COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

INFORMATION TECHNOLOGY
SECURITY AUDIT 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.

This chart contains a history of this ITRM publication’s revisions.

Version	Date	Purpose of Revision
Original	July 1, 2006	Base Document
	October 17, 2006	Minor wording changes. No impact on the intent of this standard.
Revision 1	January 11, 2007	Performance of a “Risk Assessment (RA)” as the basis for developing audit plans was included in the original standard because of an oversight. This revision corrects that oversight by deleting references to “Risk Assessment (RA)” on pages iii (**Purpose)** and 3 (**2.1 – Planning for IT Security Audits**).
Revision 2	December 5, 2011	Revision to clarify various requirements indicated in italics and line in the left margin. Revised to address the new IT governance structure in the Commonwealth. See section 2.2 for new guidance and clarification.
Revision 3	February 27, 2019	Revised to clarify IT Security Audit requirements in Section 1.4
Revision 4	September 15, 2021	Revised Section 1.2.4 by moving the explanations for internal and external audits to Section 1.5 IT Audit Frameworks; Revised Section 1.2.5 IT Security Auditors, Added additional information in Section 1.3.d. Chief Information Officer Designation ; Revised requirements in 1.4.. Scope and Frequency of IT Security Audits, including moving verbiage to other sections of the standard for clarity; Added section 1.5 Audit Frameworks incorporating existing requirements from other sections of the Standard and adding additional information related to the frameworks; Changed section name to 2. IT Security Audit Program; Added information and requirements in 2.1. Planning for IT Security Audits including relying on third party audits; Adjusted reference to the Standards in 2.2 IT Security Audit Scope, including adding references to contractual requirements and audit independence requirements; Moved requirements for the attestation to an audit standard to Section 2.5.2. IT Security Audit Reports; Added information and clarification in 2.7. Reporting IT Security Audit Results to VITA

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. Deleted language shall be noted by ~~striking it through~~.

The following examples demonstrate how the reader may identify updates and changes:

EXA-R-01 Example with No Change – The text is the same.

EXA-R-02 Example with Revision – The text is the same. *A wording change, update or clarification is made in this text.*

EXA-R-03 Example of New Text – *This language is new*.

PREFACE

Publication Designation

ITRM Standard SEC502-04

Subject

Information Technology Security Audit Standard

Effective Date

September 15, 2021

Compliance Date

January 1, 2021

Supersedes

COV ITRM Standard SEC502-03

Scheduled Review:

Every two years

Authority

Code of Virginia, §2.2-2009.A.1.
(Additional Powers of the CIO relating to security)
"Address the scope and frequency of IT Security audits"

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 conducting an IT security audit of sensitive *IT* systems that contain Agency information as identified and prioritized in an Agency's Business Impact Analysis.

General Responsibilities

(Italics indicate quote from the Code of Virginia requirements)

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.

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)
- Commonwealth of Virginia Information Technology Hosted Security Standard (ITRM Standard SEC525)

TABLE OF CONTENTS

1. Introduction

1.1 How to Use this Standard

This Standard is written to be read from front to back, as its requirements are interrelated. If the reader tries to consider just one area and skip others, the reader's Agency risks overlooking important requirements and may be unaware of areas in which the Agency does not comply with the Standard. Furthermore, this Standard is written to be read in conjunction with the following two Information Technology (IT) security documents: *Commonwealth of Virginia Information Technology Security Policy* (ITRM Policy *SEC519*) and *Commonwealth of Virginia Information Technology Security Standard* (ITRM Standard SEC501).

1.2 Definitions

The roles and responsibilities defined in the *Commonwealth of Virginia Information Technology Security Standard* (ITRM *Standard SEC501*) shall apply to this standard. For the purposes of this standard, the following definitions also shall apply:

1.2.1 Commonwealth of Virginia (COV) Information Technology (IT) System

In general, an IT system is an interconnected set of IT resources under the same direct management control. For the purposes of this standard, a Commonwealth of Virginia (COV) IT system is any such system that processes COV data.

1.2.2 Data Communications

Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate COV data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of this information.

