



Virginia Information Technologies Agency

Commonwealth Information Security Advisory Group (ISOAG) and Internal Auditor Meeting

December 14, 2006

expect the best



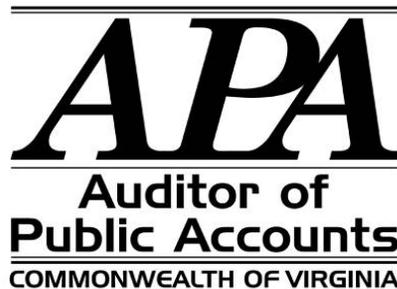
ISOAG December 14, 2006 Agenda

- | | | |
|------|--------------------------|-----------------------|
| I. | Welcome | Peggy Ward, VITA |
| II. | SJR 51 Review Results | Goran Gustavsson, APA |
| III. | ARMICS* | Randy McCabe, DOA |
| IV. | Quality Assurance | Jack Spooner, DOA |
| V. | COV IS Guidelines Status | Cathie Brown, VITA |
| VI. | Security Audit Standard | Peggy Ward, VITA |
| VII. | Other Business | Peggy Ward, VITA |

* Agency Risk Management and Internal Control Standards

expect the best

A Review of Information Security in the Commonwealth of Virginia



Presented by:

Goran Gustavsson

Information Systems Security Audit Director

December 2006

Background

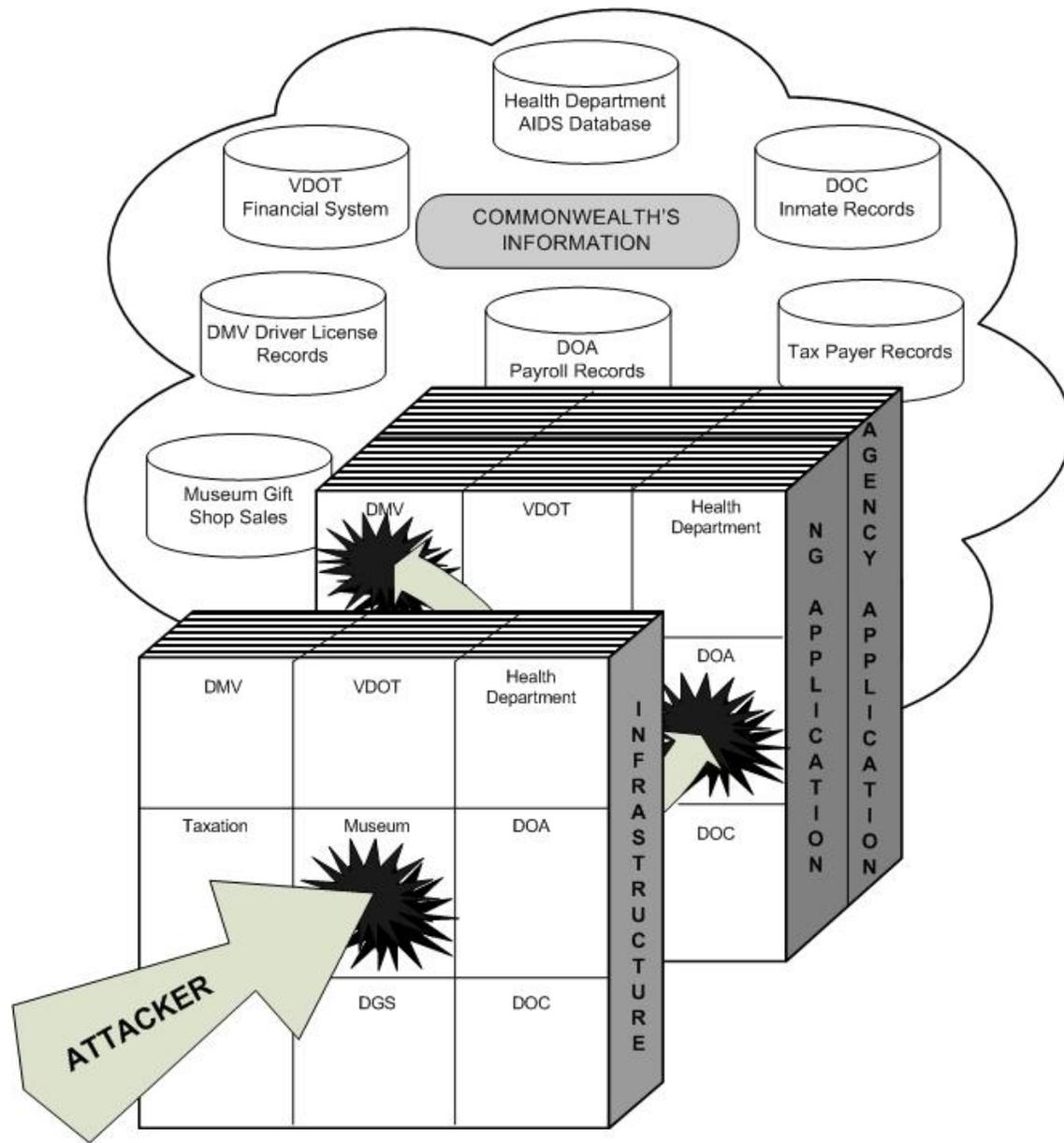
- Senate Joint Resolution 51 (SJR51)
- Introduced by Senator Jay O'Brien
- Enacted by the 2006 General Assembly
 - *“Directing the Auditor of Public Accounts to report on the adequacy of the security of state government databases and data communications from unauthorized uses.”*
(Source: <http://leg1.state.va.us/cgi-bin/legp504.exe?061+ful+SJ51ER>)

