Information Technology Risk Management Standard

Responsible Office: Technology Services
Initial Standard Approved: 02/01/2017
Current Revision Approved: 05/22/2017

Standard Statement and Purpose

This document describes the purpose, key requirements and expectations in the management of Information Technology (IT) risks within the University. This document serves as guiding document for the IT risk management program. This Standard is geared to protecting the organization and its ability to perform its mission while protecting the information and effectively treating identified risks affecting this information.

This Standard should be used in conjunction with the documents listed in the Related Documents section.

Noncompliance with this Standard may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Standard

All persons responsible for the technical and management support of systems should read and this Standard and familiarizing themselves with its contents and provisions.

Definitions

Business Impact Analysis (BIA)
Business impact analysis is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.

Cloud Computing
Internet-based computing that provides shared processing resources and data to computers and other devices on demand. This may include but is not limited to servers, networks, applications, and storage.

Credentialed Vulnerability Assessment
The credentialed vulnerability assessment involves a vulnerability scan using the University's vulnerability scanning software. Credentials are used to login to the target system and / or application, allowing the identification of weaknesses residing on the system that can be exploited by potential attackers. A qualified analyst performs an analysis of the results and recommendations for remediation are made to the system administrator.

Data Custodian
The Data Custodians can have both a business and/or technical role, though it is typically considered a business role. The Data custodians are responsible for entering, modifying and maintaining data in the enterprise databases and information systems.

Data Steward
Data stewards are appointed by and report to the data trustees. Data stewards have knowledge of and work in accordance with numerous University rules and policies across the institution, including university policies on information security and privacy. Data stewards are essentially Executive Subject Matter Experts (ESMEs) for the business domains under their authority.

Information Storage and Handling
Within the context of this document, information storage and handling refers to actions that create, store, transmit, process, modify, destroy, and / or archive information. The storage and handling of information may involve both electronic and physical actions.

Information Technology Baseline
A technology baseline is a set of technical requirements that define the minimum required standard practices. Technology Baselines are used in conjunction with Information Technology Standards and Policies.

Information Technology Guideline
A technology guideline is a recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.

Information Technology Risk Assessment (IT Risk Assessment)
The University's IT risk assessment process focuses on identifying, quantifying, and prioritizing risks present in all components of information systems used by the University to manage its information. An IT risk assessment may include the assessment of the technology and processes used to handle and store University information.

Information Technology Standard
A technology standard is a formal document for an established norm of methods, criteria, and processes for technology subjects.

Project Sponsor
The authoritative person with responsibility for the definition and initiation of a technology project. This person is the primary stakeholder of a project.

System Owner
A system owner is an employee with the oversight responsibility for the management of an IT system. The system owner is typically not the administrator managing the system, but rather the departmental business manager and sponsor of the system. The system owner holds the authority to provision, de-provision, or modify the IT system to address specific business needs.

Contacts

VCU Technology Services officially interprets this Standard. The Information Security Office is responsible for obtaining approval for any revisions through the appropriate governance structures. Direct questions regarding this Standard to the Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

This section contains the specifics and requirements for the IT Risk Management Standard.

A. General and Category III Information/Data Requirements.

The requirements delineated in this section are applicable to all systems and projects in the VCU environment and where specifically designated apply to VCU information/data that are classified as Category III.

1. Create and maintain a security control framework and review annually at a minimum.
The Information Security Office must create and maintain a security control framework that details security controls for protecting VCU information and IT assets. The framework must be reviewed annually at a minimum. (F26)

2. Must complete an IT Risk Assessment (incl. Business Impact Analysis).
Project sponsors for IT projects must request risk assessments through the University Information Security Office for all initiatives involving information storage, processing and transmission. (F4, N15)

3. Must complete system and data security/system security plan with Information Security Office review.
Prior to system deployment, system owners with the input from system administrators, data custodians and data stewards must complete a system security plan for IT systems. System security plans for established systems must be reviewed and updated periodically. All plans are subject to approval by the Information Security Office. All shortfalls identified must be documented and treated in accordance with VCU requirements. If treatment options do not exist, the shortfalls must be addressed as exceptions requiring approval from the Information Security Office. (F5, N14)

4. Identify / document critical business processes supported by system and data.
All current critical business processes must be identified and documented with associated systems and data in accordance with VCU requirements. A business unit representative with the input from system owners and data stewards must create and maintain this document. (F7)

5. Internal technical system documentation must be protected.
All technical system and network architecture documentation must be kept in a secure location. User access to documentation must be approved by management and include an audit trail. User access is subject to annual review, and when no longer necessary, must be suspended. (F19)

