

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management

INFORMATION TECHNOLOGY RISK MANAGEMENT GUIDELINE

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

ITRM Publication Version Control: It is the user's responsibility to ensure that he or she has the latest version of the ITRM publication. Questions should be directed to the Associate Director for Policy, Practice and Architecture (PPA) at VITA's IT Investment and Enterprise Solutions (ITIES) Directorate. ITIES will issue a Change Notice Alert when the publication is revised. The Alert will be posted on the VITA Web site. An email announcement of the Alert will be sent to the Agency Information Technology Resources (AITRs) at all state agencies and institutions, as well as other parties PPA considers interested in the publication's revision.

This chart contains a history of this ITRM publication's revisions:

Version	Date	Purpose of Revision
Original	12/11/2006	Base Document. This guideline replaces section "A" of the Information Security Guideline (SEC2001-01.1) relating to "Business Analysis and Risk Assessment." This guideline expands on Risk Management best practices and provides several examples along with templates to assist with performing risk assessment documentation.

PREFACE

Publication Designation

ITRM IT Risk Management
Guideline SEC506-01

Subject

Information Technology Risk Management

Effective Date

September 1, 2006

Scheduled Review

One (1) year from effective date

Authority

Code of Virginia § 2.2-603(F)
(Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information
Technologies Agency; “VITA;” Appointment of
Chief Information Officer [CIO])

Scope

This *Guideline* is offered as guidance to all
Executive Branch State Agencies and institutions
of higher education (collectively referred to as
“Agency”) that manage, develop, purchase, and
use information technology (IT) resources in the
Commonwealth.

Purpose

To guide Agencies in the implementation of the
information technology risk management
requirements defined by ITRM Standard
SEC501-01, Section 2.

General Responsibilities

(Italics indicate quote from the Code of Virginia)

Chief Information Officer

In accordance with *Code of Virginia* § 2.2-2009,
the Chief Information Officer (CIO) is assigned
the following duties: *“the CIO shall direct the
development of policies, procedures and
standards for assessing security risks,
determining the appropriate security measures
and performing security audits of government
databases and data communications. At a
minimum, these policies, procedures, and
standards shall address the scope of security
audits and which public bodies are authorized to
conduct security audits.”*

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 IT systems and
data.

IT Investment and Enterprise Solutions Directorate

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

All Executive Branch State Agencies

In accordance with § 2.2-603, § 2.2-2005, and
§2.2-2009 of the *Code of Virginia*, all Executive
Branch State Agencies are responsible for
complying with all Commonwealth ITRM
policies and standards, and considering
Commonwealth ITRM guidelines issued by the
Chief Information Officer of the Commonwealth.

Definitions

Agency All Executive Branch State Agencies and
institutions of higher education that manage,
develop, purchase, and use IT resources in the
Commonwealth of Virginia (COV).

Agency Control - If an Agency is the Data
Owner of the data contained in a Government
database, that Agency controls the Government
database.

Audit scope - The boundaries of an audit,
including definition of what will and will not be
considered within the audit.

BIA - Business Impact Analysis – The process of
determining the potential consequences of a
disruption or degradation of business functions.

COOP – Continuity of Operations Plan – A set
of documented procedures developed to provide
for the continuance of essential business
functions during an emergency.

CISO - Chief Information Security Officer – The
CISO is the senior management official
designated by the CIO of the Commonwealth to
develop Information Security policies,
procedures, and standards to protect the
confidentiality, integrity, and availability of COV
IT systems and data.

Data - Data consists of a series of facts or
statements that have been collected, stored,

processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge

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. As used in this Guideline, Data Communications is included in the definition of government database herein.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner - An Agency manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

Government Database - For the purposes of this Guideline, the term “government database” shall include all components of any COV IT system in which a database resides, and also shall include state Data Communications, as defined herein. This definition of “government database” applies irrespective of whether the COV information is in a physical database structure maintained by COV or a third-party provider. This definition, however, does not include databases within Agencies that have been determined by the Agencies themselves to be non-governmental.

ISA - Interconnection Security Agreement - An agreement executed between the System Owners of interconnected IT systems when one or both systems processes, transmits, or stores sensitive data, as defined by the standards of the Agencies owning either system.

ISO – Information Security Officer - The individual who is responsible for the development, implementation, oversight, and maintenance of the Agency’s IT security program.

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

IT Security Auditor - CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or staff of a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT security audits.

IT System - An interconnected set of IT resources and data under the same direct management control.

Risk – The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA) – The process of identifying the vulnerabilities, threats, likelihood of occurrence, potential loss or impact, and theoretical effectiveness of security measures. Results are used to evaluate the level of risk and to develop security requirements and specifications.

Risk Management – The continuous process of determining, prioritizing, and responding to risks.

Risk Mitigation – The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Sensitive Data - 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 - COV IT systems that store, process, or transmit sensitive data.

System Owner -An Agency Manager responsible for the operation and maintenance of an Agency IT system.

Related ITRM Policy and Standards

ITRM Policy, SEC500-02, Information Technology Security Policy (Effective Date: 07/01/2006)

ITRM Standard SEC501-01: Information Technology Security Standard (Effective Date: 07/01/2006)

ITRM Standard SEC502-00: Information Technology Security Audit Standard (Effective Date: 07/01/2006)

TABLE OF CONTENTS

1 INTRODUCTION	1
1.1 Overview	1
1.2 IT Risk Management Process	1
2 IT SECURITY ROLES AND RESPONSIBILITIES.....	3
2.1 Overview	3
2.2 IT Security Roles and Responsibilities Assignment Process.....	3
3 BUSINESS IMPACT ANALYSIS.....	6
3.1 Overview	6
3.2 Business Impact Analysis Process	6
3.2.1 <i>BIA Requirements</i>	<i>7</i>
4 IT SYSTEM AND DATA SENSITIVITY CLASSIFICATION	8
4.1 Overview	8
4.2 IT System and Data Sensitivity Classification Process.....	8
5 IT SYSTEM INVENTORY AND DEFINITION	11
5.1 Overview	11
5.2 IT System Inventory and Definition Process.....	11
5.2.1 <i>Definition</i>	<i>11</i>
5.2.2 <i>IT System Ownership</i>	<i>12</i>
5.2.3 <i>IT System Boundaries</i>	<i>13</i>
5.2.4 <i>IT Systems Interoperability Security.....</i>	<i>15</i>
5.2.5 <i>Documentation.....</i>	<i>15</i>
6 RISK ASSESSMENT	16
6.1 Overview	16
6.2 Risk Assessment Process	17
6.2.1 <i>Background.....</i>	<i>17</i>
6.2.2 <i>Performance.....</i>	<i>17</i>
7 IT SECURITY AUDITS	17

7.1	Overview	17
7.2	IT Security Audit Process	18
7.2.1	<i>Background.....</i>	18
7.2.2	<i>IT Security Audit Plan (Plan)</i>	18
7.2.3	<i>IT Security Auditors.....</i>	18
7.2.4	<i>Types of IT Security Audits</i>	19
7.2.5	<i>IT Security Audit Execution</i>	19
7.2.6	<i>Corrective Action Plan (CAP)</i>	20
7.2.7	<i>CAP Reporting and Verification.....</i>	20
7.2.8	<i>Reporting of Agency IT Security Audit Results to CISO</i>	20
8	APPENDICES.....	21
	Appendix A: Security Roles and Responsibilities Example and Template.....	22
	Appendix B: IT System Inventory and Definition Example and Template.....	24
	Appendix C: Interoperability Security Agreement Example and Template.....	29
	Appendix D: Risk Assessment Instructions.....	32
	Appendix E: IT Security Audit Plan Example and Template	33
	Appendix F: Corrective Action Plan Example and Template	35

FIGURES

Figure 1	Risk Management Process Flow Chart.....	2
Figure 2	Sensitivity Classification	9
Figure 3	IT System Ownership Selection Process.....	13
Figure 4	IT System Boundary Process.....	15

TABLES

Table 1	IT Security Roles and Responsibilities	4
Table 2	IT Security Standard BIA Requirements Cross Walk to COOP Manual	7
Table 3	Classification Matrix Illustration.....	10

1 Introduction

1.1 Overview

In order to provide overall Information Technology (IT) security that is cost-effective and risk based, IT Risk Management must be a part of an agency's comprehensive risk management program. This Guideline presents a methodology for IT Risk Management suitable for supporting the requirements of the Commonwealth of Virginia (COV) *Information Technology Resource Management (ITRM) Information Technology Security Policy (ITRM Policy SEC500-02)*, the *COV ITRM Information Technology Security Standard (ITRM Standard SEC501-01)*, and the *COV ITRM Information Technology Security Audit Standard (ITRM Standard SEC502-00)*. These documents are hereinafter referred to as the "Policy," "Standard" and "Audit Standard," respectively.

