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~~ *Enterprise* Architecture ~~(PPA)~~ *(EA)* Division. ~~PPA~~ EA 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~~ EA 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 2.1	August 06, 2012	Administrative changes to add Corrective Action Plan and IT Security Audit Quarterly Summary Template_excel.xlsx to section 2.5.4
Revision 2.2	January 6, 2013	Administrative changes to replace Short Title with SEC501-Control Number in section 2.5.4. See 2.1 and 2.5.4 #1 for clarification on required use of templates.
Revision 2.3	*December 8, 2016*	*This administrative update is necessitated by changes in the Code of Virginia and organizational changes in VITA. No substantive changes were made to this document.*

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.

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

Example with no change to text – The text is the same. The text is the same. The text is the same.

Example with revised text – This text is the same. *A wording change, update or clarification has been made in this text.*

Example of new section – *This section of text is new.*

REVIEW PROCESS

Enterprise Solutions and Governance Directorate Review

~~*Policy, Practices, and*~~ *Enterprise* Architecture ~~(PPA)~~ *(EA)* 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

ITRM Standard SEC502-02.3

Subject

Information Technology Security Audit Standard

Effective Date

December 8, 2016

Compliance Date

December 8, 2016

Supersedes

COV ITRM Standard SEC502-02.2 dated January 6, 2013

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 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)

~~***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 *approves* ~~*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.

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

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

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.

1.2.5 IT Security Auditors

IT Security Auditors are CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or a staff of a private firm that, in the judgment of the Agency, 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; and

c. Determining appropriate IT security measures.

1.4 IT Security Audits of *IT Systems*

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. All IT security audits must follow either the generally accepted government auditing standards GAGAS Yellow Book (**Generally Accepted Government Auditing Standards**) or the international standards for the professional practice of internal auditing IIA Red Book (Institute of Internal Auditors' Standards).

2. PERFORMANCE OF IT SECURITY AUDITS

IT Security Audits shall be conducted by personnel or organizations defined as IT Security Auditors in section 1.2.6, 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.

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 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 submission date.

Agencies are required unless otherwise approved by the CISO to use the IT Security Audit Plan Template found at: http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Word_versions/ITSecurityAuditPlanTemplate.doc .

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.

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 requirements of the Commonwealth of Virginia Information Security Standard (ITRM Standard SEC501). IT Security Auditors should also use standards that measure compliance with any other applicable Federal 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.

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.

For each finding with which the Agency concurs, the plan shall include the:

a. Planned corrective action;

b. Due date for the corrective action; and

c. Party responsible for the corrective action.

For each finding with which the Agency does not concur, the plan shall include the:

d. Agency's statement of position;

e. Mitigating controls that are in place; and

f. Agency's acknowledgment of its acceptance of risk.

Upon receipt of the plan, the IT Security Auditor shall incorporate the plan in the final IT Security Audit Report and present the final IT Security Audit Report to the Agency Head and the Agency Information Security Officer.

2.5.3 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.

2.5.4 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. Note: The official audit report submitted needs to include an attestation as to the audit standard used. (yellow or red book)

1. Agencies are required unless otherwise approved by the CISO to use the Corrective Action Plan Templates found at: http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/Word_versions/correctiveactionplantemplate.xlsx *or*

http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/Word_versions/Corrective_Action_Plan_Template.docx

2. For each finding with which the Agency concurs:
    a. Audit Name;
    b. Audit Finding No.;
    c. SEC501- Control Number;
    d. Summary;
    e. Agency Concurs;
    f. Planned Corrective Action;
    g. Responsible Person(s);
    h. Status;
    i. Due date (for the corrective action); and
    j. Exception on File (for findings not compliant with COV Information Security Standard (SEC501)).

3. For each finding with which the Agency does not concur:
    a. Audit Name;
    b. Audit Finding No.;
    c. SEC501- Control Number;
    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.

5. Corrective action plans for all findings must be submitted within 30 days of issuing the final audit report. An updated corrective action plan must be submitted quarterly (at the end of the quarter), until all corrective actions are completed. All corrective action plans and quarterly updates submitted must have evidence of agency head approval.

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