1.2.3 Data Owner

The Data Owner is the agency manager responsible for the policy and practice decisions regarding data, is responsible for following:

1. Evaluate and classify sensitivity of the data.

2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

3. Communicate data protection requirements to the System Owner.

4. Define requirements for access to the data.

1.2.4 IT Security Audit

An Information Technology (IT) Security Audit is an independent review and examination of an IT system's policies, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

~~Internal Audits~~

~~Internal audits, as recognized by the Office of the State Inspector General (OSIG), must be based the Institute of Internal Auditors (IIA) framework for the professional practice of internal auditing (i.e. "Red Book). Contractors employed by the Internal Audit department for staff augmentation are bound by the same requirements. Internal audits must be issued from an internal audit organization recognized by OSIG.~~

~~External Audits~~

~~External audits are those audits performed independent of the agency. They are performed by an outside firm or agency. They must use an acceptable auditing framework (i.e. Generally Accepted Government Auditing standards (GAGAS) or "Yellow Book"; American Institute of Certified Public Accountants (AICPA) Standard for Consulting Services; or the AICPA Statement on Auditing Standards). The use of any other audit standard or framework must be approved by Commonwealth Security and Risk Management (CSRM) prior to the start of the audit~~

1.2.5 IT Security Auditors

IT Security Auditors are CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts *or other State or Federal government auditors, private auditing firms*, *or augmented staff for existing internal audit* that has the experience and expertise required to perform IT security audits.

1.2.6 Sensitive IT Systems and Data

Sensitive Data is any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled. Sensitive IT Systems are COV IT systems that store, process, or transmit sensitive data.

For the purposes of this standard, Sensitive IT Systems and Data are any IT system or data classified by the Agency as sensitive in accordance with the requirements of the *Commonwealth of Virginia Information Technology Security Standard* (ITRM Standard SEC501), Section 2.5: System and Data Sensitivity Classification.

1.3 Chief Information Officer (CIO) Designation

The Chief Information Officer (CIO) of the Commonwealth has designated the Chief Information Security Officer (CISO) of the Commonwealth to develop policies, procedures, and standards for:

a. Assessing IT security risks;

b. Performing IT security audits of IT systems and data communications;

c. Determining appropriate IT security measures; and

d. Overseeing, planning, and coordinating the conduct of periodic security audits of all executive branch and independent agencies.

1.4 *Scope and Frequency of IT Security Audits*

~~Each Agency shall establish an IT Security Audit Program. The program shall include assessing the risks associated with the state IT systems for which it is the Data Owner and conducting IT Security Audits at a frequency relative to the risk identified by the Agency~~. At a minimum, IT systems that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years *or more frequently commensurate with risk*. ~~All IT security audits must follow an approved auditing framework.~~

~~NOTE: Auditor independence is important. An agency should not engage the same auditing firm to conduct both audits and other IT security work (i.e. risk assessments, business impact analysis) for the agency unless the auditing firm can demonstrate appropriate independence of the personnel performing the work~~.

1.5 IT Audit Frameworks

All IT security audits must follow an established auditing framework. In general, internal auditors will follow the Institute of Internal Auditors (IIA) framework and external auditors will follow Generally Accepted Government Auditing Standards (GAGAS).

> *Internal audits: Internal audit departments, as recognized by the Office of State Inspector General (OSIG), must use the Institute of Internal Auditors (IIA) the International Professional Practices Framework (IPPF), i.e. Red Book. Contractors employed by the Internal Audit department for staff augmentation are bound by the same requirements.*
>
> *External audits: External audits are those audits performed independent of the agency. They are performed by an outside firm or agency contracted to perform audit work. They must use an acceptable auditing framework (such as: the generally accepted government auditing standards GAGAS Yellow Book; American Institute of Certified Public Accountants (AICPA) Standard for Consulting Services; or the AICPA Statement on Auditing Standards).*

The use of any audit framework or standard, other than those specified in this section, shall be approved by Commonwealth Security and Risk Management (CSRM) prior to the start of an audit.

Audit practitioners conducting the audit shall be compliant with the requirements of the framework or standard used as the basis of their audit and provide appropriate documentation as evidence upon request (i.e. External Quality Assurance Report for audits based on the Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF).