The function of the Policy is to define the overall COV IT security program, while the Standard and the Audit Standard define high-level COV IT security and security audit requirements, respectively. This Guideline describes methodologies agencies may use in implementing the risk management requirements of the Policy, the Standard and the Audit Standard. In this Guideline, the methodologies are presented in the same order as presented in Section 2 – "Risk Management" of the Standard.

1.2 IT Risk Management Process

The purpose of IT risk management is to determine risks to sensitive IT systems, prioritize those risks and plan and respond to those risks in the COV that could result in material or significant negative impacts on essential business functions and the mission of agencies.

Figure 1 illustrates an approach to IT Risk Management. Activities in this process are often best accomplished as overlapping or parallel tasks.

This is because deeper or broader IT Risk Management information, needed by certain IT Risk Management activities is often obtained as other activities in the process take place. For that reason, it is suggested that previously completed tasks be revisited based on information derived from subsequently completed tasks. For example, information may be discovered during Business Impact Analysis (BIA), which helps to better define previously established IT system boundaries.

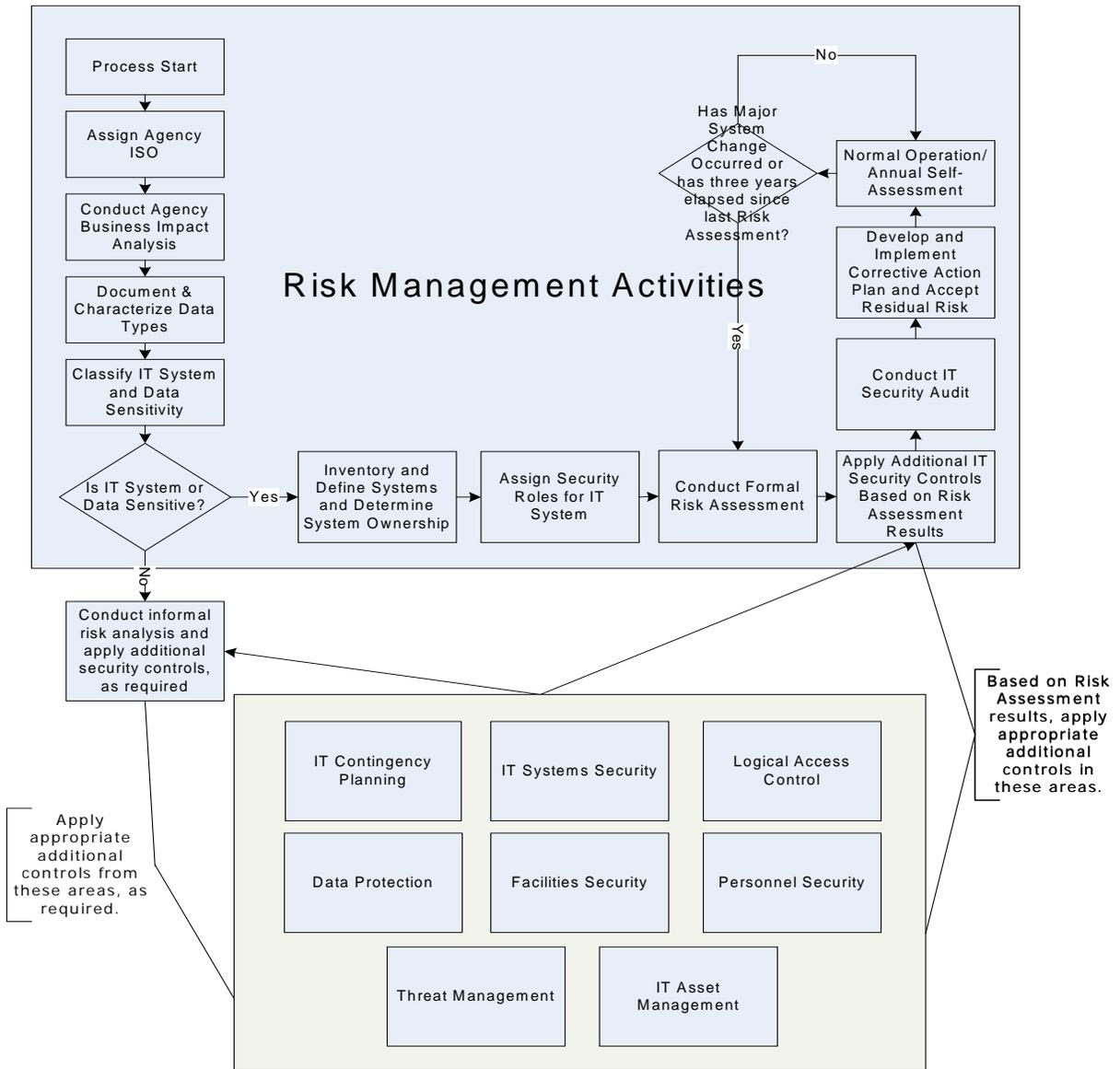


Figure 1 Risk Management Process Flow Chart

2 IT Security Roles and Responsibilities

2.1 Overview

The establishment of formal IT security roles and responsibilities delineates specific accountabilities for the protection and security of COV IT systems. Each Agency Head is ultimately accountable for protecting confidentiality, integrity and availability of the Agency's IT systems and data, and requires various IT Security roles to assist in providing this protection.

2.2 IT Security Roles and Responsibilities Assignment Process

There is a variety of IT Security roles in an effective IT Security program. Roles range from the Information Security Officer (ISO) with overall responsibility for the agency's IT Security program, to system-specific roles such as System Owner, Data Owner, System Administrator, and others as appropriate.

The Policy requires Agency Heads to designate an ISO, and strongly encourages the Agency Head to designate at least a backup ISO. To the extent practical, Agency Heads and ISOs are encouraged to assign a different person to each IT Security role. All security roles must be documented in the position description of the individual assigned to the role.

In smaller agencies, assigning a different person to each IT Security role may not be practical. In such cases, agencies should consider solutions such as having a single individual fulfill the role of ISO for several agencies, where practical.

Agencies are encouraged to go beyond the requirements of the Policy and Standard in assigning IT Security roles, where appropriate. For example, in cases where responsibilities for applications and infrastructure are divided, agencies are encouraged to designate two System Administrators, one with responsibility for applications security and one with responsibility for infrastructure security of the IT system.

Table 1, which begins on the next page, delineates each IT security role, the individual responsible for assigning the role, and role requirements, recommended qualifications, and responsibilities. Appendix A is a sample template for defining Agency IT security roles and responsibilities. System-specific roles (System Owner, Data Owner, System Administrator, and Data Custodian) should be documented in the System Inventory and Definition document for each IT system. (See Section 5 and Appendix B.).

