

# **Information Technology Resource Management (ITRM)**

## **Policies, Guidelines, Standards (PSGs) & Supporting Documents**

November 2010

## Contents

Definitions.....	3
ITRM framework for Policies, Standards, and Guidelines.....	4
ITRM Document Lifecycle Process.....	6
Create/Update/Retire.....	6
Adopt.....	7
Dispose.....	8
Appendix A: ITRM Documents.....	9

The management of information technology (IT) resources requires the establishment and control of a set of documents that convey purpose, direction, and required activities. The documents that accomplish this are the Commonwealth of Virginia ITRM Policies, Standards, and Guidelines (PSGs).

The purpose of this document is to provide an overview of these ITRM PSGs and the process that is used for their development, review, approval, maintenance, and retirement.

## Definitions

Information Technology (IT) is the hardware and software operated by an organization to support the flow or processing of information in support of business activities, regardless of the technology involved, whether computers, telecommunications, or other. In the Code of Virginia, information technology includes telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology Resources are the staff, software, hardware, systems, services, tools, plans, training, data, monies, and documentation that in combination comprise technology solutions to business problems.

Information Technology Resource Management (ITRM) is the term used to describe the processes to plan, allocate, and control information technology resources for improving the efficiency and effectiveness of business solutions.

ITRM framework consists of two categories titled Enterprise Architecture and Information Technology Management. Within these broad categories, ITRM PSGs are developed and promulgated as needed.

Policies provide general statements of purpose, direction and required activities for one or more defined areas of the ITRM framework (see below).

Standards provide required technical or programmatic activities in detail for a specific area of the ITRM framework. Data Standards are a variation of an ITRM Standard that also includes a business narrative, data model and data dictionary.

Guidelines provide information on optional activities related to an area of control for the Commonwealth's information technology resource management program. Activities in guidelines are considered to be best practices but are not required.

Reports provide an all encompassing discussion of an Enterprise Architecture domain or topic including principles, recommended practices, requirements, standards, rationale and implications. Any requirements, standards or

recommended practices presented within a report must be implemented by an ITRM Standard or Guideline.

Templates that are provided on the ITRM PSG page are part of the COV Information Security Program framework. They are tools that can be used by agencies to develop and administer their agency information security programs.

Checklists are optional tools that can be used by agencies to support procurements and solution development. The EA checklist summarizes all EA requirements and recommended practices in multiple simplified formats that can be used in RFPs and as part of a solution development sign-off process.

Data Models are an effective tool for representing the semantic structure of data and the relationships and business rules that are associated with that data. The data model should provide the basis for all further design, analysis, and review of proposed data standards. A data model must be associated with each Data Standard.

Data Dictionaries is a metadata repository that should include definitions, domains, and units of measure that quantify, identify, or describe the concept of every data requirement within a Data Standard.

## **ITRM framework for Policies, Standards, and Guidelines**

The ITRM Framework provides the logical areas and sub-areas of control that together define a comprehensive information technology resource management program for the Commonwealth. The framework consists of two categories titled Enterprise Architecture (EA) and Information Technology Management. Within these broad categories, ITRM PSGs are developed and promulgated as needed.

Security is part of the Enterprise Technical Architecture (one of the four component architectures). Security PSGs and supporting documents have been given their own category within this document (separated out from the EA category) because of the number of documents.

PSGs and supporting documents can also be separated into four tiers:

0. PSGs and supporting documents that pertain to all categories
1. PSGs that perform the highest level of governance for each category
2. Other PSGs that are category specific
3. Category supporting documents that are not PSGs

The diagram on the following page shows the current ITRM PSGs with their supporting documents separated by category and by tier.

**Commonwealth of Virginia**  
**Information Technology Resource Management (ITRM)**  
Document Map for Policies, Standards, Guidelines & Supporting Documents