Background

- Our study has a broader focus than only examining security over databases and data communications.
- Rather, our study examined the information security programs that provides control over agencies' information.
- Focused on validating the existence of agency policies and procedures that conformed with standards since timeframe prevented testing for compliance with policies and procedures.

Background

- Recognized the “layered” information security complexity between Agency, VITA and Northrop Grumman.



Process

- Evaluated information security industry best practices
 - ISO 17799, Cobit, Fiscam and NIST
- Created checklist based on industry best practices
- Distributed checklist to agencies and institutions
- Evaluated and reported on checklist findings and recommendations

Process - Checklist Distribution

- Distributed in three phases to 104 agencies and institutions of higher education in the executive, legislative and judicial branches
 - Phase I – July through August (Pilot Group)
 - Phase II – August through September
 - Phase III – September through Mid-November

Process – Checklist Distribution

- Auditor contacted agency or institution to establish a date on which checklist was sent
- Agency or institution was given 5 business days to respond and return a completed checklist, along with supporting documents
- Auditor verified the responses, and if discrepancies were discovered, the agency or institution was given 2 business days to remedy the problem

Process – Checklist Evaluation

- Checklist results were merged into a database for analysis
- Certain questions in the checklist relate directly to SEC 2001 and/or SEC 501, and an agency's or institutions answers are therefore considered during their regular audit

Process – Checklist Evaluation

- Agencies' and institutions' information security programs were rated as:
 - No Program
 - Inadequate Program
 - Adequate Program

Process – Checklist Evaluation

- No InfoSec Program Criteria:
 - The agency or institution did not have any of the basic documents required to perform a security assessment. If none of the four security assessment documents, (BIA, RA, COOP, or DRP) are available, the agency cannot correctly establish an information security program

Process – Checklist Evaluation

- Inadequate InfoSec Program Criteria:
 - If an agency has begun the process of evaluating their state of security, and has at least one of the four security assessment documents, (BIA, RA, COOP, or DRP), it will be rated as inadequate.

Process – Checklist Evaluation

- Adequate InfoSec Program Criteria:
 - In order for an agency to have an adequate security program, they must have performed a full security analysis of the information within the agency as well as have some security controls over the information. The full security analysis must include completion of the four security assessment documents (BIA, RA, COOP, and DRP). The additional security controls come from selected questions within the security survey.