Table 1 IT Security Roles and Responsibilities

Role	Designated By	Role Requirements	Recommended Qualifications	Responsibilities
Agency Head	Governor or Board, as defined by statute	Defined by Governor or Board, as defined by statute	Defined by Governor or Board, as defined by statute	Oversee Agency IT security program. <ul style="list-style-type: none"> • Designate ISO • Designate or delegate other Agency IT security roles • Review BIA, RA, COOP • Review IT Security Audit Plan & results of IT security audits • Monitor Corrective Action Plans (CAPs) • Report incidents that threaten the security of databases & data communications
ISO	Agency Head	<ul style="list-style-type: none"> • Must be a COV employee • Must not be a system or data owner • Should not exercise (or report to an individual who exercises) operational IT or IT security application or infrastructure responsibilities 	<ul style="list-style-type: none"> • In-depth knowledge of systems owned & of Agency's overall business • In-depth knowledge of Agency's IT and operating environment & requirements • Security Certifications¹ 	Overall security of Agency IT systems & liaison to the CISO of the Commonwealth <ul style="list-style-type: none"> • Develop/maintain IT security program as defined by Policy, Standard, and Audit Standard. • Assign (unless Agency Head assigns) other Agency IT security roles
Privacy Officer	Agency Head /ISO	At Agency Head's/ ISO's discretion	<ul style="list-style-type: none"> • In-depth knowledge of system owned & of Agency's overall business • In-depth knowledge of 	<ul style="list-style-type: none"> • Only mandatory if required by law or regulation • Responsibilities otherwise exercised by ISO • Provide guidance on privacy laws: <ul style="list-style-type: none"> • Disclosure of &

¹ IT Security certifications include Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified Information Security Auditor (CISA), among others.

Role	Designated By	Role Requirements	Recommended Qualifications	Responsibilities
			Agency's IT and operating environment & requirements • Security Certifications	access to sensitive data • Security & protection requirements in conjunction with IT systems when there is overlap among sensitivity, disclosure, privacy, & security issues
System Owner	Agency Head / ISO	<ul style="list-style-type: none"> • Required for all sensitive IT systems • Must be a COV employee • Must not be ISO or system administrator for system owned 	In-depth knowledge of system owned & of Agency's overall business	<ul style="list-style-type: none"> • Responsible for the overall security of the IT system • Accountable to the Agency Head • Manage IT system risk • Designate system administrator
Data Owner	Agency Head / ISO	<ul style="list-style-type: none"> • Required for all sensitive IT systems • Must be a COV employee • Must not be system administrator for system processing data owned • Must not be ISO 	In-depth knowledge of system owned & of Agency's overall business	<ul style="list-style-type: none"> • Promotes IT security awareness to data users • Develops additional requirements, guidelines & procedures needed to protect the data owned • Classify data sensitivity • Define data protection requirements for data owned & communicate requirements to System Owner • Define data access requirements • Designate Data Custodian
System Administrator	System Owner	<ul style="list-style-type: none"> • Required for all sensitive IT systems • Must not be ISO 	Required technical skills	<ul style="list-style-type: none"> • Day-to-day administration of the IT system • Implement requirements of the IT security program <p>Note: <i>Where responsibilities for applications & infrastructure are divided,</i></p>

Role	Designated By	Role Requirements	Recommended Qualifications	Responsibilities
				<i>two System Administrators may be designated, one with responsibility for applications security & one with responsibility for infrastructure security.</i>
Data Custodian (3 rd party in logical or physical possession of data)	Data Owner	<ul style="list-style-type: none"> • May be an individual or an organization (COV or partner) • Must not be ISO 	Required technical skills	<ul style="list-style-type: none"> • Protect data from unauthorized access, alteration, destruction, or usage • Operate IT systems in a manner consistent with COV IT security policies and standards
IT System Users	NA	NA	NA	<ul style="list-style-type: none"> • Read and comply with Agency IT security requirements • Immediately report potential and actual breaches of IT security • Protect security of IT systems and data

3 Business Impact Analysis

3.1 Overview

Business Impact Analysis (BIA) identifies essential business functions and assesses the impact to an agency's mission if these functions are disrupted. The role of BIA in IT Risk Management is to identify the IT systems that support essential business functions. These IT systems must be designated as sensitive with respect to availability and protected accordingly.

3.2 Business Impact Analysis Process

To fulfill the BIA requirements of the Standard, use the Virginia Department of Emergency Management's (VDEM's) *Continuity of Operations (COOP) Planning Manual*. The VDEM *COOP Planning Manual* contains instructions and worksheets to complete the Agency BIA process and may be downloaded from: <http://www.vaemergency.com/library/coop/resources/index.cfm>.

3.2.1 BIA Requirements

The BIA requirements of the Standard and the corresponding sections of the VDEM *COOP Planning Manual* that address those requirements are delineated in Table 2, which is shown on the following page. In September 2006 VDEM modified the BIA section of the *COOP Planning Manual* to include requirements of the Policy and the Standard.

Table 2 IT Security Standard BIA Requirements Cross Walk to COOP Manual

Requirements of the Standard, Section 2.3.2		VDEM COOP Planning Manual	
		Section	Worksheet
Identify	All Agency business functions.	II.A.1	10, 11
	Primary essential Agency business functions whose disruption or degradation would prevent the Agency from performing its mission during an event.	II.A.2	11, 12
	Secondary Agency business functions on which each essential function depends. Essential functions may depend upon functions not previously identified as essential & upon functions within & outside the Agency.	II.A.2	11, 12, 14
	Agency recovery time objectives for each primary & secondary essential business function, based on Agency and COV goals & objectives.	II.A.3	13, 14
	Resources that support each Agency's primary & secondary essential business function. If IT systems and/or data support a primary or secondary essential business function, the BIA must specify to what extent the essential business function depends upon the specific IT system and/or data.	II.A.3	15
	Dependencies of Agency primary & secondary essential business functions on specific IT systems and data. Specify the required	II.A.3	13

	recovery time for the IT systems and data on which a primary or secondary essential business function depends. These recovery time objectives must be based on COV & Agency goals and objectives and on the extent to which an essential business function depends upon the IT systems and data.		
Conduct	Periodic review and revision of the Agency BIA, as needed, but at least once every three years.	VII	NA

4 IT System and Data Sensitivity Classification

4.1 Overview

In order to provide IT security that is cost-effective and risk-based, agencies need to classify the sensitivity of the IT systems they own and the data they process. Sensitivity should be classified with respect to confidentiality, integrity, and availability. Determination of the agency's sensitive IT systems and data is fundamental to the IT Risk Management process. All subsequent activities in the IT Risk Management process flow from this determination.

The BIA described in Section 3 of this document classifies the IT systems that are sensitive with respect to availability. Classification identifies the systems subject to IT System Inventory and Definition, Risk Assessment and IT Security Audits, and assists in defining cost-effective and risk-based protections that are required by the IT systems and data.

4.2 IT System and Data Sensitivity Classification Process

The IT System and Data Sensitivity Classification process identifies the steps to inventory IT systems and data owned by the agency, and to classify these according to their sensitivity with respect to confidentiality, integrity and availability.

If the data processed, stored, or transmitted by an IT system is sensitive, the IT system itself is sensitive. Figure 2 illustrates the process of sensitivity classification.