Audits based on a framework or standard that has not been approved or audits conducted by practitioners that do not meet the minimum requirements of the selected auditing framework or standard will not be accepted by CSRM.

2. *IT Security Audit Program*

Each Agency shall establish an IT Security Audit Program. The program shall include assessing the risks associated with IT systems for which it is the System Owner and/or Data Owner and conducting IT Security Audits at a frequency relative to the risk identified by the Agency. At a minimum, IT systems that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.

Agencies are accountable to audit any controls of an IT system for which they have responsibility. This accountability may be explained in an interoperability agreement, a contract, a memorandum of understanding (MOU), or instructions provided by the system owner. For example, an agency may still be responsible for approving and disabling user access; securely hardening client software; monitoring for unusual activity; assuring appropriate physical security of user work stations; and planning for contingencies in the event that the service organization's system is not available.

> *Commonwealth agencies can request audit reports from the other agencies to determine whether controls have been audited related to their agency data and any issues that are identified have been addressed.*

IT Security Audits shall be conducted by personnel or organizations defined as IT Security Auditors in section 1.2.5, above, or by such other entity as approved by the CISO.

2.1 Planning for IT Security Audits

This *Standard* does not require, and shall not be construed to require, duplication of audits already performed or underway, except when it is deemed necessary by auditing entities whose audit rights, by Virginia law, cannot be infringed. Coordinated IT security audit planning is, therefore, essential and shall be the responsibility of the Agency Head or designee.

Agencies should leverage audits performed by third parties to audit agency sensitive systems efficiently. Third party audits could include government audits or third party assurance audits. Additional guidance on relying on third party audits is included below:

- *Auditor of Public Accounts/JLARC/OSIG – Agencies that rely on the audit work performed by commonwealth audit agencies must have a statement from the auditing entity stating what systems were addressed by the audit and the IT security control families that were included in the audit.*

- *Federal Government – Agencies subject to audits by Federal agencies (i.e. U.S. Department of Health and Human Services) may leverage audit report results.*

- *Service Organization Control (SOC) Reports – Agencies that use commercial services or software may use a SOC audit to assess the security of these services, i.e. a SOC 2 Type 2 audit.*

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

The IT Security Audit plan must include the following:

- The agency name, agency abbreviation and agency number,
- The contact information of individual submitting the plan,
- The system full name and abbreviation,
- The planned auditor,
- The date the system was last audited,
- Scheduled audit completion date.

Note: Scheduled audit completion date is the planned date of the completion of the future audits covering a three-year period from the *last audit completion* ~~submission~~ date.

Agencies are required to use the IT Security Audit Plan Template found at: *https://www.vita.virginia.gov/it-governance/itrm-policies-standards/#securityPSGs*If the IT system relies upon IT services provided by VITA or any other service provider, the IT Security Auditor shall rely on any applicable IT Security Audits performed during the applicable audit cycle for that component of the IT Security Audit. For IT services provided by VITA, the CISO will coordinate the VITA IT security audits. If an Agency has VITA IT security audit needs that are not met through existing or planned IT security audits, the Agency should contact the CISO to address those needs. It is the Agency's responsibility to ensure that adequate IT security audit provisions exist relative to other service providers. *Agencies shall notify CSRM in writing if they are unable to complete their IT auditing obligations due to insufficient funding, personnel constraints or other reasons.*

The CISO may also conduct IT Security Audits as circumstances warrant, or upon request of any entity with operational or audit authority over the *IT system* in question.

2.2 IT Security Audit Scope

In conducting IT Security Audits, the IT Security Auditor shall use criteria that, at a minimum, assess the effectiveness of the system controls and measures compliance with the applicable *COV ITRM Policies and Standards*. *IT Security Auditors should also use standards that measure compliance with any other applicable Federal, contractual, and COV regulations*.

NOTE: Data and homogenous 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.

Auditor independence is addressed in audit standards and frameworks. It refers to an auditor's ability to make unbiased, objective audit opinions. To ensure auditor independence, agencies shall get approval from CSRM prior to the start of any audit *where the agency has engaged the same auditing firm to conduct audits and other IT security work (i.e. risk assessments, business impact analysis) for the agency. Agencies should be prepared to explain the safeguards that will be implemented to ensure that auditor independence is achieved.*

2.3 Access Required to Perform IT Security Audits

IT Security Auditors shall be granted all access required to perform IT Security Audits, including logical and physical access on a need-to-know basis.