Process – Checklist Evaluation

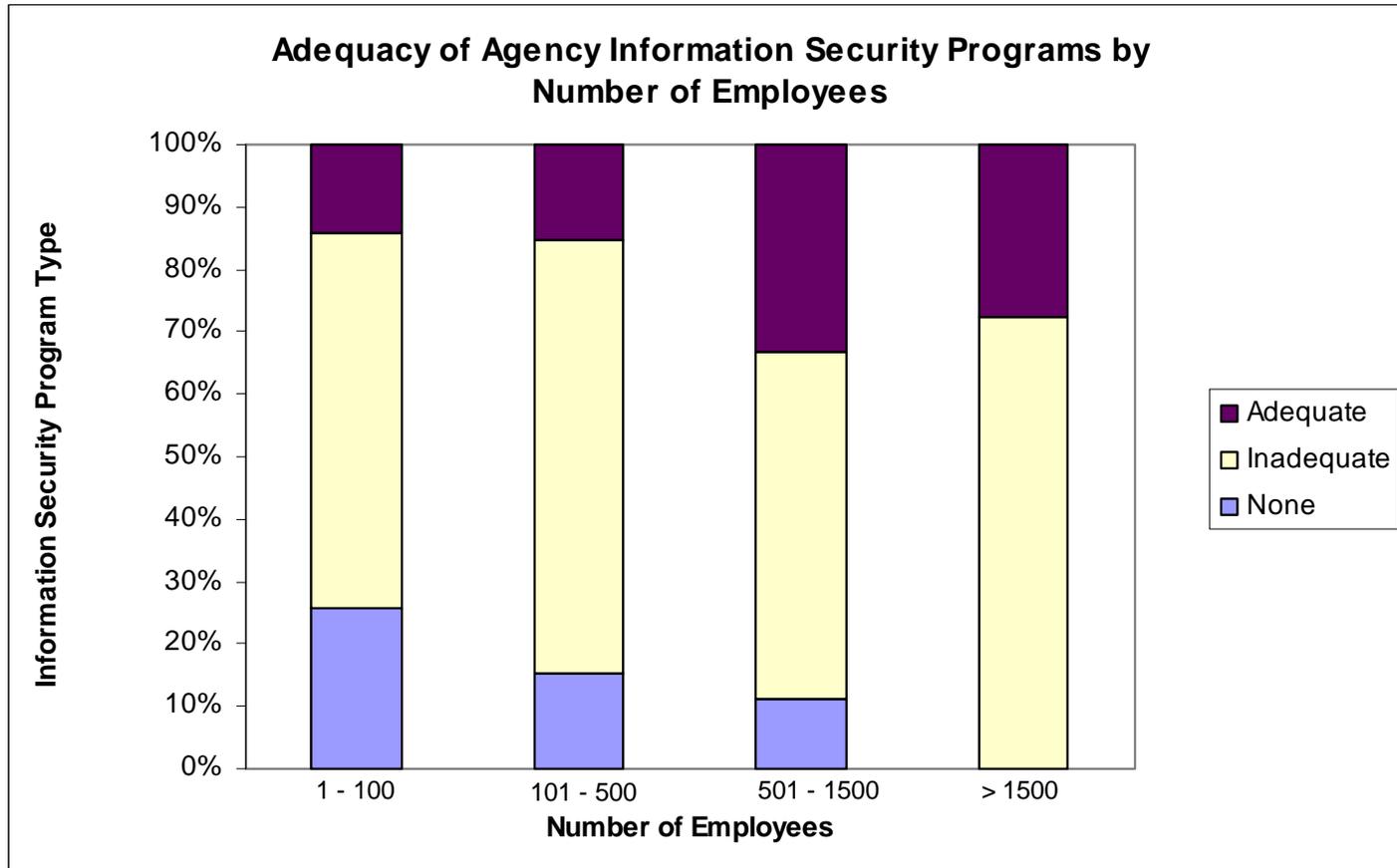
- Adequate InfoSec Program Criteria (cont'd):
 - An organizational structure that includes the assignment of an ISO
 - A formal training program
 - Policies and procedures for approving logical access
 - Process requiring users authentication for access to all systems and management approval of any exceptions after having evaluated the risks for those exceptions
 - Policies and procedures regarding password controls
 - All the critical and sensitive assets have the appropriate physical safeguards in place to protect against unauthorized access and documentation of who approves such controls
 - Active Monitoring of their systems, applications and databases.

