service/port (<http://www/80>)
13. Top 10 outbound attacks by protocol/service/port (<http://www/80>)

Appendix A Risk Management Framework Core

Function	Category	Subcategory	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	<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
		ID.AM-2: Software platforms and applications within the organization are 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 • NIST SP 800-53 Rev. 4 CM-8
	Risk Assessment (RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	<ul style="list-style-type: none"> • 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

Function	Category	Subcategory	Informative References
<p style="text-align: center;">PROTECT (PR)</p>	<p>Access Control (AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p>	<p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p>	<ul style="list-style-type: none"> • CCS CSC 16 • 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 • 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"> • 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 • 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"> • 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 roles & responsibilities</p>	<ul style="list-style-type: none"> • CCS CSC 9 • 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

Function	Category	Subcategory	Informative References
			<ul style="list-style-type: none"> • SEC501 8.2, AT-3 • NIST SP 800-53 Rev. 4 AT-3, PM-13
		<p>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities</p>	<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
		<p>PR.AT-4: Senior executives understand roles & responsibilities</p>	<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
		<p>PR.AT-5: Physical and information security personnel understand roles & responsibilities</p>	<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
	<p>Data Security (DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of</p>		<p>PR.DS-1: Data-at-rest is protected</p>

Function	Category	Subcategory	Informative References
Information Protection	information.		<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 SC-28
		PR.DS-2: Data-in-transit is protected	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 AU-4, CP-2, SC-5
	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.		<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
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	<ul style="list-style-type: none"> • 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

Function	Category	Subcategory	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.			<ul style="list-style-type: none"> • 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
		<p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p>	<ul style="list-style-type: none"> • 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
		<p>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality</p>	<ul style="list-style-type: none"> • 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, 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</p>	<ul style="list-style-type: none"> • CCS CSC 7 • COBIT 5 DSS05.02, APO13.01

Function	Category	Subcategory	Informative References
		protected	<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
DETECT (DE)	<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>DE.CM-1: The network is monitored to detect potential cybersecurity events</p>	<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
		<p>DE.CM-4: Malicious code is detected</p>	<ul style="list-style-type: none"> • CCS CSC 5 • 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"> • CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1 • 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	Response Planning (RP):	RS.RP-1: Response plan is	<ul style="list-style-type: none"> • COBIT 5 BAI01.10

Function	Category	Subcategory	Informative References
(RS)	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	executed during or after an event	<ul style="list-style-type: none"> • 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)	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	<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 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 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

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

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.

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

TEMPLATES

Agencies are required, unless otherwise approved by the CISO, to use the templates found at: <http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs>

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: <http://www.vita.virginia.gov/library/default.aspx?id=537>