



Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

October 8, 2014



ISOAG October 2014 Agenda

- | | |
|---|--|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. NASCIO Award | Mike Watson, VITA |
| III. SEC501-09 Updates | Mike Watson, VITA |
| IV. 2014 COV Security Annual Report | Mike Watson, VITA |
| V. Overall Program (Risk, Audit) | Jon Smith, Bill Freda, Ed Miller, VITA |
| VI. Risk Management Program | Jon Smith, VITA |
| VII. Cyber Security Framework | Jon Smith, VITA |
| VIII. 3 rd Party Hosting Security Considerations | John Craft, VITA |
| IX. ITRM SEC514 Updates | Bob Baskette, VITA |
| X. Small Agency Program Update | Bob Auton, VITA |
| XI. Upcoming Events | Bob Baskette, VITA |
| XII. Partner/Operation Update | Bob Baskette, VITA |



Virginia Information Technologies Agency

NASCIO Award

Michael Watson, CISO

October 8, 2014



NASCIO Award

Category: Cyber Security Initiatives

Barring Open Doors to Threats

Initiation date: January 15, 2013

Completion date: December 1, 2013



NASCIO Award

Beginning in January 2013, the Virginia Information Technologies Agency (VITA) implemented a full-scale threat analysis of the state's cyber attack data to examine an increasing trend in successful malicious attacks. VITA identified two significant attack vectors -- local administrative rights (LAR) and Java -- and used the information identified to mitigate the frequency of security and malware-related incidents.



Questions

Questions?

You may also send any questions to :
CommonwealthSecurity@VITA.Virginia.Gov



Information Security Standard SEC501-09 Updates

Michael Watson, CISO

October 8, 2014



Information Security Standard SEC501-09

- Updated to incorporate NIST 800-53 rev 4
- Administrative changes identified
- Next steps
 - IS Council Review
 - To ORCA - Approx. End of October – ORCA: 30 days



Information Security Standard SEC501-09

Compliance – Agencies are expected to be compliant with the security standards and guidelines within one year of the publication date, unless otherwise directed. Information systems that are under development are expected to be compliant upon deployment.

A key part of compliance is selecting and implementing a subset of the controls (safeguards) from the Security Control Catalog. These controls are the management, operational, and technical safeguards (or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. To implement the needed safeguards or controls, agencies must first determine the security category of their information systems.



Information Security Standard SEC501-09

KEY UPDATES

- Insider threats;
- Software application security (including web applications);
- Social networking, mobiles devices, and cloud computing;
- Cross domain solutions;
- Advanced persistent threats; and
- Industrial/process control systems;



Information Security Standard SEC501-09

Control Updates CSRM vs NIST

- Previously withdrawn, (not applicable to COV)
- New from NIST
- AU-6(6,7,9,10), AU-8(1,a,b), AU-12, AU-13, CA-7(3), CM-3, CM-5, CP-2(4), CP-7, IA-2(5), IR-3(2), IR-4(6,7,8), IR-8(f), MA-2(f), MA-5(b,c), MP-5(c), PE-2(3), PE-13(1,2,3), PE-14(1,2), PL-4, PS-4(c,d), PS-6(a,c), PS-7(b,d), RA-3(d), RA-5(10), SA-3 (supplemental guidance), SA-5(d,e, supplemental guidance), SA-11(4,6,7), SC-5, SC-7(b,11), SC-18, SC-19, SI-4(13,16,20), SI-10(2,3)



Information Security Standard SEC501-09

Audit Updates

- Reflect the maturity of the Commonwealth's security posture.
- Continuous monitoring
- Trend Analysis
- Audit Report Generation



Information Security Standard SEC501-09

Configuration Management Updates

- Cryptography
- Access restrictions and enforcement.



Information Security Standard SEC501-09

Continuity Planning Updates

- New NIST requirements - coordination with third parties for Continuity Planning



Information Security Standard SEC501-09

Investigative Response Updates

- New NIST requirements address insider threats and correlating events with outside organizations.
- Authentication for maintenance personnel
 - Think Target breach due to HVAC access



Information Security Standard SEC501-09

Physical and Environmental Updates

- Automatic fire suppression devices
- Humidity and temperature controls.



Information Security Standard SEC501-09

Personnel Security Updates

- Notifications for personnel terminations, transfers, access agreements, and 3rd party personnel security.
- Correlations of results from vulnerability scans
- Dissemination of Risk Assessments to key personnel within the organization.



Information Security Standard SEC501-09

System and Services Acquisition Updates

- Supplemental guidance for System and Service Acquisition for system documentation and life cycle support.
- Developer security testing and evaluation



Information Security Standard SEC501-09

System and Communications Protection Updates

- VOIP, mobile code reintroduced due to requests from Commonwealth Agencies
- New from NIST - separating public facing networks from internal networks with subnetworks.



Information Security Standard SEC501-09

System and Information Integrity Updates

- Information system monitoring
- Creation of traffic pattern profiles
- Additional monitoring for privileged users.



Information Security Standard SEC501-09

SEC 501-09 Draft Language

The following is a collection of the new language from NIST or that was previously withdrawn by CSRM that will be submitted to ORCA.



Information Security Standard SEC501-09

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

(6) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING

- **The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.**

(7) AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS

- **The organization specifies the permitted actions for each *information system process; role; user* associated with the review, analysis, and reporting of audit information.**



Information Security Standard SEC501-09

(9) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT

- **The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.**

(10) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT

- **The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.**



Information Security Standard SEC501-09

AU-8 TIME STAMPS

(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

The information system:

- (a) Compares the internal information system clocks every 5 - minutes with a Stratum two clock source or better]; and**
- (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than 2-seconds.**



Information Security Standard SEC501-09

AU-12 AUDIT GENERATION

Control: The information system:

- (a) Provides audit record generation capability for the auditable events defined in AU-2 a. at the operating system, services, and applications;
- (b) Allows authorized organization personnel to select which auditable events are to be audited by specific components of the information system; and
- (c) Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.



Information Security Standard SEC501-09

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control: The organization monitors [*Assignment: organization-defined open source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information.

CA-7 CONTINUOUS MONITORING

(3) CONTINUOUS MONITORING | TREND ANALYSES

- **The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.**



Information Security Standard SEC501-09

CM-3 CONFIGURATION CHANGE CONTROL

(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT

- **The organization ensures that cryptographic mechanisms used to provide system security safeguards are under configuration management.**

CM-5 ACCESS RESTRICTIONS FOR CHANGE

(1) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING

- **The information system enforces access restrictions and supports auditing of the enforcement actions.**



Information Security Standard SEC501-09

CP-2 CONTINGENCY PLAN

(4) CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS

- The organization plans for the resumption of all missions and business functions within the organization-defined time period of contingency plan activation.

(7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS

- The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

CP-7 ALTERNATE PROCESSING SITE

(6) ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE

- The organization plans and prepares for circumstances that preclude returning to the primary processing site.



Information Security Standard SEC501-09

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

(5) IDENTIFICATION AND AUTHENTICATION | GROUP AUTHENTICATION

- **The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.**

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

- **The organization coordinates incident response testing with organizational elements responsible for related plans.**



Information Security Standard SEC501-09

IR-4 INCIDENT HANDLING

(6) INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES

- **The organization implements incident handling capability for insider threats.**

(7) INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION

- **The organization coordinates incident handling capability for insider threats across all sensitive *components or elements of the organization.***

(8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS

- **The organization coordinates with the appropriate *external organizations*] to correlate and share *incident information* to achieve a cross-organization perspective on incident awareness and more effective incident responses.**



Information Security Standard SEC501-09

IR-8 INCIDENT RESPONSE PLAN

Control: The organization:

(f) Protects the incident response plan from unauthorized disclosure and modification.

MA-2 CONTROLLED MAINTENANCE

Control: The organization:

(f) Includes *the appropriate maintenance -related information*] in organizational maintenance records.



Information Security Standard SEC501-09

MA-5 MAINTENANCE PERSONNEL

Control: The organization:

(b) Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

(c) Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.



Information Security Standard SEC501-09

MP-5 MEDIA TRANSPORT

Control: The organization:

(c) Documents activities associated with the transport of information system media; and

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

- **The organization restricts unescorted access to the facility where the information system resides to personnel with security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system;**



Information Security Standard SEC501-09

PE-13 FIRE PROTECTION

- Control Enhancements for Sensitive Systems:
- (1) FIRE PROTECTION | DETECTION DEVICES / SYSTEMS
- **The organization employs fire detection devices/systems for the information system that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.**
- (2) FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS
- **The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the appropriate organization-defined personnel**
- (3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION
- **The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.**



Information Security Standard SEC501-09

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control Enhancements for Sensitive Systems:

(1) TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS

- **The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.**

(2) TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS

- **The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.**



Information Security Standard SEC501-09

PL-4 RULES OF BEHAVIOR

Control: The organization:

(c) Reviews and updates the rules of behavior on an annual basis or more frequently if required to address an environmental change ;
and

(d) Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

PS-4 PERSONNEL TERMINATION

f. Notifies the appropriate *organization-defined personnel* within an organizationally defined time-period..



Information Security Standard SEC501-09

PS-6 ACCESS AGREEMENTS

Control: The organization:

- (a) Develops and documents access agreements for organizational information systems;
- (c) Ensures that individuals requiring access to organizational information and information systems:
 1. Sign appropriate access agreements prior to being granted access; and
 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or on an annual basis or more frequently if required to address an environmental change.



Information Security Standard SEC501-09

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization:

(b) Requires third-party providers to comply with personnel security policies and procedures established by the organization;

(d) Requires third-party providers to notify the appropriate *organization-defined personnel* of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within an organization defined time period.; and



Information Security Standard SEC501-09

RA-3 RISK ASSESSMENT

Control: The organization:

(d) Disseminates risk assessment results to the appropriate *organization-defined personnel*; and

RA-5 VULNERABILITY SCANNING

Control Enhancements for Sensitive Systems:

(10) VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION

- **The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.**



Information Security Standard SEC501-09

SA-3 LIFE CYCLE SUPPORT

Supplemental Guidance: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8.