Process – Checklist Evaluation

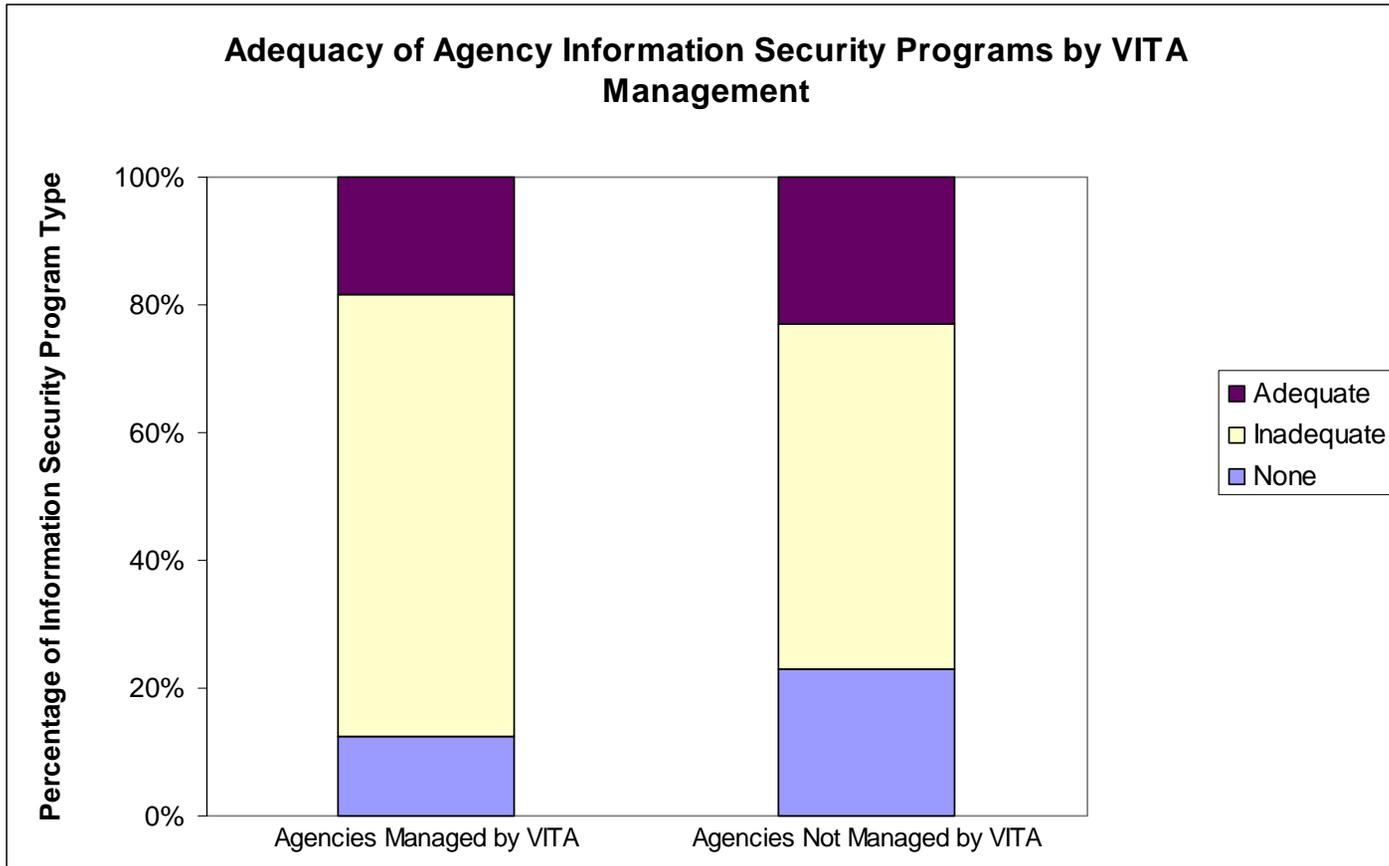
Results

	Agencies and Institutions	Percent of Total
None	17	16%
Inadequate	66	64%
Adequate	21	20%

