Virginia Information Technologies Agency

Information Security Officer (ISO)

Appointment Overview

Bob Auton
VITA - Centralized Information Security Services

Mark Martens
Security Risk Management Analyst

Areas for Review

- Commonwealth ISO Certification
- IT Security Policies and Procedures,
- ISO Manual Topics,
- ISO Knowledge Sharing site,
- Security Recurring Task Checklist,
- Role Based Training,
- ISOAG and ISO Orientation,
- Virginia Cyber Security Partnership, …

Areas for Review

ARCHER information for the following:

- Reports to prepare Quarterly Updates for Audit and Risk findings.
- Reports to download Business Processes for Business Impact Analysis, and
- Performing Risk Assessments

Also:

- Products and Services

Obtaining the Commonwealth ISO Certification

Attend Information Security Orientation training, at least once every two years.

Successfully complete at least 3 security courses authorized by the CISO (i.e. Learning Center "ISO Academy").

Possessing a recognized professional IT Security Certification, i.e., CISSP, CISM, CISA, SANS, may substitute for 2 courses.

Attending the mandatory ISOAG meeting, (normally October meeting), as designated by the CISO.

Commonwealth ISO Certification Annual Requirements

- Obtain 20 hours of training in IT security related topics annually (ISOAG meetings may count for up to 3 hours each!) Note: Continuing Profession Education credits (CPE's) for other recognized professional IT Security Certifications may apply to this requirement
  - At least 1 hour of the 20 hours should be authorized by the CISO (i.e. Learning Center "ISO Academy").

- Attend Information Security Officer Orientation (training), at least once every two years.

- Attend mandatory ISOAG meeting (normally October meeting), as designated by the CISO

VITA Policies and Procedures Background

Agencies are required to have (and review annually) policies approved to address all applicable SEC501/SEC525 control families.

Templates for each of the 17 control families are being updated to comply with the current standards.

There are also 15 additional supplemental Policies and Procedures that are available.

Location of the Policies and Procedure Templates

Policies and Procedures are located on VITA's IT Governance's ITRM Policies, Standards and Guidelines site,

- Tools and Templates section

Name - SEC501 Policies and Procedure Templates

Located at the following web address:

http://www.vita.virginia.gov/it-governance/itrm-policies-standards/sec501-p--p-templates/

SEC 501 Required Policies

VITA CSRM - Logical Access Controls Policy
VITA CSRM - Security Awareness and Training Policy
VITA CSRM - IT Security Audit, Monitoring and Logging Policy
VITA CSRM - IT Security Assessment and Authorization Policy
VITA CSRM - IT Configuration Management Policy
VITA CSRM - IT Contingency Planning Policy
VITA CSRM - IT Identification and Authentication Policy
VITA CSRM - IT Incident Response Policy
VITA CSRM - IT System Maintenance Policy
VITA CSRM - IT Media Protection Policy
VITA CSRM - Physical and Environmental Protection Policy
VITA CSRM - IT System Security Planning Policy
VITA CSRM - IT Personnel Security Policy
VITA CSRM - IT Risk Assessment Policy
VITA CSRM - IT System and Services Acquisition Policy
VITA CSRM - IT System and Communications Protection Policy
VITA CSRM - IT System and Information Integrity Policy

Roles & Responsibilities for Policy

ROLES & RESPONSIBILITY MATRIX FOR POLICY COMPONENT SECTION

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe the 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

Roles & Responsibilities Chart

Example ***VITA's Business Impact Analysis Policy Roles & Responsibilities Chart***	Agency Head	Information Security Officer	Agency Continuity Coordinator	Agency Continuity Team	Agency Directors	Data and System Owners
Tasks						
Designate an Agency continuity coordinator		A/R				
Assign members to serve on continuity team					A/R	
Coordinate BIA and continuity plans			A	R		R
Develop a list of all business functions			I		A	R
Create MEF's and PBF's			I		A	R
Determine resources for MEF's and PBF's			I		A	R
Document RTO and RPO for MEF's and PBF's			I		A	R
Produce BIA			A			R
Review BIA on an annual basis			A	R	C	C
Review and approve BIA	A/R	C				