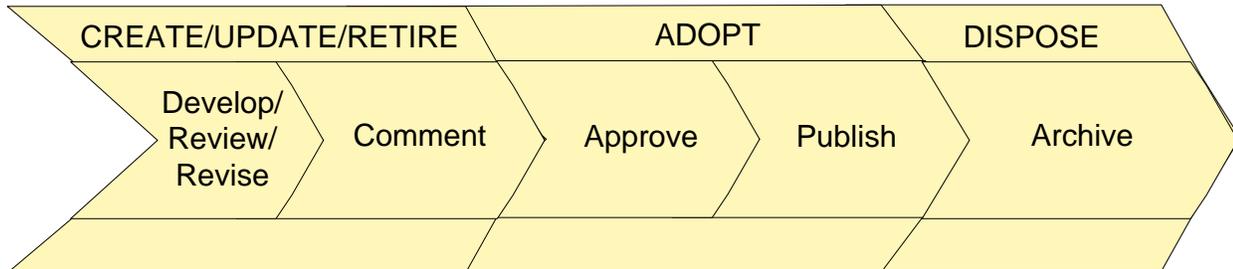
Category	Security	Enterprise Architecture (EA)	Information Technology Management
Tier 0	ITRM Policy [01] ITRM Standard on Development & Governance of PSGs [02] ITRM Glossary [03] (Supporting Document)		
Tier 1	Security Policy [11] Security Standard [12]	EA Policy [13] EA Standard [14]	Technology Management Policy [15] ITIM Standard [16] Project Management Standard [17]
Tier 2	<u>Standards</u> Audit [21] Use of Non-Commonwealth Computing Devices to Telework [22] Removal of Commonwealth Data from Electronic Media [23] Secure Remote Access to Online Court Documents [24] Virginia Real Property Electronic Recording [25]  <u>Guidelines</u> Security [26] Audit [27] Information Systems Facilities Security [28] Contingency Planning [29] Data Protection [30] Logical Access Control [31] Personnel Security [32] Risk Management [33] Threat Management [34] Asset Management [35]	Accessibility Standard [51]  Procurement Vendor Data Standard [52]  Model Virginia Map Accuracy Standards Guideline [53]	Project Manager Selection and Training Standard [72]  Commonwealth Project Management Guideline [73]  Technology Management Glossary Standard [74]
Tier 3	Templates [41]	EA Reports [61] EA Checklist [62] Data Dictionaries [63] Data Models [64]	

Note: [nn] denotes a reference to document descriptions in Appendix A.

## ITRM Document Lifecycle Process

ITRM PSGs are developed, reviewed, approved, maintained, and retired using a comprehensive and uniform process as defined in the *Standard on Development and Governance of Policies, Standards and Guidelines* (see [02] in Appendix A).

This process covers the entire PSG lifecycle:



### Create/Update/Retire

Create - requests or requirements to create a new PSG (or supporting document) can come from the Secretary of Technology, CIO, VITA staff, agencies, institutions of higher education, advisory bodies, the administration, the General Assembly, the vendor community, and other interested parties.

Update - scheduled reviews are part of the normal processes established when a PSG is approved to ensure it remains current and relevant. Most PSGs and supporting documents are scheduled to be reviewed every one to five two years.

Retire - PSGs can be rescinded if they are superseded by a completely new PSG (not just an update) or they can be retired as part of the update/review process.

Work group - creating and updating a PSG requires that a work group be established. The work group will consist of subject matter experts from the various stakeholder groups to assist in the research, review, revision and/or development of a PSG. This includes agencies, partners, higher education, etc. The work group is facilitated by VITA staff (examples: PPA Division, Data Management group, Security, Project Management Division).

### Comment

All new or revised PSG documents or actions to rescind a PSG document shall be subject to stakeholder reviews. The review and comment period will be for one of the following durations:

Standard Comment Period - applicable to all new PSGs and significant revisions to existing PSGs Documents shall be posted on the VITA Online Review and Comment Application (ORCA) for (30) thirty calendar days to facilitate review and comment by all interested parties.

Abbreviated Comment Period - applicable to administrative type updates to an existing. The document shall be posted on ORCA for (15) fifteen calendar days.

Emergency Comment Period - as determined by the CIO for new/revised **critical** PSG documents that need to be promulgated **immediately**. The document shall also be posted to ORCA for a period of (30) thirty calendar days.

Agency and Stakeholder Notification - concurrent with posting the PSG for review and comment, PPA shall notify by email Agency Information Technology Resources (AITRs) at all Executive Branch Agencies of the posting, as well as notify other stakeholders PPA considers interested in the development, revision or rescission of the PSG.

Comment Responses - following the comment period, VITA will compile all of the comments received into a single document and work with members of the applicable Work Group to:

- develop responses to each comment received;
- provide a copy of the responses and resolutions to each of the respondents;
- revise the draft PSG document as needed based on the comments received; and
- re-post the draft PSG document for further review if there are substantial changes as a result of the comment and review process.