2.4 Performance of IT Security Audits

Prior to performing each IT Security Audit, the IT Security Auditor will contact the Agency Head or designee and agree on:

- A specific scope, in accordance with Section 2.2 of this standard;
- A mutually agreeable schedule for the IT Security Audit;
- A checklist of information and access required for the IT Security Audit.

After agreeing to a scope, schedule and checklist, the IT Security Auditor will conduct the IT Security Audit.

2.5 Documentation of IT Security Audits

2.5.1 IT Security Audit Work Papers

The IT Security Auditor shall prepare audit work papers as documentation of the audit, including sufficient competent evidential matter to support all conclusions. The IT Security Auditor should take care that such work papers do not constitute an unnecessary security risk and are safeguarded appropriately.

2.5.2 IT Security Audit Reports

The IT Security Auditor will document the findings of the IT Security Audit. Prior to formal presentation of the IT Security Audit Report, the IT Security Auditor will present a draft of the report to the Agency Head or designee. They will discuss the report and make any mutually agreeable changes. The Agency Head or designee shall then be given no less than 10 business days to prepare a Corrective Action Plan ("plan"). The plan shall include concurrence or non-concurrence with each finding in the IT Security Audit Report. *The official audit report submitted needs to include an attestation as to the audit standard used (i.e. yellow or red book or other approved framework).*

2.6 Corrective Action Plan Reporting and Verification

A. Implementation

Until completion of all corrective actions in the plan, the responsible Agency Head or designee shall receive reports, at least annually from the date of the final IT Security Audit Report, on progress toward implementing outstanding corrective actions.

B. Verification

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

2.7 Reporting IT Security Audit Results to VITA

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

A record of all completed IT Security Audits conducted by or on behalf of the Agency, including the official audit report (in accordance with auditing standards), all findings, and whether the Agency concurs or does not concur with each. IT Security Audits submitted to VITA must be reflected in the IT Security Audit Plan.

1. *Agencies are required to submit the corrective action plans using the eGRC system, using the Audit Remediation Plan Template found at: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/#securityPSGs, or using another method approved by the CISO*.

   An updated corrective action plan must be submitted quarterly, *within 30 days after the end of each quarter*, until all corrective actions are completed. All corrective action plans submitted must have agency head approval.

2. *For each finding with which the Agency concurs:*
   - *a. Agency Finding Reference Field - Agency provided tracking ID;*
   - *b. Name - Name of finding;*
   - *c. Finding - Description of finding;*
   - *d. Affected Applications - List the applications affected by this finding;*
   - *e. Source Override - Audit;*
   - *f. Policy - Section Name - Reference to the applicable IT security control, i.e. AC-01 Access Control Policy and Procedures. Agency may select multiple values;*
   - *g. Magnitude of Impact - Select a high, medium or low effect of the finding;*
   - *h. Probability of Occurrence - Select a high, medium or low likelihood of the finding happening ;*
   - *i. Agency Submit Date - The date when the finding was submitted to CSRM;*
   - *j. Actual Remediation Date – The date the finding was resolved. This date is used to calculate closure;*
   - *k. Remediation Overview - Description of planned remediation steps;*
   - *l. Initial Planned Due Date – Estimated date the remediation be completed;*
   - *m. Responsible Person(s) - Who is responsible for the remediation;*
   - *n. Remediation Status - Not Started, Underway, Complete*
   - *o. Exception on File - Yes or No*
     NOTE: Agencies shall submit exceptions for findings that cannot be remediated within 90 days of the audit report.
   - *p. Remediation Response Update –Description of the remediation steps taken during each quarter*

3. For each finding with which the Agency does not concur:
    a. Audit Name;
    b. Audit Finding No.;
    c. Short Title;
    d. Agency Does Not Concur (Agency's statement of position); and
    e. Mitigating controls (that are in place and Agency's acknowledgment of their acceptance of the risk).

4. Any modification to a corrective action for any IT Security Audit conducted by or on behalf of the Agency must be reported.