Supplemental Policies and Procedures

VITA CSRM - Business Impact Analysis Policy
VITA CSRM - Disaster Recovery Staffing Policy
VITA CSRM - Emergency Response Damage Assessment Procedure
VITA CSRM - Emergency Response Employee Communications Procedure
VITA CSRM - Enterprise Background Check Policy
VITA CSRM - Information Resource Acceptable Use Policy
VITA CSRM - Information Security Incident Reporting Procedure
VITA CSRM - Information Security Incident Response Procedure
VITA CSRM - Information Security Program Policy
VITA CSRM - Information Security Roles and Responsibilities Policy
VITA CSRM - IT Security Exception and Exemptions Policy
VITA CSRM - IT System and Communications Encryption Policy
VITA CSRM - IT System and Data Classification Policy
VITA CSRM - Mobile Device Access Controls Policy
VITA CSRM - Remote and Wireless Access Controls

Guidance Provided by Supplemental Policies

Example - Information Security Incident Response Procedure:

1. **ATTACHMENT A - Initial Response Checklist**
2. **ATTACHMENT B - Windows Forensics Checklist**
3. **ATTACHMENT C - Unix Forensic Command Log**
4. **ATTACHMENT D - Description of Evidence Form**
5. **ATTACHMENT E - Chain of Custody Form**

ATTACHMENT A - Initial Response Checklist

Contact Information

Your Contact Information

Name:	
Department:	
Telephone:	
Other Telephone:	
Email:	

Individual Reporting Incident

Name:	
Department:	
Telephone:	
Other Telephone:	
Email:	

Incident Detection

Type of Incident:	☐ Denial of Service ☐ Unauthorized Access ☐ Virus ☐ Unauthorized Use of Resources ☐ Hoax ☐ Theft of Intellectual Property ☐ Other:_____ _____ _____ _____

Guidance Provided by Supplemental Policies

Another example is the Information Resource Acceptable Use Policy that has:

1. **ATTACHMENT A - Acknowledgement Of Acceptable Use Of It Resources**
2. **ATTACHMENT B - Information Security Access Agreement**

ATTACHMENT A - ACKNOWLEDGEMENT OF ACCEPTABLE USE OF IT RESOURCES

Acknowledgement Of Acceptable Use Of It Resources

I understand and agree to abide by current and subsequent revisions to the VITA CSRM Information Resource Acceptable Use Policy and the Code of Virginia, Section 2.2-2827.

I understand that VITA has the right to monitor any and all aspects of their computer systems and networks, Internet access, and Email usage and that this information is a matter of public record and subject to inspection by the public and VITA management for all computer equipment provided by VITA. I further understand that users should have no expectation of privacy regarding Internet usage and sites visited or emails sent or received in such circumstances, even if the usage was for purely personal purposes.

My signature below acknowledges receipt of the VITA CSRM Information Resource Acceptable Use Policy.

Accessing the ISO Manual

The ISO Manual is located on the ITRM Policies, Standards and Guidelines webpage, under the Tools and Templates section.

The below is a link to the VITA webpage to access the ISO Manual:

http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs

Helpful ISO Manual Sections

Sections that may be helpful –

1. So You've Just Been Appointed as Your Agency's Information Security Officer (10 Things You Should Do Immediately) – (for example, check the http://www.apa.virginia.gov/APA_Reports/Reports.aspx)