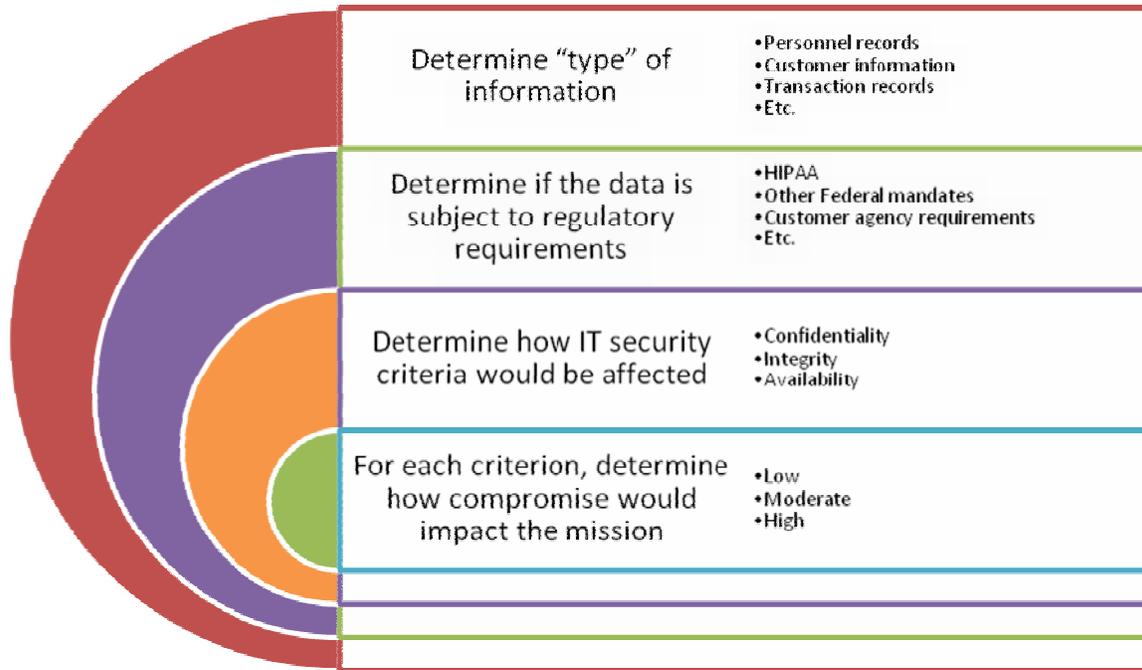


Figure 2 Sensitivity Classification

Following is one method for classifying the sensitivity of IT systems and data.

- 1) Identify the types of data processed by each agency-owned IT system. The designation of these data types may be unique to each agency and should be specific enough to provide clear differentiation among various types of data. Types of data, for example, may include personnel records, customer information, and public information, among others.
- 2) Determine if the data is subject to regulation by other agencies (Commonwealth or Federal), customer agency requirements, or other external requirements.
- 3) For each type of data, determine the level of impact of a compromise of :
 - **confidentiality**, which addresses the impact of unauthorized disclosure;
 - **integrity**, which addresses the impact of unauthorized modification; and
 - **availability**, which addresses the impact of outages, and is defined by the BIA.

Once the level of impact of a compromise is determined, classify the impact on the agency's mission, for each of the criteria of confidentiality, integrity and availability. Sensitivity classifications may be unique to each agency and should be specific enough to enable the agency to determine appropriate levels of protection for IT systems and data.

One method is to rate the impact of a compromise to confidentiality, integrity, and availability as “high”, “moderate” or “low”.

- **High** – *If compromised, the agency cannot perform a major portion of its mission.*
- **Moderate** – *If compromised, all elements of the agency mission can continue, but with significant degradation in quality or timeliness of information and service.*
- **Low** – *If compromised, all elements of the agency mission can continue with no visible adverse effect to agency customers.*

One method to perform this classification is to create a matrix like the example below:

Table 3 Classification Matrix Illustration

Type of Data	Sensitivity		
	Confidentiality	Integrity	Availability
Current Year Budget Details	Low Data is public information	High BFS is system of record for fiscal year budget data for all COV Agencies	Moderate Data is used less than daily by all COV Agencies to allocate resources
Future Year Budget Plans	High Release of the data before it is final could be damaging to COV and its Agencies	Moderate BFS is system of record for future year budget plans for all COV Agencies	Low/High Low during most of year; high during budget preparation
Agency Contact Information	Low Data is public information	Low BFS is not the system of record for this information	Low Data is available from other sources

If the level of impact on any of the criteria is rated “high,” the data and IT systems that store, process or transmit it are classified as “sensitive.” Agencies are strongly encouraged to classify IT systems as sensitive if a type of data handled by the IT system has a sensitivity of moderate on any of the criteria of confidentiality, integrity or availability.

As an example, personal contact information includes data that could be used in identity theft or to target individuals for other crimes. A compromise of this information could impact the agency’s credibility to a point where it would be difficult to execute its mission. In this case, a compromise of confidentiality is rated “high.”

Since personal contact information must be accurate to be useful, compromise of integrity would significantly degrade the quality of information and is rated “moderate.” Lastly, since the data cannot be used if it is not available, compromise of availability would significantly degrade the timeliness of service and is also rated “moderate.”

Because at least one of the criteria has been rated “high,” the sensitivity of the data type “Personal Contact Information” as well as any IT system that handles the data must also be classified as “sensitive.”

A matrix for classifying data sensitivity is included as part of the IT System Inventory template and as an example in Appendix B. The System Inventory and Definition document for each sensitive IT system should include a summary of the previously determined sensitivity level(s) of the data handled by the IT system. This description should explain the rationale for the data sensitivity classifications and the sensitivity classification of the IT system as a whole.

5 IT System Inventory and Definition

5.1 Overview

Systems are classified as sensitive or non-sensitive through the IT System and Data Sensitivity Classification process outlined in Section 4. The IT System Inventory and Definition process is required only for those systems classified as sensitive, but is encouraged for all systems.

In order to analyze a sensitive IT system for security risks and to protect the confidentiality, integrity and availability of the IT system, the System Owner must have a clear understanding of the components and boundaries of the IT system and how the IT system supports the agency.

A definition of each sensitive IT system owned by an agency provides an understanding of the IT system and assists in determining IT security roles and responsibilities. This process of IT system inventory and definition for sensitive IT systems assists in defining cost-effective, risk-based security protection for these IT systems, for the agency as a whole, and for the COV.

5.2 IT System Inventory and Definition Process

IT System Inventory and Definition refers to the process of defining all the sensitive IT systems owned by an agency.

5.2.1 Definition

Initially, in order to begin the definition process, some assumptions concerning the IT system boundaries have to be made. In general, and to the extent practical, each IT system supports a single major business function. For example, an agency e-mail system supports the major business function of communication, even though it is used by multiple different functional areas within the agency. The IT system

definition should include the characteristics that will help determine IT system ownership and the IT system boundaries. These characteristics include:

- major business function supported;
- IT system interfaces;
- ownership characteristics (e.g. wholly owned, leased, managed service contract, etc.);
- determination of data and IT system sensitivity - data is a component of an IT system; if data is sensitive, the IT system is sensitive; and
- IT Security Roles, including System Owner, Data Owner, System Administrator, and Data Custodian.

Exceptions to the general case in which each IT system supports a single major business function include systems that support multiple other systems (“support systems”) such as mainframe computers, enterprise networks, and general controls. These support systems should be separately defined, assessed for risk and included in IT Security Audits. The Risk Management activities conducted for the support systems can then be relied upon in the Risk Management activities for the IT systems they support.

For example, many organizations find it convenient and effective to define a support system consisting of the organizations enterprise network, end-user computing devices and office automation applications. Risk Management activities are conducted once for this support system; applications that use this infrastructure then rely upon these Risk Management activities and incorporate them by reference rather than repeating them.

Separate system definitions, risk assessments and IT Security Audits must be conducted for each distinct IT system. For example, a web-based application system may rely on and incorporate by reference the system definition, risk assessment, and IT Security Audit conducted for the enterprise network that it uses for transport. Separate system definition, risk assessments, and IT Security Audits must be conducted for the portions of the web-based application system that are not part of the enterprise network support system.

Appendix B contains an example of an IT System Inventory and Definition and a blank template.

5.2.2 IT System Ownership

For the purposes of this guideline, the System Owner is defined as the COV employee designated by the Agency Head or the ISO to be responsible for the

security of a particular IT system. To provide effective IT security through adequate separation of duties, the agency's ISO may not be a System Owner.

In most cases, it will be clear that a given agency is the owner of an IT system for IT security purposes. In these cases, the Agency Head or ISO, if appropriate, designates the System Owner. In cases where more than one agency claims the IT system, the agencies either negotiate who will be the owner for IT security purposes and designate the System Owner or request the CIO of the Commonwealth make the determination, as illustrated by the process map in Figure 3.