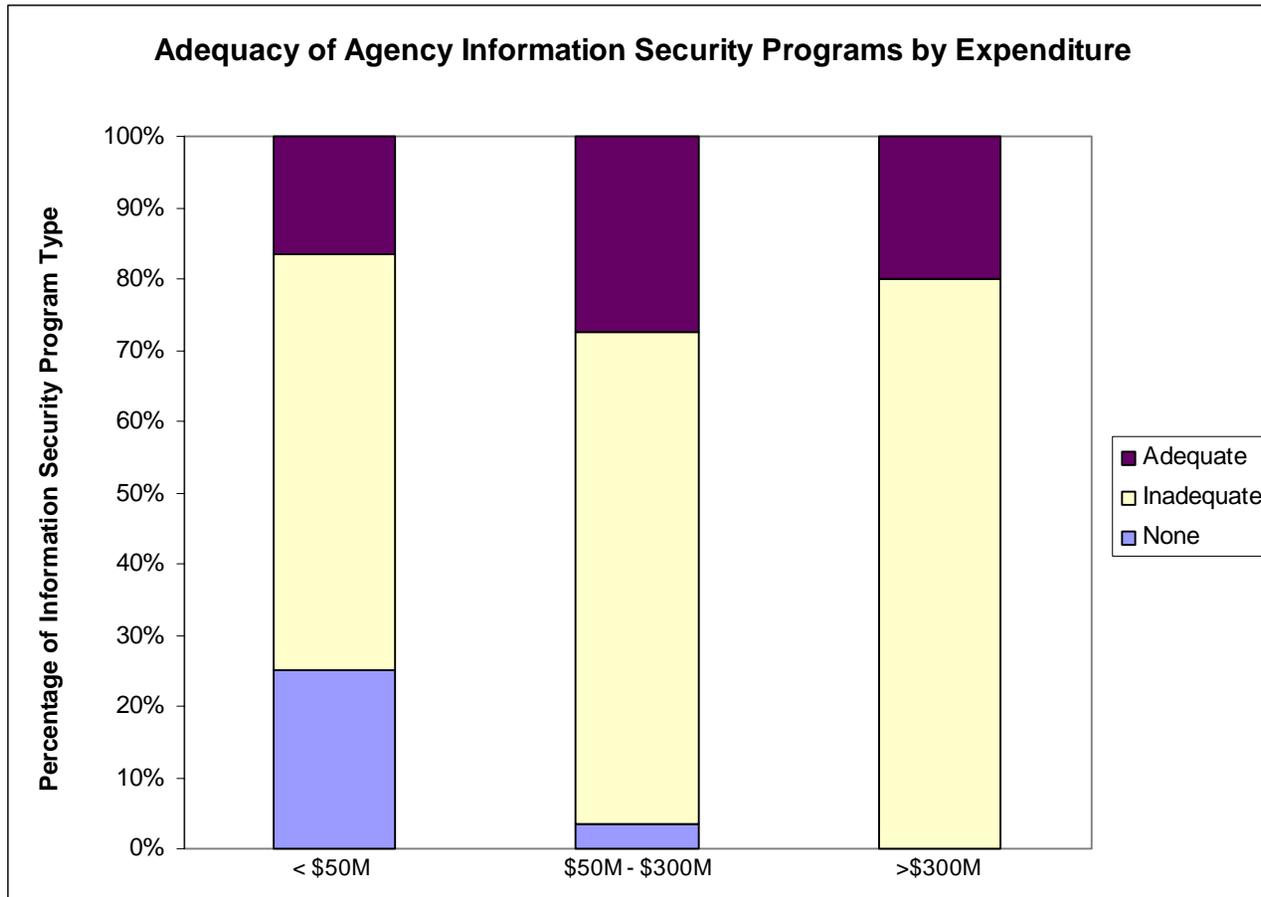
Process – Checklist Evaluation



Process – Checklist Evaluation



Process – Checklist Evaluation



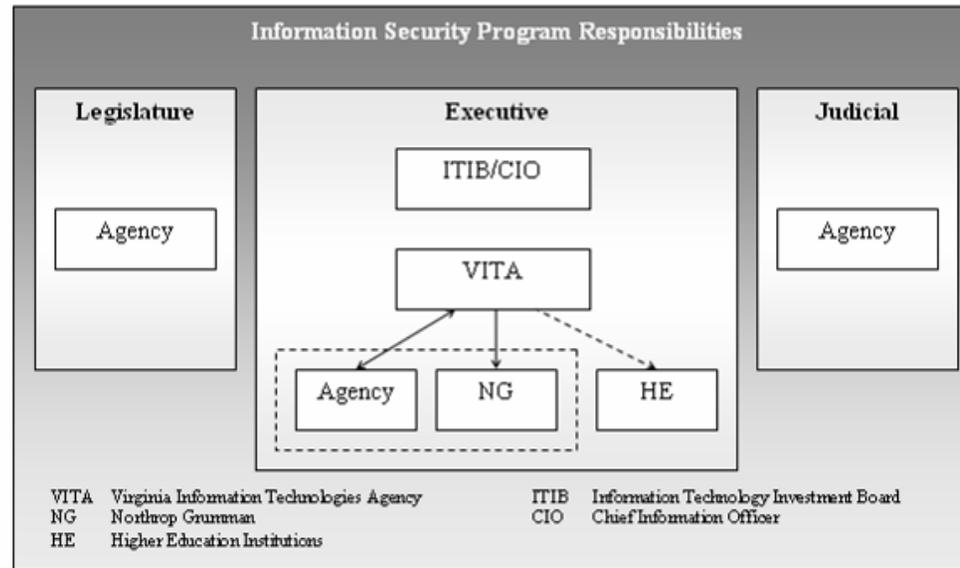
Process – Checklist Evaluation

- If you have any questions regarding your agency's checklist, please e-mail me at:
 - goran.gustavsson@apa.virginia.gov

Recommendations

- Recommendation #1
 - We recommend that VITA develop a plan to communicate infrastructure information and standards to agencies that VITA supports. Additionally, VITA should provide assistance and expertise to agencies as they develop their information security programs. VITA should also assume responsibility for ensuring that the infrastructure meets the agency's needs and mitigate threats and vulnerabilities through Northrop Grumman's standards.

Recommendations



- Recommendation #2

- The General Assembly may wish to consider granting the CIO authority over the other branches of government's information security programs. In addition, the agencies and institutions need to develop a mutual comprehensive information security program with VITA that provides adequate and comprehensive security to protect information in the Commonwealth.

Recommendations

- Recommendation #3
 - The CIO and ITIB should consider supplementing the Commonwealth's SEC 501 standard with the additional processes identified in this report.

Recommendations

- Recommendation #3 (cont'd)
 - The Commonwealth's standard does not require updated network diagrams or the designation of a network administrator responsible for updating such diagrams.
 - The Commonwealth's standard does not require vendor supplied (default) passwords to be changed immediately after installation.