3. How Vulnerability Scanning can change your life and make you feel more secure!

7. Sensitivity Analysis (Without the Help of a Shrink)

10. Information Security Training

13. Disaster Recovery ≠ Continuity of Operations

ISO Knowledge Sharing Site

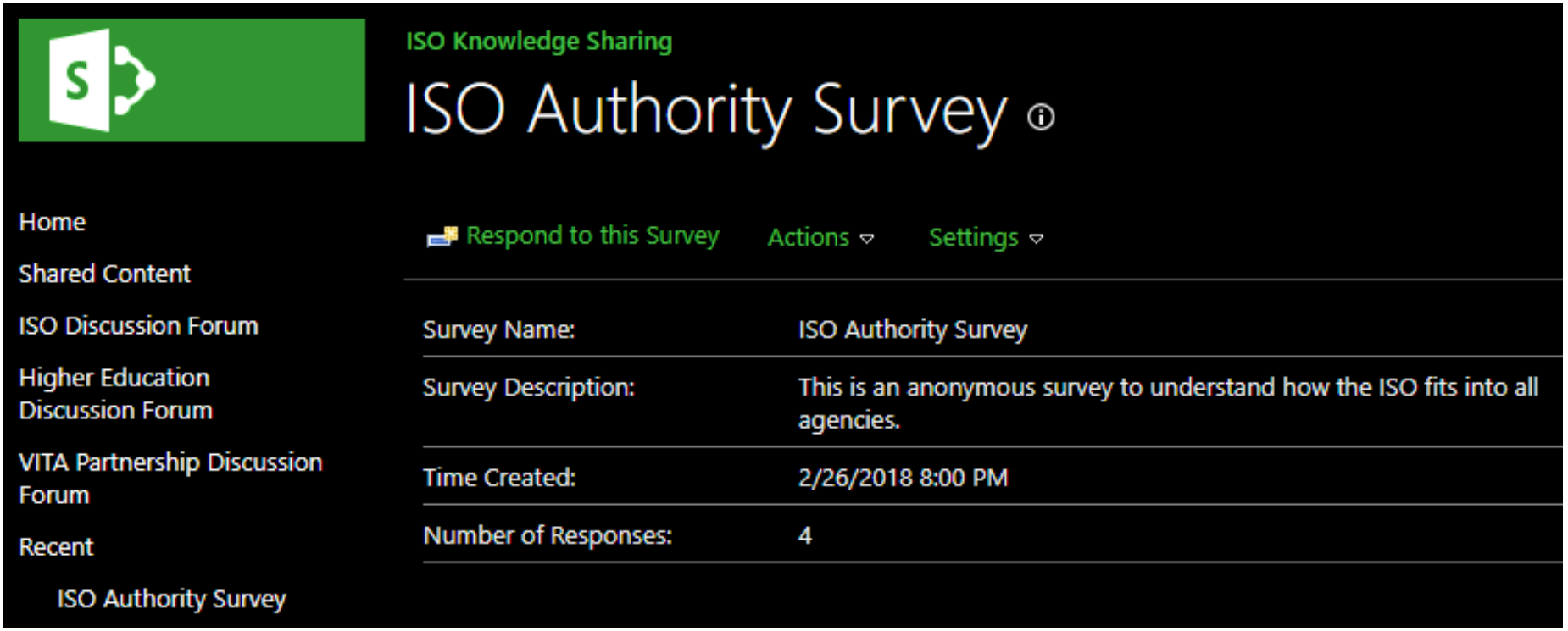
- ISO Knowledge Sharing site is a SharePoint site that provides a place for ISOs to discuss issues they would like to share with other Agency ISOs.

- New users will need to "request access" to the site and are added upon approval.

- The site is located at: https://covgov.sharepoint.com/sites/VITASec/ISOKnowledgeSharing/SitePages/Home.aspx

ISO Knowledge Sharing site

- The below is a screen shot of the ISO Knowledge Sharing site that provides the different areas for the site.



ISO Knowledge Sharing site

- Under the Shared Content Section there are number of topics –

- Archer Training Materials
  - Archer_6_2_Agency_Business_Process_Instructions_2017
  - Archer_6_2_Agency_Application_Input_And_Edit_Instructions_2018
    (Prepared by Mark Martens)

- Helpful Tools
  - SEC50109RolesResponsibilitesMatrix

- Security Templates and Guidance
  - VDH Security Recurring Task Checklist
  - VDH SITSID Template (Detailed System Information Template)

Security Recurring Task Checklists

Tasks Daily

- Provide and verify training of new users and employees
- Provide and verify security role training for any new employees assigned
- Review and document new account requests
- Review and document account removal requests
- Review and approve/deny proposed public-facing content
- Review backup logs for successful completion

Security Recurring Task Checklists

Task Monthly

- Review and approve/deny proposed system changes with the system's Change Control Committee
- Review system audit logs for inappropriate or unusual activity
- Review logs of physical access to system hardware (if applicable)
- Review and resolve system input validation errors
- Test backups of data to verify media reliability and information integrity

Security Recurring Task Checklists

Tasks Every 90 Days

- Change your passwords
- Review data on public areas of the system and remove any non-public data
- Review publicly-facing systems scans for vulnerabilities and submit the required Risk Treatment Plan to Commonwealth Security and verify vulnerabilities found in the prior scan have been remediated
- Verify any vendor-supplied software patches and security updates released in the last 90 days have been applied to the system
- Update Corrective Action Plans for any outstanding IT Audit and Risk Assessment findings and submit to Commonwealth Security

