IT Risk Management Policy

Effective Date: January 2, 2025	**Category:** Security
Scheduled Review: January 2, 2027	**Supersedes:** SEC-040

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This policy establishes the framework for managing information technology (IT) risks within the Commonwealth. It aims to protect the confidentiality, integrity and availability of Commonwealth IT assets and ensure compliance with legal, regulatory, and operational requirements.

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies"). Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

4. Roles and Responsibilities

Chief Information Officer (CIO): Oversees the implementation and enforcement of this policy.

Chief Information Security Officer (CISO): Reviews and approves risk management strategies.

Head of Governance, Risk and Compliance: Oversees IT Risk Management and IT Vendor Risk Management program and process.

Agency Information Security Officers (ISO): Ensure respective agencies comply with risk management activities and support mitigation measures.

Employees and Contractors: Adhere to risk management policy and report potential risks upon identification.

5. Policy

5.1 Risk Management

The Commonwealth is committed to proactively managing IT risks to protect its information assets, maintain operational continuity, and ensure compliance with applicable legal, regulatory, and contractual obligations. All IT systems, applications and data will be subject to a risk management process to identify vulnerabilities, assess potential impacts and implement appropriate controls.

Key Principles

Risk Identification

- Identify potential IT risks, including cybersecurity threats, operational disruptions, and technology failures, through monitoring and assessments.

Risk Assessment

- Assess risk based on their likelihood and potential impact on confidentiality, integrity, and availability of information assets.

Risk Mitigation and Treatment

- Implement risk mitigation strategies, including preventative, detective, and corrective controls, to address identified risks in alignment with Commonwealth priorities.

Compliance and Standards

- Ensure alignment with relevant standards, such as NIST framework.

Monitoring and Reporting

- Establish continuous monitoring mechanisms and regular reporting of risk management activities to senior leadership.

Training and Awareness

- Provide training and awareness to promote a culture of risk awareness among staff and stakeholders.

5.2 IT Vendor Risk Management (Third-party Risk Management)

IT Vendor Risk Assessment

The Commonwealth recognizes that third-party vendors play a critical role in its IT operations. To protect information assets and maintain a reasonable level of assurance from a security and compliance perspective, the Commonwealth is committed to managing inherit risks presented by IT vendors through a structured vendor risk assessment process, known as an IT Vendor Risk Assessment.

Prior to the procurement or use of any new Computing Service, an IT Vendor Risk Assessment shall be conducted by the Governance, Risk and Compliance team, following the process outlined in the IT Risk Management Vendor Risk Assessment Procedure.

A new IT Vendor Risk Assessment is required should there be a change to previously reviewed services and/or a change in the scope of services provided.

Additionally, any new Computing Services that an agency would like to test via a Pilot or Proof of Concept must be approved by the Department of General Services (DGS). Guidance on this may be found within the DGS, Bureau of Procurement Policy Directive 2021-1, New Technology Pilot Program and Product Demonstrations.

5.3 System and Organization Control (SOC) Reporting

SOC is a term defined by the American Institute of Certified Public Accountants (AICPA). There are three primary types of reports. The reports are designed to address different aspects of a service organization's control environment.

5.3.1 SOC 1- Internal Control Over Financial Reporting

- SOC 1 Type I – Report on the suitability of the design of the controls at a specific point in time.
- SOC 1 Type II - Report on the suitability of the design of the controls over a period of time.

5.3.2 SOC 2 – Trust Service Criteria (Security, Confidentiality, Integrity, Availability and Privacy)

- SOC 2 Type I – Report on the suitability of the design of the controls at a specific point in time.
- SOC 2 Type II - Report on the suitability of the design of the controls over a period of time.

5.3.3 SOC 3 – General Use Report (high level summary usually intended for marketing purposes)

Agencies and Service Organizations shall obtain their providers most recent, applicable SOC report and follow SOC review requirements outlined in the IT Risk Management SOC Report Review Procedure.

5.4 Risk Acceptance and Acknowledgement

The Governance, Risk and Compliance team will process the appropriate risk acceptance and/or acknowledgment form upon identification of potential risk. There are two variations of the form: IT Risk Acknowledgement Form (General IT Risks) and IT Risk Acknowledgment Form (IT Vendor Risks). The identified risks will be shared with the Commonwealth Chief Information Officer (CIO), the Commonwealth Chief Information Security Officer (CISO), the Delivery Center/Agency Information Security Officer (ISO) and identified Business Owner for initial discussion. Recommendations will be documented by the GRC team and processed for signature by those below.

- Agency Deputy Secretary for Administration or Agency Secretary
    - Signature certifies an understanding and acknowledgement of the risks outlined within the form and that in the event an issue arises, they will acknowledge responsibility.

- Agency Business Area Contact (Bureau Director)
    - Signature certifies an understanding and acknowledgement of the risks outlined within the form and that in the event an issue arises, they will acknowledge responsibility.

- Agency Office of Chief Counsel
    - Signature certifies that they have been consulted in connection with the risks outlined within the form and that they have advised the agency and delivery center of the potential legal concerns associated with the risks identified.

6. Contact

Questions or comments may be directed via email to OA IT Central.

Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision	Redline Link
Original	1/2/2025	Base Document	