Recommendations

- Recommendation #3 (cont'd)
 - The Commonwealth's standard does not require authorization and logging of all media that is stored off-site.
 - The Commonwealth's standard does not require documented security agreements between two parties (agencies) to include any mandated requirements, such as HIPAA, if applicable.

Recommendations

- Recommendation #4
 - In order to create a proper information security plan, agencies require sufficient resources with appropriate expertise to develop such a plan. Using a centralized entity, such as VITA, to help with creating and maintaining an information security plan allows the Commonwealth to leverage its cost for resources with information security expertise to assist agencies, especially small to medium-sized agencies, to perform the proper security analysis and develop an adequate information security plan.

Questions?

Contact:

Goran Gustavsson

goran.gustavsson@apa.virginia.gov

(804) 225-3350 ext. 306

Agency Risk Management and Internal Controls (ARMICS)

Randy McCabe
Department of Accounts

December 14, 2006

Quality Assurance

Jack Spooner, DSIA

December 14, 2006

Who Must Have External Assessments?

- Those who are required to comply with the IIA standards
 - Certified Internal Auditors (CIAs)
 - Members of the IIA

Why Do Agency and Educational Institution I/A Departments Have to Comply With the Standards?

- Most Agencies and Institutions are Members of the IIA
- Administrative Code of VA Requirement

When Did the External Assessment Requirement Become Mandatory?

- Prior to Jan.1, 2002- QARs not mandatory but good business practice
- Effective Jan. 1, 2002- Mandatory

Frequency of External Assessments and Starting Point

- Frequency: At least once every 5 years
- Starting Point: Earliest, 5 years from the date of your last QAR;
Latest, 5 years after QARs were mandated or 1/01/07

Types of External Assessments

- Full External Assessment
- Self-Assessment with Independent Validation

Qualifications for Those Who Perform External Assessments

- Independent
- Honest and Objective
- Competent

Costs to Perform Full External Assessment

Small Shop (1-4)	\$8,000-\$8,500
Medium Shop (5-8)	\$11,500
Large Shop (9-12)	\$14,000-\$16,000

Costs to Perform Self-Assessment With Independent Validation

Small Shop (1-4)	\$3,000-\$3,500
------------------	-----------------

Medium Shop (5-8)	\$5,000
-------------------	---------

Large Shop (9-12)	\$6,500
-------------------	---------

Choosing Between the Two External Assessment Types

- Cost
- Time Elapsed Since Last QAR
- Agency Head or Audit Committee Preference

Summary

- Required to Follow IIA Standards
- Must Have a QAR Once Every 5 Years
- Must Have a QAR by 1/01/07
- May Select a Full External Review or the Self Assessment with Independent Validation
- Suggest Contacting the IIA, Clifton Gunderson, or Richard Tarr to Perform the QAR
- Schedule a QAR for 2007

Any Questions or Comments?



Virginia Information Technologies Agency

COV IS Guidelines Update

Cathie Brown, CISM, CISSP
December 14, 2006

expect the best



IT Security Standard SEC501-01

Components of the COV IT Security Program:

- Risk Management
- IT Contingency Planning
- IT Systems Security
- Logical Access Control
- Data Protection
- Facilities Security
- Personnel Security
- Threat Management
- IT Asset Management



Development of Guidelines

- Guidelines are completed or in process for 5 of 9 components outlined in the Standard
- Components were chosen for guidelines based on need and potential benefit to the COV
- Each component of the Standard contains requirements that provide the basis for an Agency's IT Security Program



Status for Guidelines

Guideline	Status	Target Date
Risk Management Guideline & Instructions	Publish on VITA website	December 2006
Logical Access Control Guideline	Post on ORCA for review & comments	December 2006
IT Contingency Planning Guideline	Post on ORCA for review & comments	December 2006
Data Protection Guideline	Post on ORCA for review & comments	December 2006
Threat Management Guideline	Under development	



Remaining Components

Guideline documents planned:

- IT Systems Security
- Personnel Security

Guideline documents not planned at this time:

- Facilities Security
- IT Asset Management



SJR51 Recommendations for IT Standards

1. Org chart for information security reporting structure
2. Information security committee
3. ISO authority/responsibilities
 - Approve system security plans
 - Authorize operation of an information system
 - Issue interim authorizations to operate an information system
 - Deny authorizations to operate an information system
4. Agency senior management approval of data classifications, periodic review, communication to data owners and end-users
5. Documentation and periodic review of hardware/software assets
6. Network diagrams and assigned responsibility
7. Periodic review of employee job descriptions to ensure segregation of duties



SJR51 Recommendations for IT Standards

8. Involvement of data and system owners in BIA
9. Manual processing procedures for DR Plans
10. P&P to approve/remove authorization for vendors or third parties
11. Documentation of requests/approvals for emergency or temporary access
12. Require vendor supplied passwords be changed
13. Periodic review of the list of persons with physical access to sensitive resources by management
14. Authorization and logging of deposits and withdrawals of media stored off-site
15. Documented security agreements between two parties to include mandated requirements (HIPAA) if applicable



Questions or Comments?