Security Recurring Task Checklists

Tasks Annually

- Review and update the IT Risk Assessment and provide updated report to Management for review.
- Review and update the Business Impact Analysis. Provide management with report on business processes. Provide confirmation of review by entering updates in Archer.
- For users with local administrator rights ensure Agency Head exception approvals are documented annually and include the Agency Head's explicit acceptance of defined residual risks.
- Review and revalidate or remove user accounts and roles/privileges

Security Recurring Task Checklists

Tasks Annually

- Review, reassess, test, and revise the system's
  - IT Disaster Recovery Plan
  - Contingency Plan
  - Incident Response Plan
- Verify completion of annual information security awareness training of all system users
- Review and update system roles for sensitive systems and provide and verify completion of annual system-specific role-based security training for personnel with assigned security roles

Role Based Training

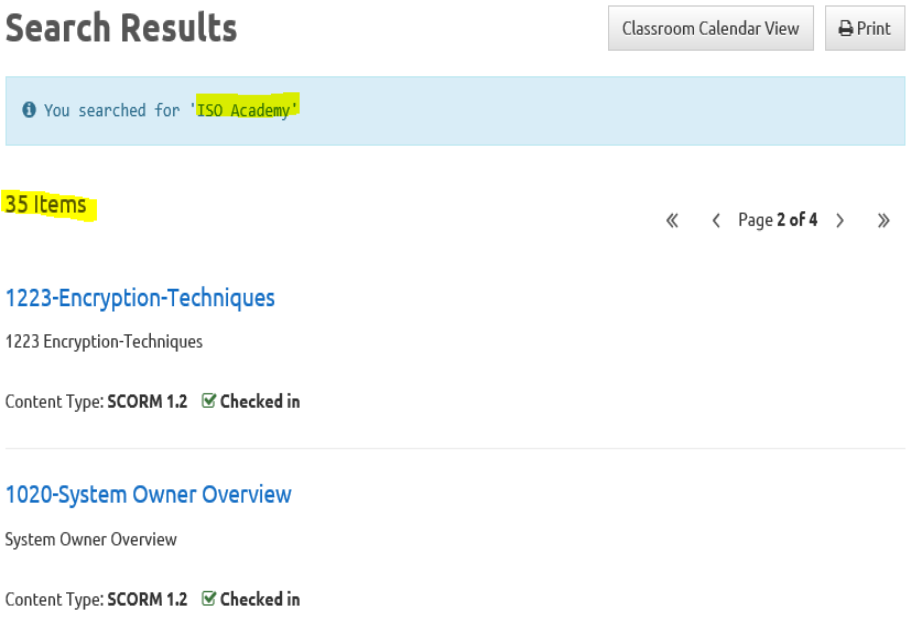
ISO Academy classes for role based training

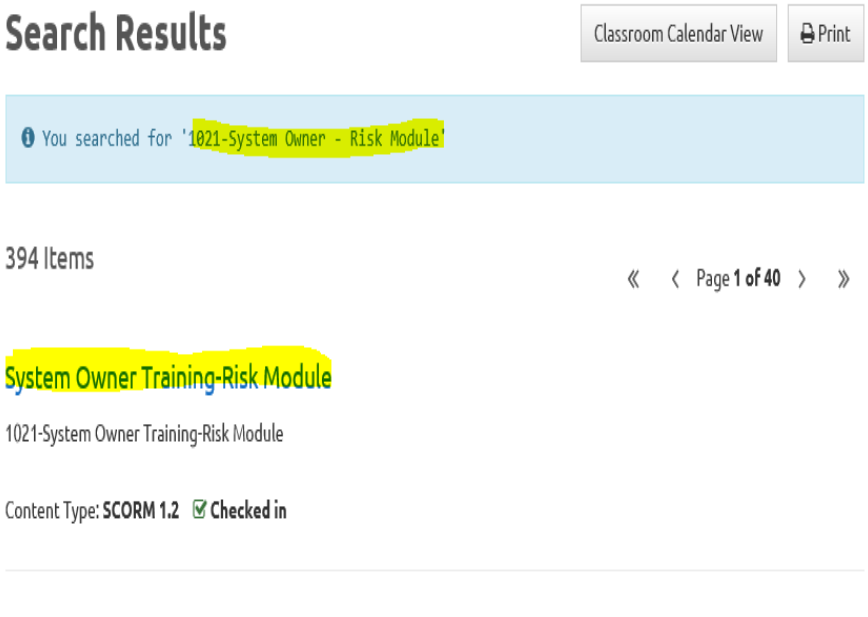
- 2.6 Privacy Officer - 1224-10 Immutable Laws of Security
- 2.7 System Owner - 1020-System Owner Overview
  1021-System Owner - Risk Module
- 2.8 Data Owner - 1025-Sensitivity Analysis
  1062-Data Protection
- 2.9 System Administrator - 1043-IT System Hardening
  1042-System Security Planning
- 2.10 Data Custodian - 1052-Logical Access Account Mgmt
  1062-Data Protection