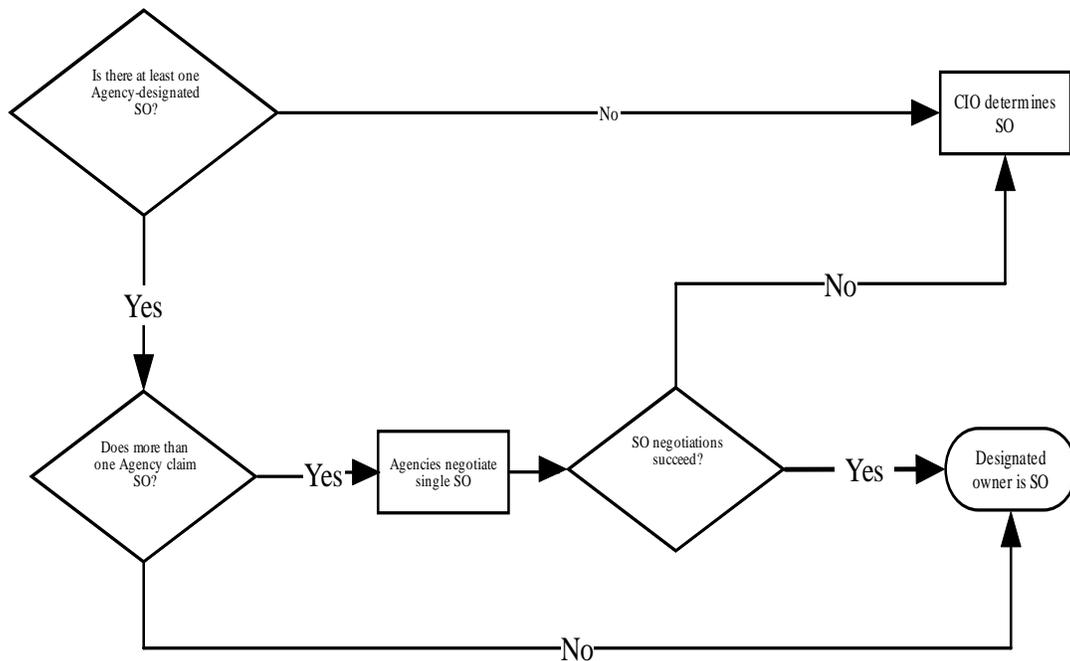


Figure 3 IT System Ownership Selection Process

5.2.3 IT System Boundaries

Determining IT system boundaries is a method of defining the IT system so that a single System Owner may control its security. A defined system boundary is essential to managing risks to a particular IT system.

A key to determining IT system boundaries is to examine the points where IT systems meet one another and to define the dividing lines between or among the IT systems. These dividing lines include not only physical connections, but also logical connections where data is exchanged.

The owner of each IT system and the owners of the data handled by each system must agree on the boundaries between or among the systems, so that all components are the responsibility of someone, and no components are covered more than once. IT system boundaries should be based on non-arbitrary characteristics, such as funding boundaries, functional boundaries, physical gaps, contractual boundaries, operational boundaries, and transfer of information custody.

The steps to determine the boundaries of an IT system, as illustrated in Figure 4, are:

- 1) choose an IT system from the IT systems inventory for consideration;
- 2) if the IT system does not support a single major business function or does not have a single System Owner, break it up into smaller IT systems, unless the IT system is a support system such as a mainframe computer, an enterprise network or general security controls;
- 3) adjust the agency's IT system inventory to reflect the refined IT system boundaries; and
- 4) record the system boundary information in the IT System Inventory and Definition document for each IT system.

(Refer to IT System Inventory and Definition example in Appendix B.) The system boundary information for each IT system should detail:

- the primary components of the IT system, including information regarding
 - system hardware (e.g., servers, routers, switches), and
 - software (e.g., applications, operating system, protocols);
- system interfaces (e.g., communication links), including
 - the purpose of each interface, and
 - the relationship between the interface and the system; and
- a description of the IT system boundary.

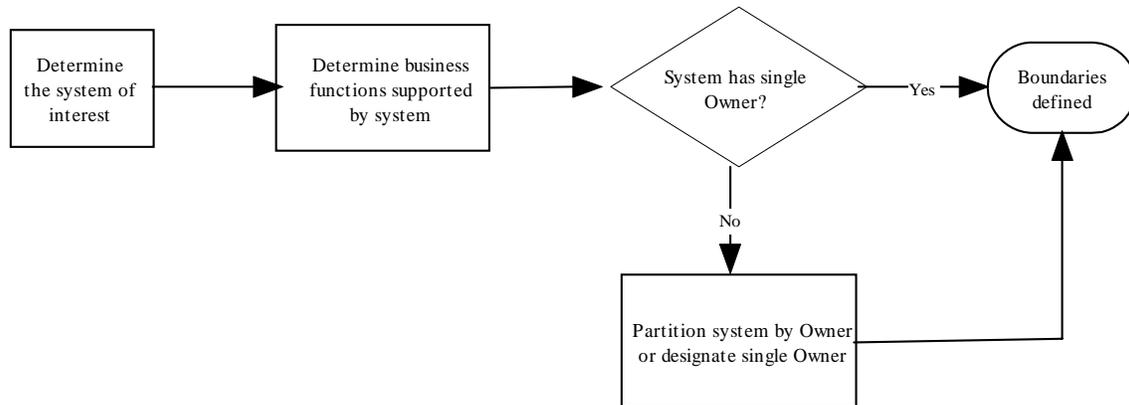


Figure 4 IT System Boundary Process

5.2.4 IT Systems Interoperability Security

Once the boundaries of an IT system have been established, and the inventory finalized, the System Owner should determine if the IT system connects to other IT systems through any of its system interfaces. If it does, the System Owner is responsible for documenting an Interoperability Security Agreement (ISA) with the System Owner of each IT system to which it connects. Section 4.3 of the Standard describes these requirements.

The ISA describes the IT systems being connected, the nature of the sensitive information and it delineates a simple agreement that each interconnected IT system will implement controls in accordance with the risk assessments of both IT systems.

Appendix C contains an example of an ISA and a template for use in completing an ISA. The status of ISAs should also be documented in the System Inventory and Definition document (see this Section and Appendix B).

For connections between IT systems that are owned by a common System Owner, the System Owner should describe the IT systems being connected and the nature of the sensitive information. A formal, signed agreement, however, is not required for connections between IT systems that are owned by a common System Owner.

5.2.5 Documentation

After the definition of IT systems is complete, it is important to document clearly the extent and limits of each IT system in order to provide security that is risk-based and cost-effective to each system. To meet this need, each sensitive IT System requires a formal definition document that includes:

- the full name of the IT system, any acronym that it uses, any other system designator or identifier and the purpose of the system;
- the Agency that owns the IT system, including

- individuals assigned responsibilities as System Owner and Data Owner(s),
- the organization(s) that manage and/or administer the IT system and its components and
- key operational and technical support personnel;
- the physical location of the IT system; and
- any other details regarding the IT system that are relevant to providing risk-based and cost-effective security for the IT system.

Appendix B contains an example of an IT system inventory and definition and a blank template. The information documented in the IT system inventory and definition is a primary input to the Risk Assessment of the IT System (see Section 6 and Appendix D).

6 Risk Assessment

6.1 Overview

To meet the requirements of the Standard, each agency-owned IT system classified as sensitive must have a Risk Assessment (RA). RA is the process of identifying vulnerabilities, threats, likelihood of occurrence, and potential loss or impact.

RA of sensitive IT systems and data:

- protects against threats that are most likely to occur and have the potential to cause the greatest damage;
- assists in identifying security controls that most effectively protect confidentiality, integrity, and availability of agency IT systems and the information they process; and
- helps organizations evaluate the type and level of risks and develop security requirements and specifications.

Results are used to evaluate the type and level of risks and to develop security requirements and specifications. Organizations use RA to determine the overall vulnerability of their sensitive IT systems and data to threats.

In order to provide risk-based and cost-effective controls for sensitive IT systems and data, it is necessary to protect against threats that are most likely to occur and have the potential to cause the greatest damage. RA of sensitive agency IT systems and data assists in identifying security controls that most effectively protect confidentiality, integrity, and availability of agency IT systems and the information they process.

This Guideline recommends one method to prepare a RA appropriate to sensitivity of the assessed IT resources. The Risk Assessment Template provided in Appendix D (under separate cover due to its length) contains definitions and instructions for assessing risk and documenting results using this method.