Virginia Information Technologies Agency

Commonwealth of Virginia Information Technology Security Audit Standard Overview

Peggy Ward

Chief Information Security and Internal Audit
Officer

Information Security Officers Advisory Group &
Internal Auditors

December 14, 2006

expect the best



COV IT Security Program Documents

- *IT Security Policy* (ITRM Policy SEC500-02)
 - Defines the overall COV IT security program
- *IT Security Standard* (ITRM Standard SEC501-01)
 - Describes high-level COV IT security requirements
- *IT Security Audit Standard* (ITRM Standard SEC507-00)
 - Describes COV IT Security Audit requirements



Purpose of the Policy and Standards

- Protect COV data against unauthorized access and use
- Maintain integrity of COV data
- Meet requirements for availability of data residing on IT systems
- Meet federal, state and other regulatory and legislative requirements
- Assess effectiveness of IT security controls



Guiding Principles

- COV Information is:
 - A critical asset that shall be protected
 - Restricted to authorized personnel for official use
- IT security must be:
 - A cornerstone of maintaining public trust
 - Managed to address both business and technology requirements
 - Risk-based and cost-effective
 - Aligned with COV priorities, industry-prudent practices, and government requirements
 - Directed by policy but implemented by business owners
 - The responsibility of all users of COV IT systems and data



CIO

- In accordance with the *Code of Virginia* § 2.2-2009, 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.”*



Applicability

- The requirements of the COV IT Security Program are applicable to all state agencies and institutions of higher education that manage, develop, purchase, and use information technology resources
- The *Policy* and *Standards* are offered as guidance only to local government entities
- The *Policy* and *Standards* are not applicable to:
 - Systems under development and/or experimental systems that do not create additional risk to production systems
 - Surplus and retired systems
 - Academic instruction or research systems
 - This exemption, however, does not relieve these academic instruction or research systems from meeting the requirements of any other state or federal Law or Act to which they are subject



Requests for Exceptions

- If compliance with an IT security requirement would result in a significant adverse impact:
 - Agency Heads should submit a written exception request to the CISO (exception request form is in the Appendix of the *IT Security Policy* and *IT Security Standard*)
- Exception requests must document:
 - The business need
 - The specific duration
 - The scope and extent
 - Agency Head approval
 - Mitigating safeguards
- CISO evaluates and grants or denies requests for all exceptions
- Agencies may appeal denied exception requests to the CIO through the CISO



Organization of the *IT Security Audit Standard*

- The *IT Security Audit Standard* consists of:
 - **Definitions** of terms used in the document
 - **Requirements** for the planning, performance, and reporting of IT security audits



COV IT Security Program Process Summary

For All Agency IT Systems:

- Assign Agency ISO
- Conduct Agency Business Impact Analysis
- Document and Characterize Types of Data
- Classify System and Data Sensitivity
- Inventory and Define Systems and Determine System Ownership
- Assign Security Roles

For Non-Sensitive Agency IT Systems:

- Conduct informal Risk Analysis
- Apply additional IT security controls, as required

For Sensitive Agency IT Systems:

- Inventory and Define Systems and Determine System Ownership
- Assign Security Roles
- Conduct formal Risk Assessment and apply additional security controls based on results
- Conduct IT Security Audits
- Develop & implement Corrective Action Plan and accept residual risk
- Conduct annual self-assessment to validate that protections remain adequate
- Repeat Risk Assessment and Security Audit processes at least every three years or upon major change to the IT System



IT Security Audit Standard

- The *IT Security Audit Standard* delineates the methodology for conducting IT security audits
- Agencies must conduct IT security audits of all Agency-owned IT systems at a frequency relative to risk
- At a minimum, all sensitive IT systems must undergo an IT security audit at least once every three years



Definitions

- **IT Security Audit**

- An independent review and examination of an IT system's policies, records, and activities that assesses the adequacy of IT system controls and compliance with established IT security policy and procedures

- **IT Security Auditors**

- Those persons having the experience and expertise required to perform IT security audits, including CISO personnel, Agency internal auditor, Auditor of Public Accounts, or staff of a private firm

- **Sensitive IT Systems and Data**

- Sensitive Data is any data which the compromise of confidentiality, integrity, and/or availability could adversely affect COV interests, Agency programs, individual privacy rights
- Sensitive IT Systems are that store, process, or transmit sensitive data



Definitions

- **Information Technology (IT) System:** An interconnected set of IT resources under the same direct management control. See also Application System and Support System.
- **Application System:** An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also Application, Support System, and Information Technology (IT) System.
- **Support System:** An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also Application System and Information Technology (IT) System.