## **Adopt**

Final Draft Reviews – finalized documents will be submitted to the PPA Director for review and action. VITA will facilitate and coordinate any needed internal management. After the reviews are complete, VITA will either:

- submit the document to the CIO for review and approval;
- return the document to the Work Group for additional work; or
- recommend to the CIO that final draft PSG be disapproved.

CIO Review and Approval - Draft PSG documents, Notices to Rescind and PSG supporting documents will be provided to the CIO for review and approval along with appropriate documentation. This includes a transmittal memorandum from the CIO to the Secretary of Technology that contains an executive summary of the proposed actions taken or recommendations relative to the new or revised PSG or rescinding of an existing PSG.

Secretary of Technology Review and Approval - CIO actions taken or recommendations to the Secretary of Technology on PSG documents will be forwarded to the Secretary of Technology for review and/or action using processes prescribed by the Secretary of Technology.

## **Publish**

VITA ensures that all approved actions by the CIO/Secretary of Technology relative to PSGs and supporting documents are published. This includes:

- preparing an appropriate notification announcement for publication in the Commonwealth's Leadership Communiqué;

- notifying Agency Information Technology Resources (AITRs) and other interested parties via email of the actions taken and availability of the resulting PSG documents;
- posting new and revised PSG documents to the VITA Website; and
- posting superseded PSG documents and rescinded PSG documents to the library archives section on the VITA Website.

### **Dispose**

Archive - all PSGs are public records and retained permanently, in accordance with General Schedule 101-100350 published by the Library of Virginia. PSGs are housed at the agency while actively referenced. Once the PSGs are no longer actively referenced, the originals are archived at the Library of Virginia.

## Appendix A: ITRM Documents

The current version of all ITRM PSGs can be found at:

<http://www.vita.virginia.gov/library/default.aspx?id=537>.

The documents listed below are presented in category / tier order (including extra categories for Security and documents that concern Security, EA and Information Technology Management).

Tier 1: PSGs and supporting documents that pertain to all categories

Tier 2: PSGs that perform the highest level of governance for each category

Tier 3: Other PSGs that are category specific

Tier 4: Category supporting documents that are not PSGs

### **ITRM Overall:**

#### **Tier 0**

01. *Information Technology Resource Management Policy (GOV102-nn)*  
This policy establishes a framework for the development and governance of Commonwealth of Virginia Information Technology Resource Management (ITRM) Policies, Standards, and Guidelines. The management of information technology (IT) resources requires the establishment and control of a set of documents that convey purpose, direction, and required activities. The documents that accomplish this are ITRM policies, standards, and guidelines (PSGs).
02. *Standard on Development and Governance of Policies, Standards and Guidelines (GOV101-nn)*  
This standard establishes a comprehensive and uniform process for developing, adopting, maintaining, and retiring, Commonwealth of Virginia Information Technology policies, standards, and guidelines (PSGs).
03. *COV ITRM Glossary*  
A single comprehensive glossary that supports Commonwealth Information Technology Resource Management (ITRM) documents.

### **Security**

#### **Tier 1**

11. *IT Information Security Policy (SEC 519-nn)*  
Protects the Commonwealth information assets by defining the minimum information security program for agencies of the Commonwealth of Virginia (COV). This policy establishes the Commonwealth Information Security program as a comprehensive framework for agencies to follow in developing agency security programs to reduce the risk to COV information irrespective of the medium containing the information.

12. *IT Information Security Standard (SEC501-nn)*

Defines the minimum requirements for each Agency's information security management program.

**Tier 2**

21. *IT Security Audit Standard (SEC502-nn)*

Agencies are continuously seeking ways to better secure their databases and data communications that are vital to fulfilling their missions and achieving desired program results. A key factor in helping achieve such outcomes and minimizing operational problems is to implement appropriate internal control. This standard enhances data security by proactively assessing that appropriate IT security controls exist around government databases and data communications.

22. *IT Standard Use of Non-Commonwealth Computing Devices to Telework (SEC511-nn)*

Defines the minimum acceptable level of security controls necessary for eligible employees to use computers, computing devices, or related electronic equipment not owned or leased by the Commonwealth to telework.