6.2 Risk Assessment Process

6.2.1 Background

The risks to IT systems and data changes over time, as does the environment in which they operate. Periodic risk assessments help to assess whether the IT security controls in place for IT systems continue to be commensurate with sensitivity and risk. The Standard requires a risk assessment of each sensitive IT system at least once every three years. An RA is valid only if it is current, so the Standard also requires an annual self-assessment to determine the continued validity of the formal RA. Validity may be affected by major changes to the IT system, system interfaces or the environment.

Major changes are defined as substantial changes that alter the mission, configuration or basic vulnerabilities of the IT system. Changes that may indicate the need for a new RA include new or significantly changed

- Business Requirements,
- Hardware,
- Application Programs,
- External Users,
- Telecommunications,
- Location of the IT system (e.g. a new physical environment or a new organization) and
- IT System Interfaces.

Minor changes that may not require a new risk assessment include such events as the replacement of existing hardware with similar hardware when capacity does not significantly change; the addition of two or three workstations on a network; or small modifications to an application program (e.g., a change in table headings).

6.2.2 Performance

The Risk Assessment Instructions (Appendix D, published separately due to its length) may be used to perform and document agency risk assessments. These instructions include explanations for participants, analysis techniques and methodologies. Agencies may select another RA methodology to meet specific agency requirements.

7 IT Security Audits

7.1 Overview

IT Security Audits are vital to governance and control of enterprise information assets. This Guideline prescribes actions to enhance Commonwealth security by defining the process for performing IT Security Audits

7.2 IT Security Audit Process

7.2.1 Background

IT Security Audits assess the results of risk management and the effectiveness of IT security controls. The IT Security Audit Standard requires IT Security Audits be performed on a frequency relative to the risk identified by the agency. At a minimum, sensitive IT systems must undergo an IT security audit once every three years.

7.2.2 IT Security Audit Plan (Plan)

The purpose of the plan is to ensure all government databases under agency control are audited on a frequency commensurate with sensitivity and risk. The agency uses the plan to:

- 1) document the systems to be audited and the frequency of the audits;
- 2) establish an audit schedule;
- 3) define the audit requirements;
- 4) identify the planned auditor; and
- 5) coordinate the audit schedule.

As noted in Section 5, in general, and to the extent practical, each sensitive IT system should support a single major business function. Exceptions to this general case include systems that support multiple other systems (“support systems”) such as mainframe computers, enterprise networks, and general controls. Each agency’s plan should include all sensitive IT systems for which it is System Owner, and should include scheduled audits at a frequency commensurate with sensitivity and risk. In addition, as outlined in Section 5, audits of application systems that make use of support systems, such as infrastructure systems and general controls should rely on the IT Security Audits of the support systems.

By February 2007 and annually thereafter, each agency must develop an IT Security Audit Plan encompassing all of the sensitive IT systems for which the respective agency is the owner. Each agency must also provide its IT Security Audit Plan to the CISO.

Appendix E contains an example of a plan and a blank template.

7.2.3 IT Security Auditors

As defined in the Audit Standard, IT Security Audits may be conducted by CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or staff of a private firm that, in the judgment of the agency, has the experience and expertise required to perform IT Security Audits.

In planning IT Security Audits, and in developing its plan, each agency should consider audits already scheduled or underway and not duplicate audits solely for the purposes of complying with the Audit Standard. Each agency must document Audits already scheduled or underway in its plan.

If an agency 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.

If an agency elects to engage a private firm to conduct IT Security Audits, it is suggested that Agencies consider the following criteria in selecting such a firm:

- the firm's experience in conducting similar audits;
- the firm's previous experience in working with COV agencies; and
- the firm's general reputation.

If any agency has engaged a firm to assist in documenting its security program, policies or procedures, it shall not engage the same firm to conduct the IT Security Audits.

7.2.4 Types of IT Security Audits

The agency determines when, how, and by whom agency-directed IT Security Audits will occur. The results of the agency Business Impact Analysis (BIA), data sensitivity and risk assessments should guide the priorities for, and scope of, agency-directed IT Security Audits. To reduce the number of IT Security Audits of the same IT system scheduled closely together (e.g. the Auditor of Public Accounts requests a security audit beginning one month after a planned Agency-directed audit), the agency should use the plan as a tool to coordinate scheduling.

The CISO may also conduct IT Security Audits as circumstances warrant.

7.2.5 IT Security Audit Execution

The execution of agency-directed audits is the sole responsibility of the Agency Head. Prior to the audit, the Agency Head or designee should conduct a meeting with the Auditor to set the scope of the audit.

Each IT Security Audit should assess the overall effectiveness of the IT system controls and measure compliance with the Policy, Standard and any other applicable laws, regulations, policies or procedures. The audit should evaluate

whether the controls in place provide protection of the IT system and data that is commensurate with sensitivity and risk.

In conducting this assessment, IT Security Auditors may wish to make use of frameworks such as The Control Objectives for Information and related Technology (COBIT), International Standards Organization (ISO) 20000, and ISO 17799. In making use of these frameworks, however, IT Security Auditors should keep in mind that the overall purpose of the audit is not to measure compliance with these frameworks, but, as noted above, to evaluate whether the controls in place provide protection of the IT system and data that is commensurate with sensitivity and risk.

7.2.6 Corrective Action Plan (CAP)

Once the IT Security Auditor has issued the preliminary security audit report, the agency prepares a CAP that describes, for each audit finding, whether the agency concurs. If the agency concurs, the CAP should document the corrective action, responsible person, and due date. If the agency does not concur, the CAP should state the agency's position and any mitigating controls. The CAP should be incorporated in the final IT Security Audit Report presented to the agency by the IT Security Auditor.

7.2.7 CAP Reporting and Verification

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 in implementing outstanding corrective actions. In addition, upon completion of the CAP, the responsible Agency Head or designee shall arrange for a follow up review to assess the effectiveness of the corrective actions.

7.2.8 Reporting of Agency IT Security Audit Results to CISO

At least once each quarter, the agency will forward to the CISO a report listing all IT Security Audits conducted by or for the agency. The report contains:

- 1) a list of all the findings and whether the agency concurs;
- 2) for each finding with which the agency concurs, a description of the corrective action the agency will take, the expected completion date, and the responsible person;
- 3) for each finding with which the agency does not concur, a description of the agency's position, any controls in place that mitigate the finding, and a statement of risk acceptance; and
- 4) the status of outstanding corrective actions for all IT Security Audits conducted by or on behalf of the agency previously.

The agency may select to create the required report by compiling all CAPs for audits completed in the previous quarter and audits previously completed with

outstanding corrective actions, and submitting them with an appropriate cover letter.

An example of a Corrective Action Plan report and a blank template are contained in Appendix F.

The CISO uses the report along with reports from other agencies, to understand the overall information security posture and readiness of Executive Branch Agencies. This understanding assists the CISO in developing and improving Commonwealth information security policies, standards and guidelines.

8 8 Appendices

These Appendices provide examples and templates that agencies may use to document their use of many of the methodologies described in this Guideline. Each template consists of an example of the document completed with fictional information and a blank version of the template for use by COV agencies.

The examples use different fonts for instructions and example information, as follows.

- Times New Roman text is used for the template itself.
- **Shaded Arial Bold text** indicates example text.
- *Times New Roman Italic text* is provided as instructions for completing the template.

The Risk Assessment Instructions in Appendix D, published under separate cover because of the length, use slightly different fonts for instructions and examples, as documented in the Risk Assessment Instructions.