Information Security Standard SEC501-09

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:

(d) Protects documentation as required, in accordance with the risk management strategy; and

(e) Distributes documentation to the appropriate *organization-defined personnel*.



Information Security Standard SEC501-09

Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. . Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.



Information Security Standard SEC501-09

SA-11 DEVELOPER SECURITY TESTING

Control Enhancements for Sensitive Systems:

(4) DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS

- **The organization requires the developer of the information system, system component, or information system service to perform a manual code review of *specific code* using the appropriate *processes, procedures, and /or techniques*.**
- Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of information systems. Such code reviews are uniquely effective at identifying weaknesses that require knowledge of the application's requirements or context which are generally unavailable to more automated analytic tools and techniques such as static or dynamic analysis. Components benefiting from manual review include for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.



Information Security Standard SEC501-09

(6) DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS

- **The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.**
- Supplemental Guidance: Attack surfaces of information systems are exposed areas that make those systems more vulnerable to cyber attacks. This includes any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers: (i) analyze both design and implementation changes to information systems; and (ii) mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.



Information Security Standard SEC501-09

(7) DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION

- **The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at the appropriate *depth of testing/evaluation*.**
- Supplemental Guidance: Verifying that security testing/evaluation provides complete coverage of required security controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating security control coverage at the highest levels of assurance can be provided by the use of formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.



Information Security Standard SEC501-09

SC-5 DENIAL OF SERVICE PROTECTION

Control Enhancements for Sensitive Systems:

(2) DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY

- **The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.**
- Supplemental Guidance: Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.



Information Security Standard SEC501-09

- **SC-7 BOUNDARY PROTECTION**

- Control: The information system:

(b) Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

(11) *BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*

The information system only allows incoming communications from [*Assignment: organization-defined authorized sources*] routed to [*Assignment: organization-defined authorized destinations*].

- Supplemental Guidance: This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of source/destination address pairs in lists of authorized/allowed communications, the absence of address pairs in lists of unauthorized/disallowed pairs, or meeting more



Information Security Standard SEC501-09

(3) DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING

- **The organization:**

(a) Employs *monitoring tools* to detect indicators of denial of service attacks against the information system; and

(b) Monitors *information system resources*] to determine if sufficient resources exist to prevent effective denial of service attacks.

Supplemental Guidance: Organizations consider utilization and capacity of information system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. Information system resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example, instituting disk quotas, configuring information systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data. Related controls: CA-7, SI-4.



Information Security Standard SEC501-09

SC-18 MOBILE CODE

Control: The organization:

(a) Defines acceptable and unacceptable mobile code and mobile code technologies;

(b) Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

(c) Authorizes, monitors, and controls the use of mobile code within the information system.

- Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.



Information Security Standard SEC501-09

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

- (a) Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
- (b) Authorizes, monitors, and controls the use of VoIP within the information system.



Information Security Standard SEC501-09

SI-4 INFORMATION SYSTEM MONITORING

Control Enhancements for Sensitive Systems:

(13) INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS

The organization:

- (a) Analyzes communications traffic/event patterns for the information system;**
- (b) Develops profiles representing common traffic patterns and/or events; and**
- (c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives .**



Information Security Standard SEC501-09

(16) INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

- **The organization correlates information from monitoring tools employed throughout the information system.**
- Supplemental Guidance: Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs. Related control: AU-6.



Information Security Standard SEC501-09

(20) INFORMATION SYSTEM MONITORING | PRIVILEGED USER

- The organization implements *additional monitoring*] of privileged users.



Information Security Standard SEC501-09

SI-10 INFORMATION INPUT VALIDATION

Control Enhancements for Sensitive Systems:

(2) INFORMATION INPUT VALIDATION / REVIEW / RESOLUTION OF ERRORS

- **The organization ensures that input validation errors are reviewed and resolved within 30-days of discovery.**
- Supplemental Guidance: Resolution of input validation errors includes, for example, correcting systemic causes of errors and resubmitting transactions with corrected input.

(3) INFORMATION INPUT VALIDATION / PREDICTABLE BEHAVIOR

- **The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.**
- Supplemental Guidance: A common vulnerability in organizational information systems is unpredictable behavior when invalid inputs are received. This control enhancement ensures that there is predictable behavior in the face of invalid inputs by specifying information system responses that facilitate transitioning the system to known states without adverse, unintended side effects.



Questions

Questions?

You may also send any questions to :
CommonwealthSecurity@VITA.Virginia.Gov



2014 Commonwealth Security Annual Report

Michael Watson, CISO

October 8, 2014



§ 2.2-2009

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.



Detailed Agency Information Security - 2014 Overall Security Program Scores

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

All ISOs must be appointed by their Agency Head. Once formally assigned , ISOs must complete the ISO education requirement by taking one of the two paths described below.

Steps to obtain COV ISO Certification for those who have a professional security certification:

- Possession of recognized professional IT Security Certification CISSP, CISM, CISA, SANS (others to be determined)
- VITA Training, Attend Information Security Orientation training
- ISO Academy, Successful completion of at least one course hour in the KC ISO Academy per year.
- ISOAG attendance, Attend the mandatory October 2014 ISOAG meeting.
- Maintain compliance with the continuing educational requirements of the professional IT security certification body.

Steps to obtain COV ISO Certification for those who do not have a professional security certification:

- VITA Training, attend Information Security Orientation training.
- ISO Academy, successful completion of at least 3 course hours per year in the KC ISO Academy.
- ISOAG attendance, attend the mandatory October 2013 ISOAG meeting.

Continuing Education Requirements in 2014 for ISOs that have already obtained the ISO Certification:

- Agree to the Commonwealth IT Security Code of Ethics
- Attend any mandatory ISOAG meetings each year
- Attend IS Orientation once every 2 years
- Obtain 20 hours of continuing education credit



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

Audit Plan Status: The Agency Head has submitted an IT Security Audit Plan for the period of fiscal year (FY) 2014-2015 or 2014-2016 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2014, Audit Plans submitted shall reflect FY 2015-2016)

- Pass - Plan is up to date and meets the criteria
- Fail - The IT Security Audit Plan on file does is not up to date and or does not meet the criteria

Current Percentage of Audits Received: The percentage of Audit Reports received per the IT Security Audit Plan in the current year.

- % - Submitted % of Audits Received for current year, based on Audit Plan
- N/A - Not Applicable due to no audits planned for the year
- N/C - Non Compliant due to no current Audit Plan in place

Percentage of Quarterly Updates Received in 2014:

- % - Submitted % of QUs for all open findings per CAPs submitted
- N/A - No Security Audits scheduled to be completed



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

3 Year Audit Obligation: This is the percent of sensitive systems audited within the last 3 years. The sensitive system list is validated against the Commonwealth Enterprise Technology Repository (CETR). For agencies required to submit to CETR, audits are not complete unless the sensitive system subject to the audit can be identified within CETR. This datapoint is based on the IT Security Audit Standard requirement: "At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years."

- N/C - Values cannot be calculated due to lack of current Audit Plan
- N/A - No Sensitive Systems to be audited

Business Impact Analysis Status: The Business Impact Analysis (BIA) has been provided by the agency. [To be considered complete all applications must follow the requirements of the IT Risk Management Standard \(SEC520-00, 3.2.2\)](#) Please note: If you have already submitted a BIA in 2012 or 2013 and have no changes, let Commonwealth Security know so you get credit for reviewing and having a current BIA on file.

- Pass – BIA is complete
- Fail – BIA has not been submitted or is incomplete
- Incomplete – Agency has submitted a BIA that is currently under review or required additional information.

BIA shall, at a minimum, identify:

- Business function name and owner
- Date BIA Completed and name of person that completed the BIA
- Primary objective of the business function
- Customers of the function (internal customers, Commonwealth Agency customers, government entity customers, public customers)



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

BIA shall, at a minimum, identify (con't):

- Identify whether the functions are mission essential
- Identify IT systems that the business functions rely on
- Description of the data used by the function, including the source, destination, and sensitivity
- Identify the recovery time objective (RTO)
- Identify the recovery point objective
- Rate the impact of non-performance of the function for:
 - Confidentiality – Impact on customer service, public perception/trust, impact on sensitive data
 - Integrity – Impact on finance, legality, regulation, customer service, public perception/trust
 - Availability – Impact on life, safety, customer service, public perception/trust, finance, recovery time objective, recovery point objective

Risk Assessment Plan Status: The Agency Head has submitted an IT Risk Assessment Plan for the period of fiscal year (FY) 2014-2015 or 2014-2016 for systems classified as sensitive based on confidentiality, integrity or availability (*Note: after July 1, 2014, Audit Plans submitted shall reflect FY 2015-2016*)

- Pass - Plan is up to date and meets the criteria
- Fail - The IT risk assessment plan on file does is not up to date and or does not meet the criteria



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

3 Year Risk Assessment Obligation: The percentage of Risk Assessment obligation met is calculated based on the percentage of sensitive systems that have had risk assessments conducted and submitted to Commonwealth Security and Risk Management within the last three years. The risk assessment date is assigned to each sensitive system and calculated as a percentage of total sensitive systems identified within the agency. For agencies required to submit to CETR, Risk assessments are not complete unless the sensitive system subject to the assessment can be identified within CETR. [The Risk Assessment information reported must follow the requirements of the IT Risk Management Standard \(SEC520-00, 3.3.3\).](#)

Pending CETR - Indicates the values cannot be calculated until the agency reconciles their audit plan system names with the CETR database.

Please Note: A status of "Pending Agency CETR Reconciliation" will change to "Failed" as of December 16, 2014. Again, please note that the closing date for the 2013 Commonwealth of Virginia Information Security Annual Report is **December 31, 2014**.