23. *Removal of Commonwealth Data from Electronic Media Standard (SEC514-nn)*

1) Defines the minimum requirements for the removal of Commonwealth data from electronic media resources prior to its being surplus, transferred, traded-in, disposed of, or replaced.

2) Prevents unauthorized use or misuse of state information, and promote the privacy and security of sensitive and/or confidential information resources within the Commonwealth.

3) Complies with federal regulations dealing with the confidentiality of personally identifiable information. Included are regulations such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act (aka, Financial Services Modernization Act), IRS 1075 and the Family Educational Rights and Privacy Act.

24. *Secure Remote Access to Online Court Documents Standard (SEC503-nn)*

1) Implements Code of Virginia § 2.2-3808.2: No court clerk shall post on a court-controlled website any document that contains code defined personal information.

2) Implements Code of Virginia § 17.1-279: Secure remote access to land records shall be by paid subscription service through individual circuit court clerk's offices pursuant to § 17.1-276, or through designated application service providers.

3) Compliance with security standards developed by the Virginia Information Technologies Agency shall be certified by the individual circuit court clerks' offices to the VITA and the Compensation Board.

25. *Virginia Real Property Electronic Recording Standard (SEC505-nn)*  
This Standard for the electronic acceptance and recordation of land records and for the release of mortgages, rescinding erroneously recorded certificates of satisfaction, requirements on secured creditors, and the form and effect of satisfaction facilitates real estate transactions in the Commonwealth. It brings Virginia in line with the recommendations for a uniform set of laws across the country for the electronic filing of land records, so once a real estate transaction goes to settlement, the attorney or settlement agent can file the documents for recordation directly from their office, streamlining real estate settlement process for the benefit of citizens of the Commonwealth and users of the electronic filing system.
26. *IT Systems Security Guideline (SEC515-nn)*  
The function of the Policy is to define the overall COV IT security program, while the Standard defines high-level COV IT security requirements. This Guideline describes methodologies for agencies to use when implementing the systems security program outlined in the policy and detailed in the Standard.
27. *IT Security Audit Guideline (SEC512-nn)*  
The function of the Policy is to define the overall COV IT security program, while the Standard defines high-level COV IT security requirements, and the IT Security Audit Standard defines requirements for the performance and scope of IT security audits. This Guideline describes methodologies for agencies to use when meeting the IT security audit requirements of the IT Security Policy, Standard, and Audit Standard.
28. *Information Systems Facilities Security Guideline (SEC517-nn)*  
Provides agencies with guidance in meeting COV Information Security Program requirements and in the development and implementation of the facilities security component of their agency information security program.
29. *IT Contingency Planning Guideline (SEC508-nn)*  
Guides agencies in the implementation of the information technology contingency planning requirements defined by ITRM Standard SEC501-01.
30. *IT Data Protection Guideline (SEC507-nn)*  
This Guideline presents a methodology for data protection 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).
31. *IT Logical Access Control Guideline (SEC509-nn)*  
Guides Agencies in the implementation of the information technology logical access control requirements defined by ITRM Standard SEC501-01.

32. *IT Personnel Security Guideline (SEC513-nn)*  
Guides Agencies in the implementation of the information technology personnel security requirements defined by ITRM Standard SEC501-01, Section 8.
33. *IT Risk Management Guideline (SEC506-nn)*  
Guides Agencies in the implementation of the information technology risk management requirements defined by ITRM Standard SEC501-01, Section 2.
34. *IT Security Threat Management Guideline (SEC510-nn)*  
This guideline presents a methodology for threat 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).
35. *IT Systems Asset Management Guideline (SEC518-nn)*  
Provides agencies with guidance in meeting COV Information Security Program requirements and in the development and implementation of the IT systems asset management component of their agency information security program.

### **Tier 3**

41. *Templates*  
Are provided on the ITRM PSG page as part of the COV Information Security Program framework. They are tools that can be used by agencies to develop and administer their agency information security programs.

## **Enterprise Architecture**

### **Tier 1**

13. *Enterprise Architecture Policy (EA 200-nn)*  
Establishes the Commonwealth's Enterprise Architecture as the primary source for providing information technology direction and technical requirements which govern the acquisition, use and management of information technology resources by executive branch agencies. This document contains Commonwealth policy statements related to applications systems development and open source software and the process used to govern agency requests for changes and exceptions to the Commonwealth's EA requirements and to ensure that all recommendations and requests for changes or exceptions are logged, reviewed, evaluated, considered, and responded to in a timely manner.