Appendix A: Security Roles and Responsibilities Example and Template

IT System Name, Acronym, and Designation	Budget Formulation System (BFS) BFA-001			
Role	Responsibility	Name	Reports to (Name and Title)	Assignment Date
Agency Head	Oversee Agency IT Security Program	John Davis	Governor	01/01/04
Information Security Officer	Overall security of Agency IT systems and liaison to the CISO of the Commonwealth.	Jane Jones	John Davis, BFA Agency Head	11/12/05
Privacy Officer	Provide guidance on privacy laws.	Roberta Richards	John Davis	07/01/05
System Owner	Responsible for the overall security of the IT system. Accountable to the Agency Head.	John James	Pete Keller, BFA CIO	11/13/06
Data Owner	Spreads IT security awareness to data users. Develops any additional local requirements, guidelines and procedures needed to protect the data.	Mike Williams Bill Michaels	Jim Johnson, BFA Budget Analysis Director	11/14/06
System Administrator	Day-to-day administration of the IT system. Implements requirements of the IT Security Management Program.	Bea Roberts	Partner Services, Inc.	11/15/06
Data Custodian	Protect data from unauthorized access, alteration, destruction, or usage and in a manner consistent with COV IT security policies and standards	Partner Services, Inc.	Partner Services, Inc.	11/15/06
IT System Users	Read/comply with Agency IT security requirements	All users	Current	Current

IT System Name, Acronym, and Designation				
Role	Responsibility	Name	Reports to (Name and Title)	Assignment Date
Agency Head	Oversee Agency IT Security Program			
Information Security Officer	Overall security of Agency IT systems and liaison to the CISO of the Commonwealth.			
Privacy Officer	Provide guidance on privacy laws.			
System Owner	Responsible for the overall security of the IT system. Accountable to the Agency Head.			
Data Owner	Spreads IT security awareness to data users. Develops any additional local requirements, guidelines and procedures needed to protect the data.			
System Administrator	Day-to-day administration of the IT system. Implements requirements of the IT Security Management Program.			
Data Custodian	Protect data from unauthorized access, alteration, destruction, or usage and in a manner consistent with COV IT security policies and standards			
IT System Users	Read/comply with Agency IT security requirements			

Appendix B: IT System Inventory and Definition Example and Template

IT System Inventory and Definition Document			
I. IT System Identification and Ownership			
IT System ID	BFA-001	IT System Common Name	Budget Formulation System (BFS)
Owned By	Budget Formulation Agency (BFA) Financial Operations Division (FOD)		
Physical Location	BFA Data Center 123 E. Elm Street, Richmond, VA 23299		
Major Business Function	Enable processing of current-year budget details and future-year budget plans		
System Owner Phone Number	John James (804) 979-3757	System Administrator(s) Phone Number	Partner Systems, Inc. (888) 989-8989
Data Owner(s) Phone Number(s)	Mike Williams (804) 979-3452 Bill Michaels (804) 979-3455	Data Custodian(s) Phone Number(s)	Bea Roberts Partner Systems, Inc. (888) 989-8989
Other Relevant Information	BFS has been in production since December 1996		
II. IT System Boundary and Components			
IT System Description and Components	<p>BFS is a distributed client-server application transported by a network provided by PSI, a third-party. The major components of the BFS include:</p> <ul style="list-style-type: none"> • A Sparc SUNW, Ultra Enterprise 3500 server running SunOS 5.7 (Solaris 7). The server has four (4) processors running at 248 MHz, 2048 MB of memory, 4 SBus cards, 4 PCI cards, and total disk storage capacity of 368.6 GB (36 drives x 10 GB). This system is provided to BFA under contract by PSI, and this Risk Assessment relies on information regarding system hardware and Operating System software provided to BFA by PSI. • One (1) network interface that is connected to BFA's data center Cisco switch. This interface is assigned two unique IP addresses. • An Oracle 9i data store with two (2) commercial off-the-shelf (COTS) application modules (ABC and XYZ) purchased from Oracle Corporation. 		

<p>IT System Interfaces</p>	<ul style="list-style-type: none"> • An interface between BFS and the Budget Consolidation System (BCS). This interface allows only the BCS to securely transmit data using the Secure Copy Protocol (SCP) on port 22 into the BFS nightly by a cron job that refreshes tables in the BFS Oracle store with selected data from BCS tables. • A modem for emergency dial-in support and diagnostics, secured via the use of a one-time password authentication mechanism. • Client software located within the Agency's Windows 2003 Server Active Directory Domain to manage access to BFS. This software utilizes encrypted communications between the client and the server and connects to the server on port 1521. Only users with the appropriate rights within the BFA Domain can access the client software, although a separate client login and password is required to gain access to BFS data and functions. This access is based on Oracle roles and is granted by the BFS system administrators to users based on their job functions. • Use of the PSI-provided network to transport BFS data.
<p>IT System Boundary</p>	<ul style="list-style-type: none"> • The demarcation between the BFS and the Local Area Network (LAN) is the physical port on the Cisco switch that connects the BFS to the network. The switch and other network components are not considered to be part of the BFS. • BFS support personnel provide the operation and maintenance of the application. The BFS personnel provide the operation and maintenance of the server and operating system. The BFS boundary is the following directories and their sub-subdirectories: /var/opt/Oracle, /databases/Oracle, and /opt/odbc. Other directories are outside the BFS boundary. • BFS is responsible for receiving data from the BCS. The BCS is a separate system and is outside the BFS boundary. • Client access to the BFS server is controlled by BFA's Windows 2003 Server Active Directory domain. This access are included within the BFS system boundary. The overall BFA Windows 2003 Server Active Directory domain, however, is not considered to be part of the BFS, and is outside the BFS boundary.

III. IT System Interconnections				
Agency or Organization	IT System Name	IT System ID	IT System Owner	Interconnection Security Agreement Summary
BFA	Budget Consolidation System	BCS	John James	No formal agreement required, as systems have common owner
BFA	IT Infrastructure System (Active Directory)	BFAITIS	John James	No formal agreement required, as systems have common owner
Partner Services, Inc. (PSI)	Enterprise Data Network	EDN	Bea Roberts	Agreement is in place; expires 12/31/2007; under renegotiation

IV. IT System and Data Sensitivity			
Type of Data	Sensitivity Ratings Include Rationale for each Rating		
	Confidentiality	Integrity	Availability
Current Year Budget Details	Low Data is public information	High BFS is system of record for fiscal year budget data for all COV Agencies	Moderate Data is used less than daily by all COV Agencies to allocate resources
Future Year Budget Plans	High Release of the data before it is final could be damaging to COV and its Agencies	Moderate BFS is system of record for future year budget plans for all COV Agencies	Low/High Low during most of year; high during budget preparation
Agency Contact Information	Low Data is public information	Low BFS is not the system of record for this information	Low Data is available from other sources

Overall IT System Sensitivity Rating and Classification	Overall IT System Sensitivity Rating Must be “high” if sensitivity of any data type is rated “high” on any of the criteria	
	<input checked="" type="checkbox"/> HIGH LOW	<input type="checkbox"/> MODERATE
	IT System Classification Must be “Sensitive” if overall sensitivity is “high”; consider as “Sensitive” if overall sensitivity is “moderate”	
	<input checked="" type="checkbox"/> SENSITIVE SENSITIVE	

IT System Inventory and Definition Document				
I. IT System Identification and Ownership				
IT System ID		IT System Common Name		
Owned By				
Physical Location				
Major Business Function				
System Owner Phone Number		System Administrator(s) Phone Number		
Data Owner(s) Phone Number(s)		Data Custodian(s) Phone Number(s)		
Other Relevant Information				
II. IT System Boundary and Components				
IT System Description and Components				
IT System Interfaces				
IT System Boundary				
III. IT System Operability and Agreements				
Agency or	IT System	IT	IT System	Interoperability

Appendix C: Interoperability Security Agreement Example and Template

Memorandum of Understanding

May 30, 2006

Memorandum of Understanding

This Memorandum of Understanding comprises an Interoperability Security Agreement (ISA) between the System Owners of the **Budget Formulation System (BFS), system ID BFA-001** “owned” by the **Budget Formulation Agency** and the **Commonwealth Enterprise Network (CEN), system ID NET-001** “owned” by the **Commonwealth Network Agency**. The interoperability between BFS and CEN provides the transport of BFS data using the CEN.

