Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Information Security Risk Management Standard

Document Name: Information Security Risk Management Standard	Effective Date: October 15th, 2018
Document ID: IS.021	Last Revised Date: March 19, 2025

Table of Contents

1. PURPOSE

1.1. The purpose of this ***standard*** is to define the key elements of the Commonwealth's ***information*** security ***risk*** assessment model to enable consistent identification, evaluation, response, mitigation and monitoring of ***risks*** facing IT processes.

2. AUTHORITY

2.1. Pursuant to M.G.L. Ch. 7d, the Executive Office of Technology Services and Security, (EOTSS), possess the authority to establish ***policies***, ***procedures***, and objectives with respect to activities concerning ***information*** technology. M.G.L. Ch. 7d provides in pertinent part: "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of ***information, information systems***, ***assets***, ***applications***, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, boards, commissions, ***agencies***, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), by any form of contractual arrangement, are required to comply with this document, as a condition of use. Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel*** comply with the requirements herein to safeguard ***information***.

4. RESPONSIBILITY

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***standard***. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***standard***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***standard*** on an annual basis, or when significant ***policy*** or procedural changes necessitate an amendment. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

4.2. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in the monitoring and maintenance of compliance with this ***standard***.

4.3. Additional ***information*** regarding this ***standard*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/*policies*.

4.4. In the event of any conflict between the provisions contained in this ***standard*** and the provisions set forth in any of the Enterprise Information Security Policies, the provisions in the Enterprise Information Security Policies will govern.

4.5. Definitions of terms in bold may be found in the *IS.Glossary of Terms* at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Branch and all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

5.2. In the event any Commonwealth Agency or Office is unable to comply with any of the requirements of this document, the agency or office must submit an Information Security Policy Non-Compliance Report to the Enterprise Risk Management Office online through ServiceNow, https://www.mass.gov.service-now.com).

5.3. The Non-Compliance Report will:

5.3.1. Specifically state the reason/cause of the non-compliance

5.3.2. Identify and explain in detail the ***risks*** created due to the non-compliance

5.3.3. Provide a detailed explanation of the ***controls*** the agency, or office will implement to mitigate the ***risks*** to an acceptable level

5.3.4. Specify the time-frame required to implement the ***controls*** and mitigate the identified ***risks***. All Risk Mitigation Plans (RMP) will be for a limited time.

5.3.5. The names and contact information for both the ***risk owner*** and the ***control owner*** designated by the agency to accept and manage the ***risks*** associated with the non-compliance and implement the ***controls*** that will effectively mitigate the identified ***risks***.

6. STANDARD STATEMENTS

6.3. Information Security Risk Management

6.3.1. ***Information*** security ***risks*** that could compromise the confidentiality, integrity or availability of the Commonwealth's IT processes must be identified, analyzed, and mitigated to an acceptable level to meet organizational objectives and compliance requirements. The steps involved in creating IS ***risk*** management ***standard*** are as follows:

6.3.1.1. Risk Identification - The objective of ***risk*** identification is to produce a comprehensive list of ***risks*** that could impact the Commonwealth.

6.1.1.1.2. The ***Chief Information Security Officer*** **(*CISO*)** will work with the Chief Risk Officer, (CRO), to develop a Process, ***Risk*** and ***Control*** framework.

6.1.1.1.3. The framework will incorporate IT processes, ***risks*** and common ***control*** objectives mapped to authoritative sources, applicable regulatory requirements, and Commonwealth ***controls***.

6.1.1.1.4. The Commonwealth must establish ***process owners*** to support the ***risk*** assessment process and to determine the appropriate ***risk*** treatment.

6.1.1.2. Information security risk assessments

6.1.1.1.1. ***Information*** Security, (IS), ***risk*** assessments aid in identifying key IS ***risks*** within the Commonwealth's IT environment and how these IS ***risks*** may affect the Commonwealth's ability to achieve the overall organizational objectives.

6.1.1.1.2. ***Information*** Security ***risk*** assessments will be conducted on an annual basis and the results reported to the Chief Risk Officer, (CRO). The report, including all Commonwealth Agencies and Offices, will include identified ***risk*** levels to the standard set of IT ***processes***, new ***risks*** identified and the status of ***risk*** remediation efforts underway to reduce the ***risks*** to an acceptable level.