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

IDS Reports Submitted – Agencies shall provide Intrusion Detection System Reports to VITA at the end of each quarter. IDS reports should provide the following information:

1. Name of Agency
2. Date Range for the Report (example: Jan 1st 2013 – March 31st, 2013)
3. Total number of attacks per month (example: Jan 2013 = 1,000,000, Feb 2013=1,500,000, March 2013= 1,250,000)
4. Total number of high attacks per month
5. Total number of medium attacks per month
6. Total number of low attacks per month
7. Top 10 high attacks & number of attacks seen (example: SSH Brute Force, total: 100 attacks)
8. Top 10 Source IPs
9. Top 10 Destination IPs
10. Top 10 countries of origin of attacks with percentages per month (example: Jan 2013: US – 80%, China =4%, Russia = 3%, Canada = 3%, U.K. = 3%, India=2%, Brazil=2%, Germany=2%, Ireland=2%, Sweden=2%)
11. Top 10 types of attacks (example: Denial of Service, Privilege Escalation)
12. Top 10 inbound attacks by protocol/service/port (http/www/80)
13. Top 10 outbound attacks by protocol/service/port (http/www/80)



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

Vulnerability Scans Results Reported - For each IT system classified as sensitive, the data owning agency shall:

1. Conduct a vulnerability scan of the information system and hosted applications at least once every 90-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported.
2. Document and report vulnerabilities and risks identified in the vulnerability scans and related remedial actions to CSRM once every 90-days.

*Note: If no vulnerabilities were identified in a vulnerability scan, Agency must notify CISO that the vulnerability scan was conducted and there were no findings.

**Note: If VITA is an agency's service provider for performing the required vulnerability scans on an agency's behalf, those results are automatically reported to the CISO on the agency's behalf.

Vulnerability scans must be reported to the CISO using the Risk Assessment and Risk Treatment Plan templates



Secretariat: Administration

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
CB			N/C	N/A	N/C		N/C			
DGS			100%	0%	100%		N/C			
DHRM			0%	N/A	0%		N/C			
ELECT			0%	N/A	0%		N/C	Pending		



Secretariat: Agriculture & Forestry

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DOF			N/C	33%	N/C		N/C			
VDACS			100%	54%	38%		N/C			



Secretariat: Commerce & Trade

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
BOA	●	●	N/A	N/A	100%	●	N/C	●	●	●
DHCD	●	●	0%	0%	40%	●	N/C	●	●	●
DMME	●	●	N/C	0%	N/C	●	N/C	●	●	●
DOLI	●	●	N/C	N/A	N/C	●	N/C	●	●	●
DPOR	●	●	N/A	100%	100%	●	N/C	●	●	●
SBSD	●	●	N/C	N/A	N/C	●	N/C	●	●	●
TIC	●	●	0%	N/A	N/A	●	N/C	●	●	●
VEC	●	●	N/C	50%	N/C	●	N/C	●	●	●
VEDP	●	●	N/A	N/A	0%	●	N/C	●	●	●
VRA	●	●	N/C	N/A	N/C	●	N/C	●	●	●
VRC	●	●	N/A	N/A	N/A	●	N/C	●	●	●



Secretariat: Education

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DOE			0%	N/A	24%		N/C			
FCMV			N/A	N/A	N/A		N/C			
GH			N/C	N/A	N/C		N/C			
JYF			N/C	N/A	N/C		N/C			
LVA			0%	N/A	67%		N/C			
NSU			50%	N/A	47%		N/C			
RBC			N/C	N/A	N/C		N/C			
SCHEV			0%	N/A	0%		N/C			
SMV			N/A	N/A	0%		N/C			
SVHEC			N/A	N/A	N/A		N/C			
VCA			N/A	N/A	N/A		N/C			
VMFA			N/C	0%	N/C		N/C			
VSDB			N/C	N/A	N/C		N/C			
VSU			83%	38%	40%		N/C			



Executive

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
GOV			N/C	N/A	N/C		N/C			
OAG			N/C	N/A	N/C		N/C			
OSIG			N/A	N/A	N/A		N/C			



Secretariat: Finance

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DOA			0%	0%	53%		N/C			
DPB			N/A	N/A	0%		0%	Pending		
TAX			13%	50%	78%		N/C			
TD			0%	N/A	0%		N/C			



Secretariat: Finance

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DCR			N/C	0%	N/C		N/C			
DEQ			0%	0%	83%		N/C			
DGIF			0%	N/A	0%		N/C			
DHR			0%	33%	N/A		N/A			
MRC			0%	N/A	100%		100%			
VMNH			N/A	N/A	0%		N/C			



Secretariat: Health & Human Resources

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
CSA	●	●	N/C	N/A	N/C	●	N/C	●	●	●
DARS	●	●	50%	47%	79%	●	N/C	●	●	●
DBHDS	●	●	N/C	N/A	N/C	●	N/C	●	●	●
DHP	●	●	0%	N/A	50%	●	N/C	●	●	●
DMAS	●	●	20%	50%	84%	●	N/C	●	●	●
DSS	●	●	0%	0%	6%	●	N/C	●	●	●
VDH	●	●	40%	50%	58%	●	N/C	●	●	●
VFHY	●	●	N/A	N/A	N/A	●	N/A	●	●	●



Independent Branch Agencies

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
IDC			0%	0%	50%		N/C			
SCC			33%	80%	100%		N/C			
SLD			40%	0%	67%		N/C			
VCSP			0%	N/A	83%		N/C			
VRS			0%	36%	100%		N/C			
VWC			0%	0%	100%		N/C			



Secretariat: Natural Resources

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DCR			N/C	0%	N/C		N/C			
DEQ			0%	0%	83%		N/C			
DGIF			0%	N/A	0%		N/C			
DHR			0%	33%	N/A		N/A			
MRC			0%	N/A	100%		100%			
VMNH			N/A	N/A	0%		N/C			



Secretariat: Public Safety

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
ABC	●	●	0%	71%	50%	●	N/C	●	●	●
CASC	●	●	N/A	N/A	N/A	●	N/C	●	●	●
DCJS		●	N/C	N/A	N/C	●	N/C	●	●	●
DFP	●	●	N/C	N/A	N/C	●	N/C	Pending	●	●
DFS	●	●	0%	N/A	100%	●	N/C	●	●	●
DJJ	●	●	N/C	100%	N/C	●	N/C	●	●	●
DMA	●	●	N/C	N/A	N/C	●	N/C	●	●	●
DOC	●	●	N/C	45%	N/C	●	100%	●	●	●
DVS	●	●	0%	N/A	100%	●	N/C	●	●	●
VDEM	●	●	0%	N/A	0%	●	N/C	●	●	●
VSP	●	●	50%	48%	88%	●	N/C	Pending	●	●



Secretariat: Technology

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
IEIA			0%	N/A	0%		N/C			
VITA			0%	50%	0%		N/C			



Secretariat: Transportation

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DMV			N/C	25%	N/C		N/C			
DOAV			N/A	75%	100%		N/C			
DRPT			N/C	N/A	N/C		N/C	Pending		
MVDB			N/C	N/A	N/C		N/C			
VDOT			11%	55%	81%		N/C			



FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings, CSRM will record this action from the audit report received. No further action will be needed.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

December 31, 2014



Annual Report - Risk Management Data Points

Jon Smith

Director, Risk Management

ISOAG

October 8, 2014



Business Impact Analysis (BIA)

- Purpose
 - To identify the level of impact that IT systems have to agency business functions
 - To identify the level of impact systems have to the Commonwealth as a whole
- Metrics
 - All business processes must be labeled as mission essential or not mission essential
 - All business processes must be rated for impacts on:
 - Life
 - Safety
 - Finances
 - Regulation/compliance
 - Customer service
 - Privacy



BIA Metrics (Continued)

- All business processes must have an identified Recovery Time Objective (RTO)
- All business processes must have an identified Recovery Point Objective (RPO)
- All business processes must identify whether the process includes the processing of data sensitive relative to confidentiality and the number of records
- All business processes must identify applications (both internal and external to the agency) on which the processes rely
- Source and destination of the data
- All applications must be associated with at least one business process



BIA & CSRM

What does CSRM do with the BIA submitted?

- Review for completeness based on metrics for compliance and follow up with submitter as necessary
- Import data to RSA Archer (GRC software)
- Analyze data to identify inconsistencies, anomalies and risks
- Evaluate whether systems are correctly rated for sensitivity based on the business functions that they support
- Understand cross agency dependencies



Risk Assessment

- Purpose
 - Assess COV sensitive systems and data environments for risks to agency business
 - Ensure that identified risks are resolved, mitigated and/or monitored
- Metrics
 - 3 year risk assessment plan
 - Risk assessments of sensitive systems conducted not less than every 3 years
 - Risk treatment plan for findings with a value greater than low



Risk Assessment Metrics (Cont'd)

- Agencies must:
 - Submit 3 year risk assessment plan annually
 - Submit risk assessments as completed
 - Submit risk treatment plans for findings with a risk value greater than low
 - Submit quarterly updates on the progress of treating the risks until the risk has been resolved, reduced to acceptable risk level, or accepted.