14. *Enterprise Architecture Standard (EA 225-nn)*

Establishes direction and technical requirements which govern the acquisition, use and management of information technology resources by executive branch agencies. The intent of this document is to provide a single consolidated list of requirements related to the Commonwealth's Enterprise Architecture for use by executive branch agencies and their business partners.

Architecture direction for agencies when planning or making changes or additions to their information technology is presented in the standard in two forms:

- Requirements – statements that provide mandatory Enterprise Architecture directions
- Technology Component Standard Tables – tables that indicate what technologies or products agencies may acquire at a particular point in time. The requirements are mandatory when acquiring a new or replacing an existing technology or product.

**Tier 2**

51. *Information Technology Accessibility Standard (GOV103-nn)*

Requires that procured electronic and information technology products comply with the Section 508 and other related accessibility requirements.

52. *Procurement Vendor Data Standard*

This standard defines procurement vendor information that is required to support the purchase and payment of goods and services pursuant to Code of Virginia §§ 2.2-1115.

53. *Model Virginia Map Accuracy Standards Guideline (OTH701-nn)*

This guideline is based on the American Society of Photogrammetry and Remote Sensing (ASPRS) Accuracy Standards for Large-Scale Maps. It was developed to serve as a common guideline that can be used by state, regional and local governing bodies in Virginia to meet their needs for a map accuracy standard.

### **Tier 3**

#### **61. *EA Reports***

Provides an all encompassing discussion of an Enterprise Architecture domain or topic including principles, recommended practices, requirements, standards, rationale and implications. Any requirements, standards or recommended practices presented within a report must be implemented by an ITRM Standard or Guideline. Current EA Reports are:

- Applications Domain
- Web Site Topic
- Database Domain
- Enterprise Systems Management Domain
- Information Domain
- Health Information Exchange Topic [under final review]
- Electronic Records Management Topic [under final review]
- Integration Domain
- Networking and Telecommunications Domain
- Platform Domain
- Desktop Productivity Tools Topic

#### **62. *EA Checklist***

An optional tool that can be used by agencies to support procurements and solution development. The EA checklist summarizes all EA requirements and recommended practices in multiple simplified formats that can be used in RFPs and as part of a solution development sign-off process.

#### **63. *Data Dictionaries***

Metadata repositories that include definitions, domains, and units of measure that quantify, identify, or describe the concept of every data requirement within a Data Standard.

#### **64. *Data Models***

Are effective tools for representing the semantic structure of data and the relationships and business rules that are associated with that data. The data model should provide the basis for all further design, analysis, and review of proposed data standards. A data model must be associated with each Data Standard.

## **Information Technology Management**

### **Tier 1**

#### **15. *Technology Management Policy (GOV 2002-nn)***

Establishes a comprehensive and uniform policy for the management of technology investments in the Commonwealth of Virginia (COV).

16. *Information Technology Investment Management (ITIM) Standard (CPM 516-nn)*

Establishes standards for the management of information technology investments in the Commonwealth of Virginia (COV). The purpose of the Commonwealth of Virginia Information Technology Resource Management ITIM Standard (ITIM Standard) is to:

- describe the phases in the ITIM process;
- define how the value of an IT investment is measured in each phase;
- identify the required actions associated with each phase; and,
- assign roles and responsibilities for those actions,

in order to maximize the business value of IT investments in the Commonwealth.

17. *Project Management Standard (CPM 112-nn)*

Establishes standards for the management of information technology projects with total cost greater than or equal to \$100,000 in the Commonwealth of Virginia (COV).

**Tier 2**

71. *Project Manager Selection and Training Standard (CPM 111-nn)*

Establishes standards for the selection and training of Project Managers in the Commonwealth of Virginia (COV).

72. *Commonwealth Project Management Guideline (CPM 110-nn)*

Establishes guidelines for the management of information technology projects with total cost greater than or equal to \$100,000 in the Commonwealth of Virginia (COV).

73. *Technology Management Glossary Standard (GOV 2003-nn)*

Facilitates the development, improvement, and standardization of technology management throughout the Commonwealth of Virginia by the use of a common set of terms. This standard establishes a comprehensive and uniform set of definitions and acronyms for commonly used Commonwealth Technology Management terms. [Will be rescinded - ITRM Glossary replaces this document]