6.1.1.1.3. Commonwealth Agencies and Offices must implement a ***risk***-based management process that weighs a potential ***risk's*** impact and likelihood against the business operational impact and organizational resource cost of mitigating or minimizing the ***risk*** to an acceptable level.

6.1.1.2. Information security risk assessment model

6.1.1.2.1. As part of the ***risk*** assessment process, Commonwealth Agencies and Offices will consider the likelihood and impact upon Commonwealth IT ***processes***. Commonwealth Agencies and Offices will also evaluate both the ***inherent risks*** and ***residual risks*** to their IT ***processes*.**

6.1.1.2.2. The ***risk*** level is determined using ratings for impact and likelihood.

6.1.1.3. Impact

6.1.1.3.1. Commonwealth Agencies and Offices must ensure that ***process owners*** will be assigned to each IT ***process*** and will be responsible for determining the impact of the identified ***risk***.

6.1.1.3.2. Impact categories and definition: The impact of a ***risk*** is based on the financial, reputational, legal, regulatory, and operational impact which a ***risk*** may have if realized against a specific IT ***process***. Impact categories include:

Impact Categories	**Definition**
Financial	Financial impact to the Commonwealth based upon a ***risk*** being realized.
Reputational	Impact of a loss of confidence from its ***personnel***, constituents, business partners and regulators, which would degrade the Commonwealth's reputation.
Legal and regulatory	Impact could result in exposure to liability, enforcement, observations, recommendations and/or comments from other state entities and/or federal oversight agencies and/or regulators, or violations of contracts with ***third parties***.
Operational	The operational impact to ***processes***, people and technology in which Commonwealth employs to achieve its strategy and normal business operations.

6.1.1.3.3. Impact criteria: The Chief Risk Officer, (CRO), will develop an impact criteria to align to each impact category based upon the below ***risk*** scale.

Impact Rating	Impact Measurement	Description
Critical	4	The ***risk*** could be expected to have multiple severe or *catastrophic* [1] adverse effects on organizational operations, organizational ***assets***, systems, individuals, or other organizations.
High	3	The ***risk*** could be expected to have *severe* [2] adverse effects on organizational operations, organizational ***assets***, systems, individuals, or other organizations.
Moderate	2	The threat event could be expected to have *serious* [3] adverse effects on organizational operations, organizational ***assets***, systems, individuals, or other organizations.
Low	1	The threat event could be expected to have *limited* [4] adverse effects on organizational operations, organizational ***assets***, systems, individuals, or other organizations.

[1] A catastrophic adverse effect means that, for example, the ***risk*** might: (i) cause a catastrophic degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational ***assets***; (iii) result in major financial loss; or (iv) result in catastrophic harm to individuals involving loss of life or life-threatening injuries.

[2] A severe adverse effect means that, for example, the ***risk*** might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its functions; (ii) result in major damage to organizational ***assets***; or (iii) result in major financial loss.

[3] A serious adverse effect means that, for example, the ***risk*** might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational ***assets***; or (iii) result in significant financial loss.

[4] A limited adverse effect means that, for example, the ***risk*** might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational ***assets***; or (iii) result in minor financial loss.

6.1.1.4. Likelihood

6.1.1.4.1. A ***Process Owner*** must be assigned to each IT ***process*** and will be responsible for determining the likelihood of occurrence of the identified ***risk***.

6.1.1.4.2. The ***Process Owner*** will determine inherent likelihood by taking into consideration the likely exposure to a ***risk*** in the absence of ***controls***.

6.1.1.4.3. Likelihood Rating and Measurement: Likelihood rating is the probability of a ***risk*** occurring over a predefined time period.