Risk Assessment & CSRM

- What does CSRM do with the risk assessment information?
 - Review for submissions completeness
 - Track risk assessment planning and progress
 - Review and track risk findings and resolution progress
 - Determine if there are common risks identified that may benefit from an enterprise wide solution
 - Trending



Vulnerability Scanning

- Purpose
 - Identify functions, ports, protocols and services that should not be accessible to users or devices
 - Identify improperly configured or incorrectly operating information flow mechanisms
 - Identify software flaws such as missing patches or end-of-life/end-of-support software
 - Measure potential impact of exploitation of discovered vulnerabilities and take remedial actions



Vulnerability Scanning

- Vulnerability scanning is not a “one and done” activity

Scan -> remediate -> rescan -> remediate ->rescan

- Agency vulnerability scanning programs must consider and scan multiple tiers of the IT systems
 - Hardware and OS level scanning (servers, firewalls, etc.)
 - Application vulnerability scanning (i.e. web application vulnerability scanning – public and internal)



Vulnerability Scanning

- IT partnership infrastructure assets of VITA full service customers are scanned on behalf of the customers
- Agencies operating infrastructure assets outside of the partnership enterprise are responsible for the vulnerability scanning of those assets
- Agencies (to include VITA full service customers) are responsible for the vulnerability scanning of their applications
- VITA does offers a web vulnerability scanning service – Bill Freda will discuss in more detail



Vulnerability Scanning Requirements

- Vulnerability scanning SEC 501 (RA-5)
 - Public facing and sensitive systems must be scanned once every 90 days and as new vulnerabilities potentially affecting these systems are identified
- Reporting to CSRM (SEC 520)
 - Document and report vulnerabilities and risks identified in the vulnerability scans of sensitive public facing systems and related remedial actions to CSRM once every 90-days

*Note – If your agency does not have public facing sensitive systems, you must notify CommonwealthSecurity@vita.virginia.gov



Vulnerability Scanning & CSRM

- What will CSRM do with these reports?
 - Track identified vulnerabilities/findings and remedial actions
 - Determine if high risk vulnerabilities should have mitigating controls put in place until vulnerability has been remediated
 - Identify risks to the Commonwealth/enterprise
 - Identify common vulnerabilities and determine if enterprise or Commonwealth wide solutions should be recommended to mitigate common risks



Vulnerability Scanning in the COV

- Exploitation of vulnerable public facing web applications remains a primary vector of attack against Commonwealth systems
- Vulnerability scanning requirements are not new, however the reporting requirements were introduced with SEC 520 for sensitive public facing systems
- Lack of reporting to CSRM indicates that the vulnerability scanning process is still immature
- Future releases of SEC 520 will expand requirements to report on all public facing vulnerability scanning activities



Intrusion Detection System (IDS)

- Purpose
 - To monitor incoming and outgoing network traffic for signs of attack
 - IDS/IPS can be signature or behavior based
 - Can provide intelligence on:
 - Severity of attacks
 - Types of attacks
 - Origin of attacks
 - Protocols and services being attacked
- Metrics:
 - Quarterly submission of IDS reports



IDS Requirements

- Agencies shall report the following IDS information to CSRM at the end of each quarter:
 - Name of Agency
 - Date Range for the Report
 - Total number of attacks per month (Total, high, medium, and low)
 - Top 10 high attacks & number of attacks seen
 - Top 10 source IPs
 - Top 10 destination IPs
 - Top 10 countries of origin of attacks with percentages per month
 - Top 10 types of attacks
 - Top 10 inbound attacks by protocol/service/port
 - Top 10 outbound attacks by protocol/service/port



IDS Requirements

- For full service VITA customers, with all assets residing on the partnership infrastructure, these reports are submitted on the agency's behalf
- Agencies with networks external to the partnership enterprise must submit IDS reports for those networks

*Note - If you are having trouble configuring reports for the requirements, contact CSRM



IDS & CSRM

- What does CSRM do with these reports?
 - Analyze reports for threat intelligence
 - Who's attacking us?
 - Where are they attacking us from?
 - How often are they attacking us?
 - What types of attacks are they using?
 - When are they attacking us
 - Identify attack trends
 - Determine if solutions should be implemented to mitigate risks



Questions?





Virginia Information Technologies Agency

Web Application Vulnerability Scanning Service

Bill Freda
Security Analyst



Why we created this service

- The Web Application Vulnerability Service
 - Created to fill a gap
 - Began as a necessity in response to incidents
 - Designed as a tool for state entities to use to supplement their existing application security program
 - Very expensive to obtain this service from a professional penetration testing providers
 - Quality of providers is unpredictable



What we used to do

- In response to an incident we will conduct a web application vulnerability assessment to address the incident.
 - Generally assists in locating the exploited vulnerability and guiding the remediation of the incident
- We would conduct a web application vulnerability assessments upon request for free (pre service creation)



What we currently Provide

- Incident Response Web Application Vulnerability Assessments at no charge
- Non-Incident Response Web Application Vulnerability Assessments for a fee.
 - **Basic Application Vulnerability Scan**
 - **Enhanced Application Vulnerability Scan**
 - **Enhanced Application Vulnerability Scan - Annual Plan**



Basic Application Vulnerability Scan

- Under the basic scan option, the customer is hiring VITA to perform a single scan of one application. The customer will be provided with a standard report from the scan. The customer is responsible for verifying and remediating the vulnerabilities that were identified by the scan. This option is appropriate for customers that have the ability to verify and remediate the vulnerabilities without support from VITA.
 - \$1856.93/scan



Enhanced Web Application Vulnerability Scan

- Under the enhanced scan option, the customer is hiring VITA to perform a single scan of one application, verify the vulnerabilities identified by the scan and provide advice and guidance on how to remediate the identified vulnerabilities. The customer will be provided with a customized report that they can use to remediate the vulnerabilities that were identified by the scan. This option is appropriate for customers that do not have the ability to verify and remediate the vulnerabilities without support from VITA.
 - \$3016.22/scan



Enhanced Web Application Vulnerability Scan – Annual Option

- Same as the Enhanced Single option but includes 6 scans any way you slice it.
 - \$15,199.11
- We are also priced and approved for Web Application Penetration Testing.
 - Same pricing as the Enhanced option
 - Offering Available in FY2015
- <http://shop.vita.virginia.gov/>
 - Under Security



Testing for Web Server Configuration Checks

- Checks for Web Servers Problems – Determines if dangerous **HTTP methods are enabled on the web server (e.g. PUT, TRACE, DELETE)**
- Verify Web Server Technologies
- Vulnerable Web Servers
- Vulnerable Web Server Technologies – such as “PHP 4.3.0 file disclosure and possible code execution.

Red indicates a frequent finding



Testing for Parameter Manipulation Checks

Cross-Site Scripting (XSS)	Path Disclosure
Cross-Site Request Forgery (CSRF)	XPATH Injection
SQL Injection	LDAP Injection
Code Execution	Cookie Manipulation
Directory Traversal	Arbitrary File creation
HTTP Parameter Pollution	Arbitrary File deletion
File Inclusion	Email Injection
Script Source Code Disclosure	File Tampering
CRLF Injection	URL redirection
Cross Frame Scripting (XFS)	Remote XSL inclusion
PHP Code Injection	DOM XSS



MultiRequest Parameter Manipulation & Passwords

- Blind SQL/XPath Injection
- Input Validation
- Buffer Overflows
- Sub-Domain Scanning
- Weak Password Checks
- Weak HTTP Passwords
- Authentication attacks
- Weak FTP passwords



Text Search File Checks, Upload Checks And Directory Checks

Checks for Backup Files or Directories	HTTP Verb Tampering
Cross Site Scripting in URI	Directory Listings
Checks for Script Errors	Source Code Disclosure
Unrestricted File uploads Checks	Check for Common Files
Looks for Common Files (such as logs, traces, CVS)	Check for Email Addresses
Discover Sensitive Files/Directories	Microsoft Office Possible Sensitive Information
Discovers Directories with Weak Permissions	Local Path Disclosure
Cross Site Scripting in Path and PHPSESSID Session Fixation.	Error Messages
Web Applications	Trojan Shell Scripts



Port Scanner and Network Alerts

Finds All Open Ports on Servers

Displays Network Banner of Port

DNS Server Vulnerability: Open Zone Transfer

DNS Server Vulnerability: Open Recursion

DNS Server Vulnerability: Cache Poisoning

Finds List of Writable FTP Directories

FTP Anonymous Access Allowed

Checks for Badly Configured Proxy Servers

Checks for Weak SNMP Community Strings

Finds Weak SSL Ciphers



Seeking Web App Vulnerability Knowledge

- OWASP !
 - The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.
- https://www.owasp.org/index.php/Main_Page



What is the OWASP Top 10?

- The OWASP Top 10 provides:
- A list of the 10 Most Critical Web Application Security Risks
- And for each Risk it provides:
- A description
- Example vulnerabilities
- Example attacks
- Guidance on how to avoid
- References to OWASP & other related resources



SANS MSISAC Developer Classes

Developer			
<u>Course</u>	<u>Price</u>	<u>Options †</u>	<u>Free Demo</u>
<u>DEV522: Defending Web Applications Security Essentials</u>	\$4,670	<u>GWEB \$599</u>	<u>DEV522 Demo</u>
<u>DEV541: Secure Coding in Java/JEE: Developing Defensible Applications</u>	\$3,950	<u>GSSP-JAVA \$599</u>	<u>DEV541 Demo</u>
<u>DEV544: Secure Coding in .NET: Developing Defensible Applications</u>	\$3,950	<u>GSSP-.NET \$599</u>	<u>DEV544 Demo</u>

<http://www.sans.org/ondemand/courses/all/>

- MSISAC Government Purchase in June/July Buy Window offers huge discounts.
- 2014 Cost = \$1650 per seat



Questions?

- For more information please contact CSRM:
 - commonwealthsecurity@vita.virginia.gov
- Contact your agency CAM