6. Server quarterly vulnerability assessment and remediation.
All servers storing or handling data must undergo a vulnerability assessment quarterly. All critical and high level vulnerabilities identified must be remediated prior to the following quarterly vulnerability scan, with remediation verified by subsequent scans. (H38)

B. Category II Information/Data Requirements.
The requirements delineated in this section are applicable to VCU information/data that are classified as Category II. In addition to the requirements from the General and Category III Information Section, the handling and storage of Category II information/data must also adhere to the following requirements:

1. Risk Assessments must be formal and include a Business Impact Analysis component.
All risks identified must be documented and treated in accordance with VCU requirements. This requirement is in effect throughout all project and system lifecycles. Documentation must be reviewed and updated periodically. (F5, N14)

C. Category I Information/Data Requirements.
The requirements delineated in this section are applicable to VCU information/data that are classified as Category I. In addition to the requirements from the General/Category III and Category II Information/Data Sections, the management of Category I information/data must also adhere to the following requirements:

1. Server pre-provisioning vulnerability assessment and remediation.
All servers, including applications operating on those servers storing or handling Category I Information/data must undergo a credentialed vulnerability assessment prior to deployment. All critical and high level vulnerabilities identified must be remediated prior to provisioning, with remediation verified by subsequent pre-production scans. (H36)

2. Server full annual vulnerability assessment and remediation.
All servers storing or handling data must undergo at least one credentialed vulnerability assessment annually. All critical and high level vulnerabilities identified must be remediated without unreasonable delay, with remediation verified by subsequent scans. (H37)

3. Dedicated security requirements.
Category I data must have a dedicated information security requirements used to govern the protection and handling of such data. Information Security Office is responsible in documenting specific information security requirements related to Category I information. Data stewards are responsible to collectively develop and enforce such requirements with the assistance from the Information Security Office. These requirements must be periodically reviewed and updated. (N20)

D. Special Requirements.
The following requirements apply to personnel or systems used to handle specific data/information types; all data types listed in this section are considered Category I data and must also adhere to the requirements listed in the Category I Information Section.

1. Data security and privacy policy or statement for data
All data security and privacy policies must address the following:

- Procedure for filing a complaint on detection of inappropriate misuse
- Procedure for data sharing and disclosure
- Procedure to opt-out or opt-in for sensitive information access
- Procedure to access individual's own information
- Procedure for third party information sharing and vetting
- Procedure for establishing acceptable use of collected data
- Procedure for enforcement of privacy and security policies

All policies must be published and followed. Policies must be periodically reviewed and updated. Required by FERPA, PCI-DSS, Financial Aid Information, HIPPA, CUI, PII of EU Citizens, FISMA (mod), and CFR Title 21 Part 11 (FDA) information. (N21)

2. Perform quarterly external vulnerability assessment by qualified vendor.
Perform quarterly external vulnerability scan by a qualified scanning vendor and remediate all critical and high level vulnerabilities. Required by PCI-DSS. (H55)

E. Exception Request
All requests for exception(s) to this standard are evaluated by the Information Security Office on a case-by-case basis. Exception requests should be made using the Information Security Exception Request Form found in Information Technology Professionals (ITPros) Intranet – IT Resources - Forms. Authorized access to the IT Pros Intranet can be requested by emailing uccnoc@vcu.edu. The completed exception request form is automatically emailed the Authoritative Unit Head listed in the request. After the Authoritative Unit Head approves the request, the Information Security Office will provide the secondary review and approval as appropriate. Evaluation criteria for exception include the

requirement to which an exception is requested, the sensitivity of the information affected, compensating controls in place to mitigate additional risks, and business processes affected by the exception. The Information Security Office will send the exception request review decision and any additional correspondence to the requestor's and the authoritative unit head's email addresses.

Forms

1. VCU Information Security Exception Form

Related Documents

The VCU Information Technology Policy Framework contains VCU Information Technology Policies, Standards and Baseline requirements, all of which must be followed in conjunction with this Standard.

Baseline documents can be found in the VCU University Computer Center IT Professionals Intranet under Security Baselines. Access to the IT Professionals Intranet requires approval. Requests for access can be made via email to uccnoc@vcu.edu.

1. **Computer Network and Resources Use Policy**
2. **Information Security Policy**
3. **Exposure and Breach of Information Policy**
4. **Data Classification Standard**
5. **Network Management and Security Policy**

Revision History

Approval/Revision Date	*Title*
02/01/2017	New Standard
05/22/2017	Minor Revisions

FAQs

There are no FAQs associated with this Standard.