Type of Data	Sensitivity Ratings		
	Confidentiality	Integrity	Availability
Current Year Budget Details	Low Data is public information	High BFS is system of record for fiscal year budget data for all COV Agencies	Moderate Data is used less than daily by all COV Agencies to allocate resources
Future Year Budget Plans	High Release of the data before it is final could be damaging to COV and its Agencies	Moderate BFS is system of record for future year budget plans for all COV Agencies	Low/High Low during most of year; high during budget preparation
Agency Contact Information	Low Data is public information	Low BFS is not the system of record for this information	Low Data is available from other sources

The System Owners of the two IT systems agree to the following:

- To maintain the security of their respective IT systems in accord with the controls specified by the most current risk assessment for each IT system. This requires each System Owner to share the applicable security requirements of their respective IT systems with each other.
- To inform the other of any significant changes to the risks to their respective IT systems. This includes any major configuration changes as defined by ITRM Standard SEC501-01.
- To inform the other, in a timely and deliberate manner, of any security breaches to their respective IT systems.

This ISA shall remain in force until **June 30, 2007** unless jointly re-accomplished by the ISOs.

John James, Budget Formulation Agency

Date

Robert Brown, Commonwealth Network Agency

Date

Memorandum of Understanding

This Memorandum of Understanding comprises an Interoperability Security Agreement (ISA) between the System Owners of the _____ “owned” by the _____ and the _____ “owned” by the _____. The interoperability between _____ and _____ provides _____. The table below outlines the nature of the sensitive data shared between the systems:

Type of Data	Sensitivity Ratings		
	Confidentiality	Integrity	Availability

The System Owners of the two IT systems agree to the following:

- To maintain the security of their respective IT systems in accord with the controls specified by the most current risk assessment for each IT system. This requires each System Owner to share the applicable security requirements of their respective IT systems with each other.
- To inform the other of any changes to the risk profile of their respective IT systems. This includes any major configuration changes as defined by ITRM Standard SEC501-01.
- To inform the other, in a timely and deliberate manner, of any security breaches to their respective IT systems.
- *(include additional Agency-specific requirements here).*

This ISA shall remain in force until _____ unless jointly re-accomplished by the ISOs.

Date

Date

Appendix D: Risk Assessment Instructions

Please note: this Appendix is large and is published under separate cover.

Appendix E: IT Security Audit Plan Example and Template

PURPOSE: This Plan coordinates the execution of security audits for the IT systems supporting government databases (as defined by ITRM Standard SEC502-00).

IT Security Audit Plan

Agency Name and Acronym	IT Security Audit Plan				
	Date Submitted	Submitted By			
Budget Formulation Agency (BFA)	01/02/2008	Name & Title	Phone Number	E-mail Address	
		Jane Jones, BFA ISO	(804) 979-2461	jane.jones@bfa.virginia.gov	
IT System Name, Acronym, and Designation	Expected Auditor	Next Three Planned Audit Dates Fiscal Years			Areas for Special Emphasis and Additional Audit Requirements [‡]
		2008	2009	2010	
Budget Formulation System (BFS) BFA-001	The Auditing Firm	1 st quarter		1 st quarter	a) Security procedures for laptop use at employee homes. b) Policies regarding protection of mobile storage (flash drives, DVDs, etc.)
Budget Consolidation System (BCS) BFA-002	APA	2 nd quarter			a) IRS 1075 requirements. b) Requirements for users to complete background checks before receiving BCS access.
Budget Reconciliation System (BRS) BFA-003	BFA Internal Audit Staff	3 rd quarter	3 rd quarter	3 rd quarter	a) Security controls governing remote access to BRS data

[‡] All IT Security Audits must evaluate overall effectiveness of controls, as well as compliance with the IT Security Policy (ITRM Policy SEC500-02), Standard (ITRM Standard SEC501-01), and any other applicable laws, regulations, policies, or procedures. Use this column to indicate any audit areas that require special attention or any additional audit requirements.

IT Security Audit Plan

Agency Name and Acronym	IT Security Audit Plan				
	Date Submitted	Submitted By			Areas for Special Emphasis and Additional Audit Requirements [‡]
		Name & Title	Phone Number	E-mail Address	
IT System Name, Acronym, and Designation	Expected Auditor	Next Three Planned Audit Dates Fiscal Years			Areas for Special Emphasis and Additional Audit Requirements [‡]
		2008	2009	2010	

[‡] All IT Security Audits must evaluate overall effectiveness of controls, as well as compliance with the IT Security Policy (ITRM Policy SEC500-02), Standard (ITRM Standard SEC501-01), and any other applicable laws, regulations, policies, or procedures. Use this column to indicate any audit areas that require special attention or any additional audit requirements.

Appendix F: Corrective Action Plan Example and Template

PURPOSE: This Plan describes IT Security Audit findings; documents responsibility for addressing the findings; and describes progress towards addressing the findings. *Provide enough information to enable the reader to understand the nature of the finding, the impacts, and the planned remedy.*

IT Security Audit Quarterly Summary

Audit Name: Budget Formulation System (BFS) BFA-001; Issued 03/08

Audit Finding No. & Agency Concurrence	Short Title	Summary	Risk	Responsible Person(s) and Due Date	Status*	Status Date	Concurs: Planned Action & Status Does Not Concur: Mitigating Controls & Risk Acceptance
1 BFA Concurs	Develop Policy for Storage of Sensitive BFS Data on Mobile Devices	BFA should develop and enforce policies and procedures requiring Agency Head approval for storage of sensitive BFS data on mobile devices, including employee laptops, USB drives, CDs, and DVDs.	Compromise of confidentiality of BFS data	John James 09/08	U	9/15/08	Policies and procedures have been developed; implementation is underway and will be completed this month.
2 BFA Concurs	Enforce BFA Account Management Procedures for BFS	BFA should enforce existing Agency procedures to remove unneeded accounts from BFS.	Compromise of confidentiality and integrity of BFS data	Bill Michaels Michael Williams 09/08	U	09/15/08	Procedures for removal of unneeded BFS accounts are now being enforced; review of all BFS accounts to identify and remove unneeded accounts is underway and will be completed this month.

* Status Legend: NS = Not Started; U = Underway; C = Completed

Audit Finding No. & Agency Concurrence	Short Title	Summary	Risk	Responsible Person(s) and Due Date	Status*	Status Date	Concurs: Planned Action & Status Does Not Concur: Mitigating Controls & Risk Acceptance
3 BFA Concurs	Enforce Password Change Requirements on BFS	BFA should enforce existing Agency requirements for password changes every 90 days on BFS		John James 09/08	C	09/15/08	BFS has been reconfigured to require password changes every 90 days.

Audit Name: Budget Consolidation System (BCS) BFA-002; Issued 04/08

Audit Finding No. & Agency Concurrence	Short Title	Summary	Risk	Responsible Person(s) and Due Date	Status*	Status Date	Concurs: Planned Action & Status Does Not Concur: Mitigating Controls & Risk Acceptance
1 BFA Does Not Concur	Require BCS Users to Complete Background Checks Before Receiving BCS Access	BFA should enforce policies and procedures requiring BCS users to complete criminal background checks before receiving access to the BCS, due to the sensitivity of BCS data	Compromise of confidentiality, integrity, or availability of BFS data	John Davis	NS	N/A	BFA believes that screening during hiring process sufficiently mitigates the risk of giving users access to BCS while background checks are underway.

* Status Legend: NS = Not Started; U = Underway; C = Completed

IT Security Audit Quarterly Summary

Audit Name: _____

Audit Finding No. & Agency Concurrence	Short Title	Summary	Risk	Responsible Person(s) and Due Date	Status*	Status Date	Concurs: Planned Action & Status Does Not Concur: Mitigating Controls & Risk Acceptance

Audit Name: _____

Audit Finding No. & Agency Concurrence	Short Title	Summary	Risk	Responsible Person(s) and Due Date	Status*	Status Date	Concurs: Planned Action & Status Does Not Concur: Mitigating Controls & Risk Acceptance

* Status Legend: NS = Not Started; U = Underway; C = Completed

* Status Legend: NS = Not Started; U = Underway; C = Completed