Virginia Information Technologies Agency

Commonwealth of Virginia October 2014 ISOAG

Agency Data Points

AUDITS

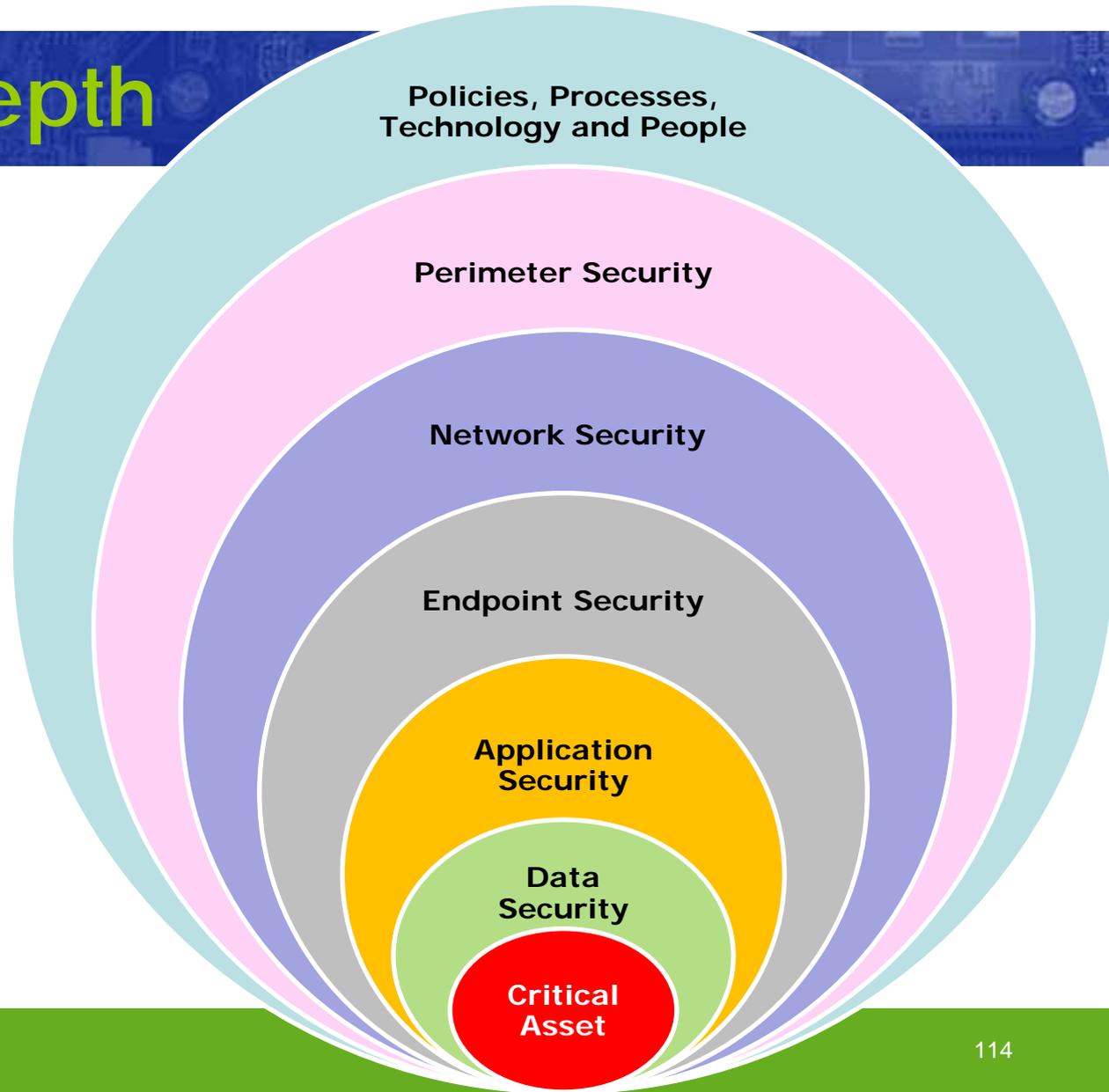
Ed Miller, VITA

Defense-in-Depth

From Wikipedia:

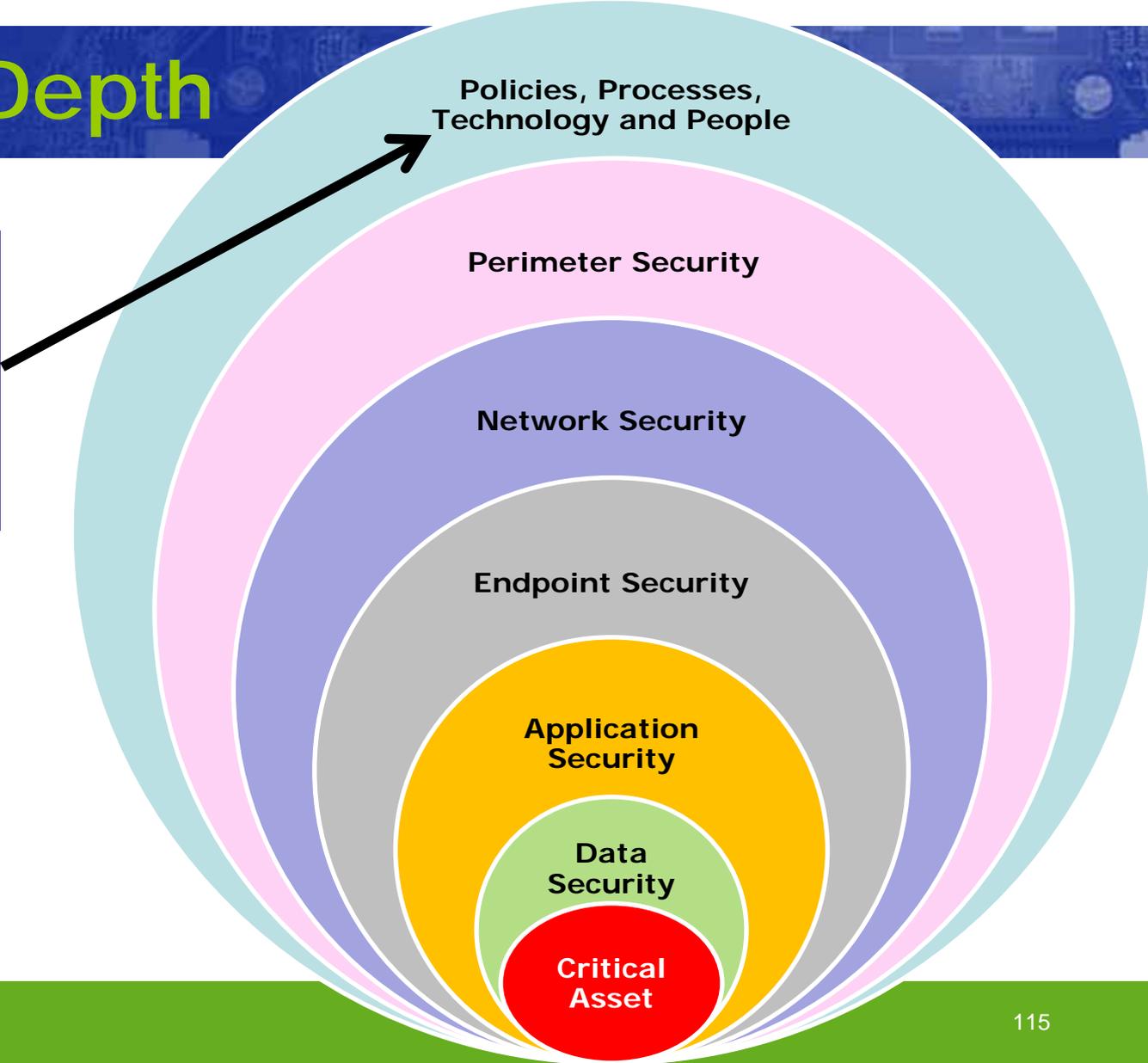
Defense-in-depth is an information assurance (IA) concept in which **multiple layers of security controls** (defense) are placed throughout an information technology (IT) system.

Its intent is to **provide redundancy** in the event a security control fails or a vulnerability is exploited .



Defense-in-Depth

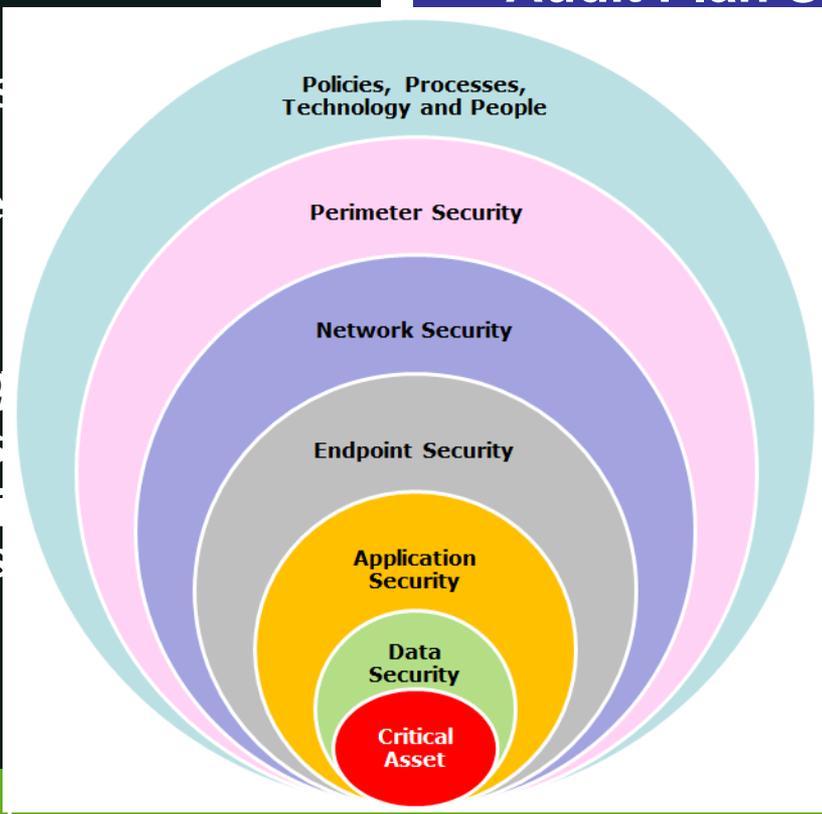
**Policies,
Processes,
Technology &
People**



Policies, Processes, Technology & People

- IT Security Governance
- Risk Management
- Security Awareness Training
- Security Policies Compliance
- Security Architecture Design
- Vulnerability Assessments
- Threat Modeling
- Security Metrics
- Incident Detection Reporting & Response
- Monitoring and Assessments
- Auditing

- ## DATA POINTS
- ISO Certification Status
 - Audit Plan Status
 - Number of Audits Received
 - Number of Quarterly Updates
 - Risk Assessment Obligation
 - Impact Analysis
 - Incident Response Plan Status
 - Vulnerability Assessment
 - Security Scans Submitted
 - Security Scans Results





Data Points

ISO Certification Status

In order obtain the ISO Certification for *the first time*: , you need to meet the following conditions:

1. Have an industry recognized 3rd party IT security certification (CISSP, CISM, etc.) & take 1 course in the KC/ISO Academy –OR- if you don't have a 3rd party IT security certification, you must take 3 courses in the KC/ISO Academy.
2. Attend any mandatory ISOAG meetings in 2014
3. Attend IS Orientation once every 2 years