Security Audits of Government Databases

- The Agency's IT security audit program shall include, for sensitive systems:
 - Assessing the risks associated with the state government databases for which it is the Data Owner
 - Conducting IT Security Audits at a frequency relative to the risk identified by the Agency



Planning for IT Security Audits

- Agencies shall place reliance on audits already performed or underway
- Annually, each Agency shall develop an IT security audit plan for the government databases for which it is the Data Owner
- The IT security audit plan shall be based on the Agency's Business Impact Analysis (BIA) and Risk Assessment (RA)
- The Agency Head shall submit the Agency IT security audit plan to the CISO no later than 7 months after the effective date of this standard



Planning for IT Security Audits

If a system relies upon IT services provided by VITA or any other service provider, the IT Security Auditor shall rely on any applicable IT Audits performed during the applicable audit cycle where possible.



IT Security Audit Scope

- The IT Security Auditor shall use criteria that, at a minimum:
 - Assess the adequacy of IT system controls,
 - Measure compliance with the applicable requirements of:
 - ***Commonwealth of Virginia Information Technology Security Policy (ITRM Policy SEC500-02)***
 - ***Commonwealth of Virginia Information Technology Security Standard (ITRM Standard SEC501-01)***
 - Measure compliance with any other applicable Federal and COV regulations



Performance of IT Security Audits

- Prior to performing each IT Security Audit, the IT Security Auditor and the Agency Head or designee will agree on:
 - A specific scope
 - A schedule for the IT Security Audit
 - A checklist of information and access required for the Audit



Documentation of IT Security Audits

- IT Security Audit Work Papers
- IT Security Audit Reports
- Corrective Action Plan Reporting and Verification
- Reporting IT Security Audit Results to VITA



IT Security Audit Work Papers

- The Auditor shall prepare audit work papers to provide:
 - Documentation of the audit
 - Sufficient competent evidential matter supporting all conclusions
- The Auditor shall take care that:
 - Work papers do not constitute an unnecessary security risk
 - Are safeguarded appropriately



IT Security Audit Reports

- IT Security Auditor prepares a draft of the report for the Agency Head or designee and makes any mutually agreeable changes, then presents final IT Security Audit report to the Agency Head or designee
- Agency prepares a Corrective Action Plan (CAP) within 10 business days of receiving the final IT Security Audit report:
 - For each finding with which the Agency concurs, include the:
 - Corrective action planned
 - Due date for the corrective action
 - Party responsible for the corrective action
 - For each finding with which the Agency does not concur, include the:
 - Agency's statement of position
 - Mitigating controls that are in place
 - Agency's acknowledgment of its acceptance of the residual risk
- IT Security Auditor incorporates the CAP in the final Audit Report for presentation to the Agency Head and the Agency ISO



CAP Reporting and Verification

- Implementation
 - The Agency Head or designee shall receive reports, at least annually from the date of the final Audit Report, on progress in implementing outstanding corrective actions
- Verification
 - The Agency Head or designee shall arrange for a follow-up review to verify implementation of the specified corrective actions



Reporting IT Security Audit Results to VITA

- Each Agency Head or designee shall submit to the CISO a quarterly report containing:
 - A record of all IT Security Audits conducted and findings
 - Whether the Agency concurs or does not concur with each finding
 - The CAP for each finding with which the Agency concurs
 - The statement of position, mitigating controls, and risk acceptance for each finding with which the Agency does not concur
 - Status of outstanding corrective actions for all IT Security Audits previously conducted by or on behalf of the Agency



25 Agencies included in the NG SAS 70

1. Compensation Board
2. Department of Accounts
3. Department of Alcoholic Beverage Control
4. Department of Corrections
5. Department of Education
6. Department of Fire Programs
7. Department of General Services
8. Department of Health Professions
9. Department of Human Resource Management
10. Department of Juvenile Justice
11. Department of Mental Health, Mental Retardation & Substance Abuse Services
12. Department of Military Affairs
13. Department of Motor Vehicles
14. Department of Planning and Budget
15. Department of Rail and Public Transportation
16. Department of Rehabilitative Services
17. Department of Social Services
18. Department of Taxation
19. Department of Transportation
20. Department of the Treasury
21. Department of Veteran's Services
22. State Board of Elections
23. Virginia Department of Health
24. Virginia Employment Commission
25. Virginia Museum of Fine Arts



Questions and Answers





Other Business