6.1.1.4.4. Below are the qualitative criteria used for assessing the likelihood of a ***risk*** occurring:

Likelihood Rating	Likelihood Measurement	Description
Highly Likely	4	Greater than 75% chance of the ***risk*** occurring.
Likely	3	The chance of the ***risk*** occurring is greater than 50% and less than/equal to 75%

Possible	2	The chance of the ***risk*** occurring is greater than 25% and less than/equal to 50%
Unlikely	1	The chance of the ***risk*** occurring is less than/equal to 25%

6.1.2. Control effectiveness

6.1.2.1. ***Control*** effectiveness is a measure of how effective a ***control*** is at meeting the ***control*** objective within the Commonwealth's IT environment. This measurement is leveraged to determine the reduction of inherent likelihood to residual likelihood.

6.1.2.2. ***Control*** effectiveness is determined by the ***Control Owner*** based upon the effectiveness of the ***control*** to meet its intended ***control*** objective and minimize the likelihood of a ***risk*** to be realized.

6.1.2.3. ***Control*** effectiveness rating:

Control Effectiveness Rating	Control Effectiveness Measurement	Description
Effective	1	Mitigating ***controls*** substantially prevent exploitation of the ***vulnerability*** or limit the scope of impact to a low level.
Partially Effective	2	Mitigating ***controls*** prevent most cases of exploitation of the ***vulnerability*** or limit the scope of impact to a moderate level.
Ineffective	3	Mitigating ***controls*** do not substantially prevent exploitation of the ***vulnerability***, nor do they effectively limit the scope of impact of exploitation.

6.1.3. Calculation of ***risk***

6.1.3.1. The level of ***risk*** to a ***process*** is based on the likelihood of a ***risk*** being realized and the severity of the impact that the ***risk*** would present to the Commonwealth's IT systems.

6.1.3.2. ***Inherent risk*** factor: ***Inherent risk*** is the impact and likelihood of a ***risk*** to be realized in absence of ***controls***. An ***inherent risk*** can be calculated by the following calculation:

Impact * Likelihood = ***Inherent risk***

6.1.8.2. ***Residual risk*** factor: Using the impact, likelihood and ***control*** effectiveness rating, the ***residual risk*** can be determined as follows:

Impact * (Likelihood * ***Control*** effectiveness reduction) = ***Residual risk***

6.1.8.2.1. Control effectiveness reduction can be derived from the below table.

Control Effectiveness Rating	Control Effectiveness Measurement	Reduction in Likelihood Rating
Effective	1	50%
Partially Effective	2	25%
Ineffective	3	0%

6.1.4. Risk Response

6.1.4.1. The Risk Response or Risk Treatment Plan is prepared after the ***inherent risk*** is calculated to determine if treatment is needed to manage the ***risk*** to an acceptable level.

6.1.4.2. Treatment approaches include accepting the ***risk***, mitigating the ***risk*** by applying ***controls***, transferring the ***risk***, or avoiding the ***risk***.

6.1.5. Risk Acceptance

6.1.5.1. Commonwealth Agencies and Offices will identify the level of ***risk***[1] that the organization is willing to accept while pursuing strategic objectives and ***risk*** mitigation/approach.

6.1.5.2. Commonwealth Agencies and Offices must ensure that ***risk*** tolerance is defined at an ***agency*** level while taking into consideration the organizational impact and likelihood for the various types of ***risks*** (e.g., financial, safety, compliance, or reputation).

6.1.5.3. The Chief Risk Officer, (CRO), in consultation with the ***Commonwealth CISO*** will have final say on whether an established ***risk*** tolerance is acceptable to the Commonwealth as an organization.

6.1.5.4. Residual Acceptance and Tolerance

6.1.5.4.1. Commonwealth Agencies and Offices must ensure that the ***Process Owner*** will be made aware of any ***residual risks***, which are deemed "Critical" or "High" by the ***CISO*** or CRO.

6.1.5.4.2. The CRO and security team will provide recommendations to reduce the ***risk*** to a reasonable and appropriate level. If the ***Process Owner*** fails to observe the CRO's recommendation or implements alternate mitigating ***controls***, Commonwealth Agencies and Offices must ensure that the ***Process Owner*** is accountable and must sign off that they accept the ***residual risk*** to their agency.

6.1.5.4.3. The CRO must be informed and approve ***risk*** acceptance of any "Critical" or "High" ***residual risks***.

6.1.6. Risk Mitigation

6.1.6.1. When the IT ***risk*** has been acknowledged, corrective action will be implemented to mitigate or reduce the IT ***risk***.