Data Points

ISO Certification Status

In order to *maintain* your status as a Commonwealth Certified ISO in 2014, you need to meet 4 basic conditions:

1. Agree to the Commonwealth IT Security Code of Ethics
2. Attend any mandatory ISOAG meetings in 2014
3. Attend IS Orientation once every 2 years
4. Meet the requirements for continuing education for any 3rd party IT security certifications that you hold OR obtain 20 hours of continuing education credit per year. At least 1 of your continuing education hours (i.e. 1 course) must be obtained through the KC/ISO Academy



How to Earn Continuing Education (CPE)

- Take add'l IT security courses in the KC ISO Academy (1 course=1 hr)
- Attend training courses or seminars related to IT Security
- Attend IT security conferences
- Attend ISOAG Meetings
- Attend chapter meetings of a recognized IT security organization
- Take IT security related academic courses at a higher ed institution
- Complete IT Security related webcasts, podcasts or other computer based training
- Read IT security related books or articles (limit of 10 hrs/year)
- Publish an IT Security related book or article
- Attend vendor sales/marketing presentations (limit of 5 hrs/year)
- Teach or present on an IT security related topic
- Serve or volunteer for committee work on the **COV Security Council**

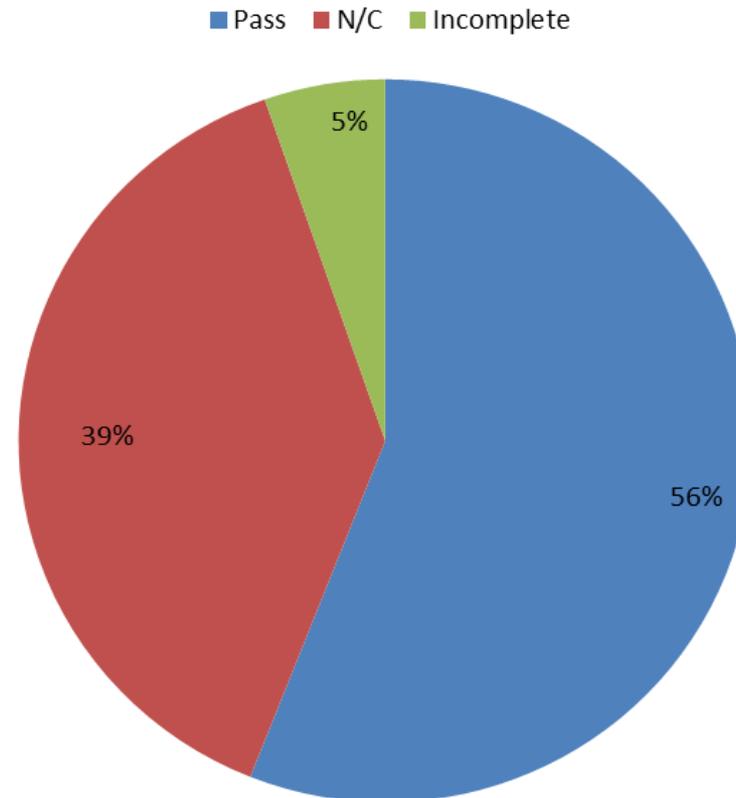


Reporting Continuing Education to CSRSM

- When you have completed **all 20 hours** of required continuing education activities in 2014, send an email to commonwealthsecurity@vita.virginia.gov indicating that you have completed.
- We do not need notification for each time you complete a specific or individual activity. We would appreciate a brief description of the activities you performed.
- We also do not require any specific documentation that you have completed any education requirements, your voucher is good enough. However, we do suggest that you maintain your own records of completion and other supporting documentation.

ISO Certifications

Commonwealth ISO Certifications 2013





Audit



§ 2.2-2009

- A. To provide for the security of state government electronic information from unauthorized uses, intrusions or other security threats, ***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 electronic information...***
- B. The CIO shall also develop policies, procedures, and standards that shall address the ***scope of security audits and the frequency*** of such security audits....



IT Security Audit Standard

- ITRM Policies, Standards and Guidelines
- IT Security Audit Standard (SEC502-02) (01/06/2013)



Audit

Each Agency shall establish an IT Security Audit Program.

The program shall include assessing the risks associated with the state *IT systems* for which it is the Data Owner and ***conducting IT Security Audits at a frequency relative to the risk*** identified by the Agency.

At a minimum, IT systems that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, ***shall be assessed (audited) at least once every three years.***



Conduct IT Security Audits

- PERFORMANCE OF IT SECURITY AUDITS
- Create and submit an IT Security Audit Plan to the CISO
 - AH approval Required
 - Review and submit annually
 - Populated from Risk Management Framework
 - BIA, Data Classification, Data Sensitivity Review, Risk Assessments, Changes, Adds, Deletes



Data Points

2014 Audit Plan Status

IT Security Audit Plan Template

Agency Information		Contact Information	
Agency Name	Department of Divisions	Name	Jill Edgar
Agency Acronym	DOFD	Title	ISO
Agency Number	000	E-mail	Jill.edgar@dofd.virginia.gov
Date of submission	6/1/12	Phone	804-555-9876

IT System Acronym *	IT System Name	Planned Auditor	Date Last Audited (MM/YY)	Scheduled Audit Completion Date (Minimum once every 3 years)			Areas for Special Emphasis and Additional Audit Requirements
				2013 (MM/YY)	2014 (MM/YY)	2015 (MM/YY)	
SAS	System Application System	Internal Audit	3/31/12		3/31/14		
XYZ	Database XYZ	Internal Audit	11/30/10	8/31/13			
HAA	Historical Archiving Application	Verify Assurance LLP	NEW			4/30/15	

Submit an Audit Plan to CSRM annually using the standard template.

CC: your AH and get it to us by 12/31 each year.

If your agency has access to CETR, the systems you list to audit, MUST be found in the CETR database.

Every sensitive system is required to be audited, at least once every 3 years, or more frequently commensurate with risk.



Data Points

2014 Percentage of Audits Received

IT Security Audit Plan Template

Agency Information		Contact Information	
Agency Name	Department of Divisions	Name	Jill Edgar
Agency Acronym	DOFD	Title	ISO
Agency Number	000	E-mail	Jill.edgar@dofd.virginia.gov
Date of submission	6/1/12	Phone	804-555-9876

IT System Acronym *	IT System Name	Planned Auditor	Date Last Audited (MM/YY)	Scheduled Audit Completion Date (Minimum once every 3 years)			Areas for Special Emphasis and Additional Audit Requirements
				2013 (MM/YY)	2014 (MM/YY)	2015 (MM/YY)	
SAS	System Application System	Internal Audit	3/31/12		3/31/14		
XYZ	Database XYZ	Internal Audit	11/30/10	8/31/13			
HAA	Historical Archiving Application	Verify Assurance LLP	NEW			4/30/15	

This metric is simply the % of audits on your audit plan, scheduled for the current year, that were completed so far this year.



Data Points

2014 Percentage of Quarterly Updates Received

Corrective Action Plan and IT Security Audit Quarterly Summary 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.

Submission Date:	3/29/2013
------------------	-----------

Audit Name:	02-2013-A							
IT System Name (s):	Historical Archive Database							
Audit Finding Number	SEC501-07 Control Number	Summary	Agency ¹ Concurs	Planned Corrective Action or Mitigating Controls ²	Responsible Person(s)	Status ³	Due Date	Exception on File ⁴
1	CM-2	Baseline Config	Concurs	System will be configured using CIS baseline utility for SQL server	Adam Freeman	U	5/15/2013	No
2	AC-8	System Banner Notification	Concurs	System needs to display a system use notification banner prior to granting access to the system	Jay Britt	C	4/30/2013	No
3	MA-5	Maint Personnel	Concurs	3 of 7 personnel sampled for performing maintenance on HAA did not have proper authorization forms in file. All maint staff will be updated with proper authorization forms.	Janet Lupinski	U	4/17/2013	No

Every quarter, each agency is required to submit a "Quarterly Update" to summarize the status of all open IT security audit findings until they are resolved.

Once all findings are resolved, you can stop sending us QU's.

However, make sure you send us at least 1 more QU to let us know that they are resolved.



Data Points

2014 Percentage of Quarterly Updates Received

- The metric shows the current % of quarterly updates (QU's) received, based on the total # of QU's expected by the end of the year.
- For any finding open since 2013, we expect to receive a QU each quarter in 2014, until the finding is closed.
- For new findings reported in 2013, we expect to receive a QU each quarter in 2014, following the quarter in which the finding was first reported.



Data Points

2014 Percentage of Quarterly Updates Received

Example: Agency currently has findings that are still open from 2013

October 2014 marks the start of the 4th quarter for the CY. So for any finding open since 2013, we would expect, or soon expect, to have 3 QU's submitted to us.

So: As of Oct: [4 QU's expected by CY-end] / [3 QU's rec'd] = 75%

Further assume that the agency submitted a new audit report & CAP in March 2014. In this case, it means that only 3 QU's are expected for those findings by the end of CY 2014.

So: As of Oct: [3 QU's expected by CY-end] / [2 QU's rec'd] = 67%

2014 Percentage of Quarterly Updates Received: = 71%



Data Points

3 Year Audit Obligation

This metric is simply the percentage of sensitive systems, as reported on your audit plan, that have been audited over the last 3 years: 2014-2013-2012.

When an audit is completed, you must submit the audit report and associated CAP to CSRM. We will review it and record the findings in Archer.

Archer uses an attribute for each "system" called "Year Placed Into Service" that is pulled from CETR. It also updates a field for the system called "Last Audit Date" whenever an audit is recorded.

So, if the system was placed into service prior to 2012, and the last audit date is blank or more than 3 years ago, it's going to negatively impact this metric.

Summary

That covers the data points for:

ISO Certification Status

Audit Plan Status

Percentage of Audits Received

Percentage of Quarterly Updates Received

3 Year Audit Obligation



RSA Archer

RSA Archer is the commonwealth's eGRC program (Enterprise Governance, Risk & Compliance).

We have been using at CSRM for just over a year now.