Role Based Training

Accessing ISO Academy Classes

- Commonwealth of Virginia Learning Center – COVLC
- Search Phrase for classes – "ISO Academy" or "Class Name"
- Learning Center Information: DOMAIN where ISO Classes are located - VITA Learning Center – Agency -136





Information Security Officers Advisory Group

- Information Security Officers Advisory Group (ISOAG) meetings are held monthly at CESC or via web-meeting.
- Attendees include COV or local government employees.
- ISOAG Meeting Reminder emails are sent monthly to register for the upcoming month's meeting.
- Also there may be a Knowledge Sharing Luncheon before the meeting where you can join other ISOs and Auditors for lunch before the ISOAG meeting to discuss current challenges facing your agency.

Information Security Officers Advisory Group

- Prior ISOAG Meetings presentation can be viewed on the VITA website at the following link:
- http://www.vita.virginia.gov/commonwealth-security/isoag-meetings/

- To be added to the email ISOAG distribution list for attendance at the meeting please send an e-mail request to:

CommonwealthSecurity@VITA.Virginia.Gov

Remember to check the CPE box when you register!

IS Orientation Sessions

- IS Orientation classes are presented quarterly throughout the year.
- Commonwealth Agency ISOs are required to attend orientation at least once every two years to maintain their COV ISO certification.
- The classes are open to all COV state or local government employees interested in information security.
- Sessions in 2019 will focus on using Archer to meet Commonwealth Security compliance requirements.
- To be added to the email distribution list please send an e-mail request to:

  CommonwealthSecurity@VITA.Virginia.Gov

Virginia Cyber Security Partnership

- The Virginia Cyber Security Partnership (VCSP) is a non-profit organization of cyber security professionals. It was established in 2012, as a collaboration between the private and public sectors to create a trusted place to collectively discuss Cyber threats.

- New users can apply on line and will receive a Membership Account once their application is approved.

- How to Join - https://vacsp.com/membership/

Virginia Cyber Security Partnership

- VCSP site includes a Resource Calendar that provides information on upcoming local IT Security events.
  Example of April, 2019 Events:
  - Cybersecurity Career Discussion Panel - April 2 @ 5:30 pm - 7:30 pm EDT
  - *2019 Commonwealth of Virginia Information Security Conference - April 11 - April 12*
  - ISACA Richmond: Information System Audit Topics with Stephen Weber - April 25 @ 11:30 am - 1:00 pm EDT

Virginia Cyber Security Partnership

- The website has a page devoted to News-

VCSP Member Dan Han Featured On SANS

Archer Demonstration

- Reports to prepare Quarterly Updates for Audit and Risk findings,
- Reports to download Business Processes for Business Impact Analysis,
- Performing Risk Assessments, and
- Products and Services.

Quarterly Update Templates

- https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/docs/Audit-Remediation-Plan-Template-12_28_18.xlsm
- https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/docs/Risk-Treatment-Plan-Template-12_28_18.xlsm
- Archer Report
- COV: Quarterly Update Report

BIA Update

- https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/docs/BIA_Spreadsheet_Template.xlsx
- Archer Report:
- COV: Complete Business Impact Analysis

Risk Assessments in Archer!

- CSRM Risk Assessments are in Beta and currently only being used by ISO services
- CSRM Analysts must create the record to get you started
- All 17 domains are covered by questions with “yes” “no” answers

Products and Services

- Security Program information for Service Towers is contained in Archer under Business Infrastructure / Products and Services.
- SSPs are under Attachments
- G Suite and Help Desk currently have SSPs that can be viewed along with Findings and data classification inventory information (PII, PHI, FTI, etc)

More to come..

- More Enterprise Applications that your agencies utilize will appear under this section of Archer as these tools are rolled into production.

Questions

Bob Auton
Robert.Auton@VITA.Virginia.gov

Mark Martens
Mark.Martens@VITA.Virginia.gov