6.1.6.2. The identified ***risks*** and the planned remediation actions must be documented in a ***Plan of Action and Milestones (POAM)***. The ***POAM*** must be updated as remediation actions occur.

6.1.6.3. Identify Mitigating ***Controls***

6.1.6.3.1. Commonwealth Agencies and Offices will ensure that the ***Process Owner,*** in coordination with the CRO, identifies and proposes the

[1] For agencies that connect to MAGNet or receive services from EOTSS.

implementation of supplemental ***controls*** to reduce or eliminate the ***risk*** to Commonwealth ***processes*** commensurate with the impact and determined ***residual risk***.

6.1.6.3.2. ***Control*** types will include:

6.1.6.3.2.1. Preventive — prevents the ***risk*** by reducing the likelihood of a threat exploiting ***vulnerabilities***.

6.1.6.3.2.2. Detective — monitors and/or alerts success factors to stem further losses.

6.1.6.3.3. Development of a remediation plan

6.1.6.3.3.1. For ***residual risks*** that are unacceptable to the organization, Commonwealth Agencies and Offices must ensure that the ***Process Owner*** will develop a remediation plan in coordination with the CRO.

6.1.6.3.3.2. The remediation plan must be approved by the CRO.

6.1.7. ***Risk*** Transfer

6.1.7.1. The IT ***risk*** has been acknowledged, and the IT ***risk*** is insured across the organization.

6.1.8. ***Risk*** Avoidance

6.1.8.1. The IT ***risk*** is avoided entirely, and the organization ceases to perform the activity/activities that caused the IT ***risk*** to materialize.

6.1.9. Risk Reporting

6.1.9.1. Commonwealth Agencies and Offices must ensure that the CRO, in collaboration with the ***Process Owner(s)*** will produce a ***risk*** assessment report to provide necessary ***information*** to the ***Risk Governance Committee***, including:

6.1.9.1.1. Overall Executive dashboard that depicts the critical IT ***residual risks***, management's response, and the associated action plan(s).

6.1.9.1.2. Recommended changes listed by priority, with approximate levels of effort/cost to implement.

6.1.9.1.3. IT ***risk*** response actions — e.g., by division, ***Inherent Risk*** rating, by ***Residual Risk*** rating, etc.

6.1.9.1.4. Trending of IT ***risk*** assessment results — e.g., comparison of previous IT ***risk*** assessment results vs. current IT ***risk*** assessment results to:

6.1.9.1.4.1. Determine changes in ***Inherent Risk*** and ***Residual Risk*** ratings.

6.1.9.1.4.2. Use IT ***risk*** criteria/attributes to help prioritize and determine how often to conduct the IT ***risk*** assessments.

6.1.9.1.5. Level of ***residual risk*** that would remain after the recommended changes are implemented.

6.1.9.1.6. At a minimum, all IS ***risks*** rated as "Critical" and "High" must be reported to the **Risk Governance Committee**. The ***risk*** ratings will be expressed using the following levels:

Residual Risk		**Likelihood**			
		Highly Likely (4)	**Likely (3)**	**Possible (2)**	**Unlikely (1)**
Impact	**Critical (4)**	**Critical (16)**	**Critical (12)**	**High (8)**	**Moderate (4)**
	High (3)	**Critical (12)**	**High (9)**	**Moderate (6)**	**Low (3)**
	Moderate (2)	**High (8)**	**Moderate (6)**	**Moderate (4)**	**Low (2)**
	Low (1)	**Moderate (4)**	**Low (3)**	**Low (2)**	**Low (1)**

6.2. Information Security Training and Awareness

6.2.1. The objective of the Commonwealth ***information*** security training is to educate ***users*** on their responsibility to help protect the confidentiality, availability, and integrity of the Commonwealth's ***information assets***.

6.2.2. Commonwealth Agencies and Offices must ensure that all ***personnel*** are trained on all relevant rules and regulations for cybersecurity.