Most agency ISO's have been given read-only access to Archer for their agency's data.





RSA Archer in 2015

We're planning to expand access in 2015 to:

- Secondary ISO's
- Auditors
- AITR's

We are also looking into the feasibility of allowing agencies' direct online submission using Archer for:

- BIA's
- Risk Assessments
- Audit Plans
- Audit Reports
- Quarterly Updates

Look for some new training courses on how to use Archer in 2015.



Questions?

Ed Miller

804-416-6027

Edward.miller@vita.virginia.gov



Virginia Information Technologies Agency

FEEDBACK

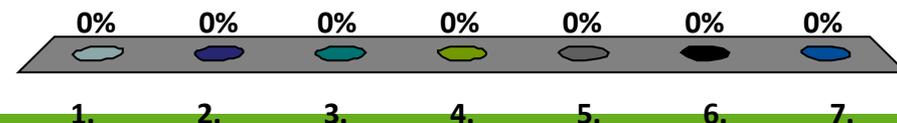
Commonwealth of Virginia
October 2014 ISOAG





Overall, how well do you feel you understand your agency's data points?

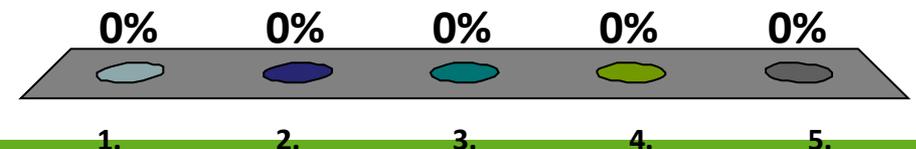
1. Completely Understand
2. Understand
3. Somewhat Understand
4. Neutral
5. Somewhat Confused
6. Confused
7. Completely Confused





Do you think that these metrics have helped your agency identify places where improvements in security can be made?

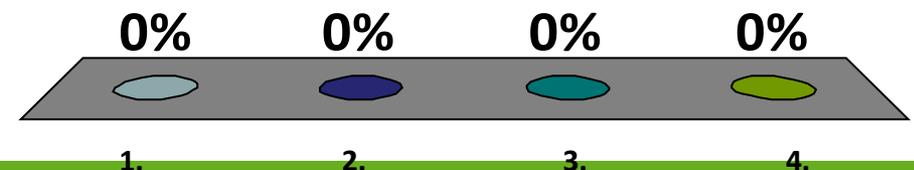
1. Significantly helped
2. Somewhat helped
3. Neutral
4. Not very helpful
5. Not at all helpful





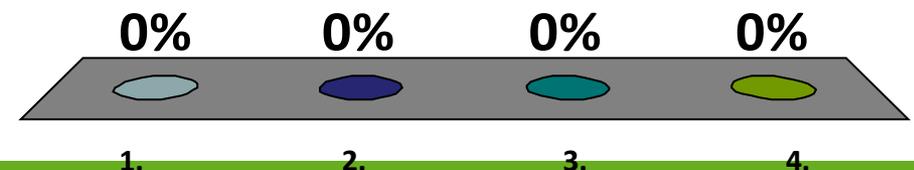
Identify the “audit” metric that you are the most uncertain of what it means.

1. Audit Plan Status
2. % of Audits Received
3. % of Quarterly Updates Received
4. 3 Year Audit Obligation



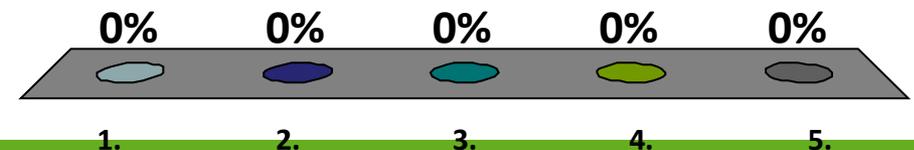
Identify the “audit” metric that you are the most uncertain of what you need to do to improve it.

1. Audit Plan Status
2. % of Audits Received
3. % of Quarterly Updates Received
4. 3 Year Audit Obligation



Identify the “risk” metric that you are the most uncertain of what it means.

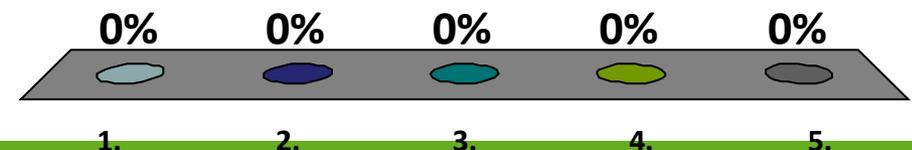
1. Business Impact Analysis Status
2. Risk Assessment Plan Status
3. 3 Year Risk Assessment Obligation
4. IDS Reports Submitted
5. Vulnerability Scan Results Reported





Identify the "risk" metric that you are the most uncertain of what you need to do to improve it.

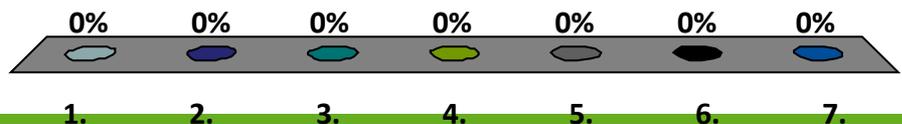
1. Business Impact Analysis Status
2. Risk Assessment Plan Status
3. 3 Year Risk Assessment Obligation
4. IDS Reports Submitted
5. Vulnerability Scan Results Reported





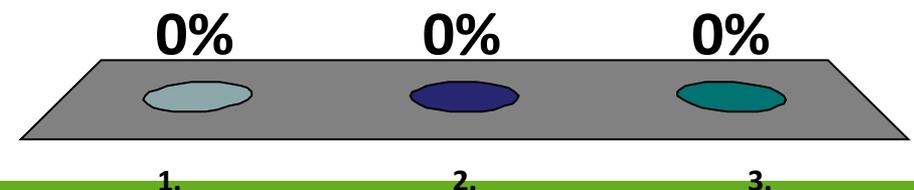
How well do you understand the requirements to obtain or maintain your Commonwealth ISO Certification?

- 1. Completely Understand
- 2. Understand
- 3. Somewhat understand
- 4. Neutral
- 5. Somewhat confused
- 6. Confused
- 7. Completely confused



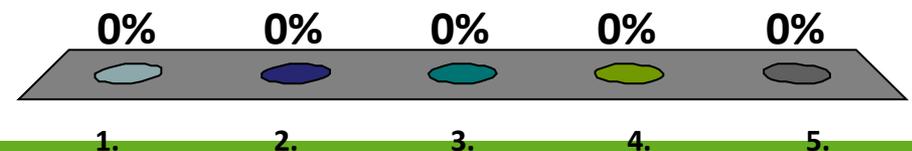
Does your agency head (or agency executives) ask you to explain your agency's scores to them?

1. Yes
2. Sometimes
3. Never



The commonwealth data points, as they appear for your agency, reflect mostly on the progress of your agency's ... ?

1. IT Security Management
2. Internal Auditing
3. Agency Head
4. Transformation
5. Not applicable – outside of your agency's control





Thank you!

Please turn in your clickers!



Commonwealth IT Risk Management Program

Jon Smith

Director, Risk Management

ISOAG

October 8, 2014



IT Risk Management

IT risk management is the application of risk management to information technology context in order to manage IT risk, i.e.:

The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise – (Wikipedia)



Risk Management Inputs

- Business impact analysis
- IT risk assessment findings
- IT security audit findings
- Vulnerabilities
- Security incidents
- Operational findings
 - Patching, End-of-life/end-of-support software, etc...
- Cyber intelligence
 - Vulnerability announcements (security alerts/advisories)
 - Sources: MSISAC, US CERT, FBI, DHS, Fusion Center, ISOs, etc...



Risk Impacts

- Understanding the IT systems and the business processes they support helps determine:
 - the potential impacts to the business if/when an event, such as a disaster or security incident affects an IT system
 - the business processes that are potentially impacted by an identified vulnerability or threat (i.e. vulnerability scanning, zero-day announcement, intelligence, etc...)
 - the potential impacts and risks associated with findings (risk, security audit, and operational findings)



Mitigating Controls

- Not all threats and risks can be eliminated
 - Reduce the likelihood of occurrence
 - Limit the impact
 - Reduce the sensitivity of the data/system
- Remediation of vulnerabilities may not be immediately possible (i.e. patches not released)
- What are possible mitigating controls for open vulnerabilities?
 - Additional monitoring
 - Whitelisting
 - Restricting public access (internet)
 - Remove from the network



Remediation

- Prioritize remediation and restoration based on:
 - Overall risk/threat
 - Impacts to the business
 - Life
 - Safety
 - Finances
 - Regulation/compliance
 - Customer service
 - Privacy
 - Mission
 - Likelihood of occurrence
 - Dependencies



Risk Management Planning

- Remediation and risk treatment activities require planning
 - Corrective action plans (audit)
 - Risk treatment plans (risk findings)
 - Resource planning (strategic planning)
- Incorporate security and risk management planning into the IT strategic planning process
 - VITA/CSRM is identifying operational risks and issues (ORI) in relation to IT security and risk management
 - Compliance
 - Operational risks (end-of-life software, critical vulnerabilities, etc...)
 - Agencies must plan for remediation of ORIs



Risk Management Framework

- February 2014:
 - Governor McAuliffe Announces Virginia Adopts National Cybersecurity Framework
- SEC 520 IT Risk Management Standard
 - Risk Management Framework based on the National Cybersecurity Framework
 - Five primary functions of security and risk management
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover



Identify

- Develop the institutional understanding to manage the information security risks to the organizations IT systems, assets, data, and the business functions necessary to accomplish commonwealth agency missions that they support
- Metrics:
 - Business impact analysis'
 - Risk assessments
 - IDS reports
 - IT security audits
 - Vulnerabilities (vulnerability scanning)
 - Cyber intelligence
 - Open findings related to Identify



Protect

- Develop and implement the appropriate safeguards, prioritized through the organization's risk management program to ensure the continued operation of the organization's business functions
- Metrics:
 - ISO Certification
 - Open findings related to Protect



Detect

- Develop and implement the appropriate activities to identify the occurrence of an information security event
- Metrics:
 - IDS reports
 - Vulnerability scanning reports
 - Open findings related to Detect



Respond

- Develop and implement the appropriate activities to take action regarding a detected information security event
- Metrics:
 - Each agency should have reported at least one suspected security issue
 - Response time
 - Open findings related to Respond



Recover

- Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a information security event.
- Metrics:
 - BIA – Identifies RTO/RPO
 - Open findings related to Recover



Commonwealth Risk Assessment

- CSRM will facilitate a Commonwealth wide Risk Assessment
- MSISAC, in partnership with the Department of Homeland Security (DHS), annually facilitates a National Cyber Security Review (NCSR)
 - Survey based assessment
 - Open to all State, Local, Tribal and Territorial (SLTT) government entities
 - Results include reports that help you assess how your organization compares to similar organization
 - No cost to SLTT government entities
- CSRM participates in the review annually
- DHS is seeking additional participants in 2014
- CSRM is considering utilizing the NCSR survey as part of the Commonwealth risk assessment



Questions?





Virginia Information Technologies Agency

3rd Party Hosting Security Considerations

John Craft
Security Architect



eGov Offerings

- COV has several hosting vendors on the eGov contract:
 - Sitevision
 - Cyberdata
 - AIS
- Detailed contract and procedural information:
 - http://shop.vita.virginia.gov/ProductDetail.aspx?id=6442470595&TX_ID=6442469741



ITP Offering

- ITP Hosting Offering
 - Request additional information for this service through your CAM
 - Key characteristics of this service to consider:
 - Customizable
 - Contractual control already in place
 - Established security controls already in place
 - 24x7 monitoring, IDS/IPS, boundary control, auditing and logging, incident response, etc.
 - Architecture complies with enterprise standards

Other Hosting Vendors

- “From a security standpoint, is it possible for my agency to use a different vendor than those named on the eGov contracts or the ITP?”
 - Amazon Web Services (AWS)
 - Microsoft Azure
 - Dropbox
 - Box
- Possibly, with considerations
- Established procedure for requesting



Other Hosting Vendors Process

- Request through CAM
- CAM engages service owner
- Service owner creates decision brief
 - Uniqueness of requirement and sensitivity of data are primary considerations
- Commonwealth CIO evaluates and provides approval / denial decision to agency with any associated conditions or requirements



Standards Compliance

- Vendor must comply with COV security and audit standards:
 - SEC501-08 IT Information Security Standard
 - “Prohibit the storage of any Commonwealth data on IT systems that are not under the **contractual control** of the Commonwealth of Virginia. The owner of the IT System must adhere to the latest Commonwealth of Virginia information security policies and standards as well as the latest Commonwealth of Virginia auditing policies and standards.”
 - SEC502-02 IT Security Audit Standard
 - SEC514-03 Removal of Commonwealth Data from Electronic Media Standard
 - Any other standards that apply to the data / service



Contractual Control

- What does this mean?

In addition to complying with all applicable standards, the vendor must contractually agree to offer equivalent security and audit controls to those already utilized by the enterprise and define mechanisms that will allow the agency to validate that the vendor is effectively implementing and executing those controls.



Significant Security Considerations

- 24x7 monitoring and logging
- Incident response
- IDS / IPS
- Secure remote management and authentication
- Vendor access controls
- Vendor audit reports (e.g., SSAE-16)
- Data encryption (sensitive data)
- Data removal / destruction policy
- Data backup and disaster recovery
- Vendor employee security awareness training
- Vendor employee background checks
- Physical security of hosting facility(s)

SEC501-08 References

- Specific sections to reference when investigating:
 - AC-2, AC-2-COV, AC-17, AC-17-COV, AC-20, AC-20-COV, AT-2, AT-3, AT-4, AU-2, AU-3, AU-5, AU-6, CA-3, CA-3-COV, CA-7, CP-9, CP-9-COV, CP-10, IR-1-COV, IR-4, IR-5, IR-5-COV, IR-6, IR-6-COV, MP-1-COV*, MP-2, MP-5, MP-6, MP-6-COV, PE-3, PE-3-COV, PE-6, PE-8, PE-13, PE-14, PS-7, RA-5, RA-5-COV, SA-6, SA-6-COV, SA-9*, SC-3, SC-4*, SC-13, SC-13-COV, SC-28, SI-2-COV, SI-3, SI-3-COV, SI-4, SI-10
- Lots of considerations but several stand out.



MP-1-COV(3)

Prohibit the storage of any Commonwealth data on IT systems that are not under the contractual control of the Commonwealth of Virginia. The owner of the IT System must adhere to the latest Commonwealth of Virginia information security policies and standards as well as the latest Commonwealth of Virginia auditing policies and standards.

SA-9

- The organization:
 - a) Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable laws, directives, policies, regulations, standards, and guidance;
 - b) Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
 - c) Monitors security control compliance by external service providers.



SC-4

- The information system prevents unauthorized and unintended information transfer via shared system resources.
 - Hosted environments often store data for multiple customers on a single physical platform.
 - Can present challenges for logical security or data removal / destruction (SEC514 concern)



3rd Party Hosting

Questions?



ITRM SEC 514 Updates

Bob Baskette

Director, Security Architecture and
Incident Management



ITRM SEC 514 Updates

- SEC 514 requires that all electronic media containing Commonwealth data, whether stored on Commonwealth assets or that of a service provider, shall have all of that Commonwealth data securely removed from the electronic media before the electronic media is surplus, transferred, traded-for, otherwise disposed of, or replaced.



ITRM SEC 514 Updates

- The Commonwealth's Removal of Commonwealth Data from Electronic Media standard (ITRM SEC514) will be updated to address new technologies.
 - Multi-Function devices
 - Solid State Drives
 - Mobile Devices
 - Cloud-based Resources (eGOV Vendors)



ITRM SEC 514 Updates

- Best Practices will be updated to:
 - Ensure that the standard addresses uncommon storage devices that may contain sensitive information so that those devices will be including in the sanitization process.
 - Document a decision tree that can inform agencies as to which sanitization method to use for different types of data classifications.



ITRM SEC 514 Updates

- Best Practices will also be updated to:
 - Provide a thorough sanitization guidance based on device type, data type and disposal method to include reuse, repurpose, and auction at the end of their useful cycles.
- The updated standard should be on OCRA in late January, 2015 for comment.



Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!



Small Agency ISO Program Update

Bob Auton
October 8, 2014



Small Agency ISO Background

At the end of 2013, the Small Agency ISO Program began focusing on the areas of assistance for Small Agencies. At the beginning of 2014, eight potential Small Agencies were selected to assist. The purpose of the program was to assist the selected Small Agencies, who had minimal IT related resources, maintain their information security management program.

The Agencies we have selected to work with are primarily Small Agencies that have approximately 50 employees or less. The Agencies were also not in compliance with a majority of the SEC-501-08 control requirements.



Assistance Provided for Current Year

We have assisted seven Small Agencies in the following areas:

- Updating application information in the Commonwealth Enterprise Technology Repository (CETR),
- Updating the Business Impact Analysis Template, Risk Assessment Template, Risk Treatment Plan Template, Risk Assessment Plan Template, and the IT Security Audit Plan Template,
- Provided detailed examples of information to provide for a typical Business Impact Analysis template,
- Provided access to IT Security Awareness Training for Agency personnel,
- Provided a “Statement of Requirements” for contracting out an Agency’s Business Impact Analysis and a Risk Assessment.



Audit Assistance for Small Agencies

We recently reached out to the Virginia Department of Transportation (VDOT) to use the VDOT IT Audit service contracts in order to provide IT audits services to small Agencies at a more affordable cost.

We contacted approximately 18 small Agencies to identify the Agencies that may be interested in collectively obtaining IT Security Audit services. We had eleven Agencies that provided positive response to our request noting they have approximately 36 systems that require an IT Security Audit.

We plan to use the number of systems needing IT Security Audits as a potential leverage during the contractor negotiations in order to obtain a more favorable pricing for Small Agencies IT Security Audits.



Planned Assistance for Next Year

- ❖ Next year we plan to continue to assist the Agencies we are assisting this year so they may ensure adequate controls are still in place for their information security management program in the future.
- ❖ We also plan to assist seven to eight Agencies, that have approximately less than 50 Agency employees and are having a difficult time maintaining the required controls for their IT Risk Management Program.



Questions

Questions?

You may also send any questions to :
CommonwealthSecurity@VITA.Virginia.Gov



Virginia Information Technologies Agency

Upcoming Events





2015 Security Conference

"COVA Information Security Conference: Unifying the Business Enterprise"

April 2 & 3, 2015

Location: Crowne Plaza

2015 Security Conference



Keynote Speaker

April 2, 2014

Michael Fey

**Chief Technology Officer and General
Manager of Corporate Products for
Intel Security Group**

2015 Security Conference



Keynote Speaker

April 3, 2014

Karen Evans

National Director for the US Cyber Challenge (USCC).



IS Orientation

When: Thursday, December 4, 2014

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1223

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



2014 Official ISACA - CISM and CISA Fall Review Course

ISACA Virginia Chapter is sponsoring a 3-day CISM and CISA Review Course

Dates: October 25, 2014 - from 8:30am to 4:30pm
November 15, 2014 - from 8:30am to 4:30pm
November 22, 2014 - from 8:30am to 4:30pm

Location: University of Richmond
Robins School of Business
BUS wing of the building

Cost: ISACA Members: \$450
Non-members: \$500

***Registration Deadline Wednesday, October 15, 2014 - 5:00 PM**

Register on-line at www.isaca.org/chapters5/Virginia/Pages/default.aspx. Click Events.



Future ISOAG

November 5, 1:00 - 4:00 pm @ CESC

Speaker: TBA

ISOAG meets the 1st Wednesday of each month in 2014



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

8 October, 2014



NORTHROP GRUMMAN



Partnership Q & A

Bob Baskette

8 October, 2014



ADJOURN

THANK YOU FOR ATTENDING