6.2.3. Implement an enterprise-wide ***information*** security awareness and training program.

6.2.3.1. Develop appropriate training materials in collaboration with Human Resources and Legal.

6.2.3.2. Conduct periodic refresher training for all ***personnel*****,** including contractors and temporary staff.

6.2.3.3. The training will:

6.2.3.3.1. Explain acceptable use of ***information*** technology

6.2.3.3.2. Inform ***personnel*** about relevant ***policies*** and ***standards***

6.2.3.3.3. Detail each individual's accountability for each of the provisions of all ***policies*** and the underlying ***procedures***.

6.2.3.3.4. Test each individual's understanding of all ***policies*** and of his or her role in maintaining the highest ethical ***standards***.

6.2.4. Initial education and training apply to ***personnel*** who transfer to new positions or roles with substantially different ***information*** security requirements, not just to new starters, and should take place before the role becomes active.

6.2.5. New Hire Security Awareness Training

6.2.5.1. All new ***personnel*** must complete an Initial Security Awareness Training course. This course will be conducted via web-based learning or in-class training and will be included in the new hire orientation checklist. The New Hire Security Awareness course must be completed within 30 days of new hire orientation.

6.2.6. Annual Security Awareness Training

6.2.6.1. All ***personnel*** are required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to ***personnel*** 12 months after course completion, alerting ***personnel*** to annual refresher training completion deadlines.

6.2.7. Role-Based Training

6.2.7.1. Additional security training is provided to the following groups:

6.2.7.2. Privileged ***Users***

6.2.7.3. Executives

6.2.7.4. Members of the Security Incident Response Team (SIRT)

6.2.8. The awareness program will be updated regularly by the Enterprise Security Office so that it remains consistent with organizational ***policies*** and ***procedures*** and will be built on lessons learned from ***information security incidents***.

6.2.9. The awareness program will ensure that all principles, ***policies***, ***procedures,*** and training materials are accessible by all ***personnel*** as appropriate.

6.2.10. All Commonwealth ***personnel*** must complete the annual ***information*** security training. Completion rates will be tracked and reported to ***personnel*** managers and IS leadership. Training records are maintained as defined by organizational policies and procedures

6.2.11. All new hires must sign the acceptable use policy (*See IS.002 Acceptable Use Information Technology Policy)*.

7. CONTROL MAPPING

Section	NIST SP800-53 R5	CIS 18 v8	NIST CSF
7.1 Information Security Risk Management	RA-1	CSC 16	ID.GV-1
			ID.AM-5
	RA-3	CSC 16	ID.RA-1
	CA-1	-	ID.GV-1
			ID.RA-1
	CA-5	CSC 16	-
	CA-6	-	-
	PM-4	-	ID.RA-6
	PM-9	-	ID.GV-4

		-	ID.RA-3
			ID.RA-1
			ID.RA-1
			ID.RA-1
	CA-2	-	ID.RA-1
	CA-7	CSC	ID.RA-1
	RA-7	CSC 7	ID.RA-2
			ID.RA-4
			ID.RA-5
			ID.RM-1
			ID.RM-2
			ID.RM-3
			-
7.2 Information Security Training and Awareness	AT-1	CSC 14	ID.GV-1
	AT-2	CSC 14	
	AT-3	CSC 14	
	AT-4	-	-
			-
			ID.RA-2
			PR.IP-10

			ID.RA-2

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.92	John Merto	01/28/2018	Corrections, formatting.
0.95	Sean Vinck	5/7/2018	Corrections and formatting.
0.96	Andrew Rudder	5/31/2018	Corrections and formatting.
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	6/1/2018	Final Pre-Publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	Annual Review and minor edits
1.4	Thomas E. McDermott	11/30/2023	Corrections, Formatting, Updating and Annual Review
1.4	Anthony O'Neill	11/30/2023	Final Review
1.5	Thomas E. McDermott	12/9/2024	Corrections, Formatting and Annual Review
1.5	Anthony O'Neill	12/9/2024	Final Review

1.6	Thomas McDermott	2/19/2025	Updates, Corrections and Formatting
1.6	Miklos Lavicska	3/7/2025	Corrections and Formatting
1.6	Anthony O'Neill	3/19/2025	Final Review