ISO Manual

An Information Security Officer's Guide

2013 - COV IS Council
ISO Manual Committee

Table of Contents

ISO Manual Background Information

The ISO Manual was identified in 2012 by the Information Security Council Members as a project for calendar year 2013. The ISO Manual Committee Members and the Co-Chairs who prepared sections and also reviewed sections for the ISO Manual are:

Karen Ashby, Dept. for Aging and Rehabilitative Services,

Cherrey Wallace, Dept. of Corrections,

Theresa Fleming, Dept. of Medical Assistance Services,

Melanie Seigler, Dept. of Forestry,

Deborah Edwards, Dept of Treasury,

Bob Haugh, Co-Chair, Dept. of Emergency Management, and

Bob Auton, Co-Chair, Dept. of Juvenile Justice\VITA

The ISO Manual Committee Members would also like to acknowledge the many areas of assistance that was provided by the Commonwealth Security and Risk Management support personnel, Bill Freda.

Introduction

If you're an Information Security (IS) professional, with a wall full of certificates listing all manner of acronyms, you're likely pleased with your new appointment as an agency 's Information Security Officer (ISO); but if this is your first ISO assignment, you're likely feeling more than a little intimidated. The purpose of this manual is to assist both the experienced IS professional and the lucky staffer who has been assigned ISO responsibilities for the first time.

The ISO Manual Committee of the Commonwealth's Information Security Advisory Council has prepared this manual to provide an informative, functional and authoritative, yet light-hearted guide to the Commonwealth's IS policies and standards. Our objective is to make what can be an intimidating set of responsibilities less intimidating for a newly appointed ISO, especially one who has no prior experience or extensive training and experience.

1. So You've Just Been Appointed as Your Agency 's Information Security Officer (10 Things You Should Do Immediately)

Following are ten activities that we recommend you should undertake immediately upon being notified that you've been appointed the agency ISO. These activities are described at a high level and many are addressed in greater detail in the various sections of the manual. We will provide the section information if appropriate for the activity. While we propose a logical order to accomplishing these tasks, circumstances may dictate a different approach.

A. Your Appointment (with destiny)
Lawyers, doctors and other professionals will tell you that, "if it's not written down, it didn't happen." That's the case with ISO appointments, as well. The Commonwealth Information Security Standard, a.k.a SEC-501, requires that the ISO must be appointed, in writing, by the agency head, but the "writing" can be electronic, that is, in the form of an email. If you received your appointment as a hard copy document, send a copy to the Commonwealth Security email address:

CommonwealthSecurity@vita.virginia.gov

If you received your appointment as an email, ensure that Commonwealth Security received a copy, or forward it yourself.

You should also put a tickler on your calendar 23 months from the date of your appointment. ISO appointments are valid for two years, so that tickler should remind you to remind your agency head about the renewal. Commonwealth Security will send you a friendly reminder, but it would be helpful to keep on top of that renewal yourself. This requirement is included in Appendix J which has a timetable listing of a majority of the additional SEC-501 requirements.

B. Establish a strong relationship with your agency head.
Some might argue that the very fact that you've been appointed as the ISO is testament that you've offended the agency head. Commonwealth Security prefers to think that the agency head has identified you as worthy of special trust and confidence to handle this very important responsibility.

Ultimately, the agency head is responsible for the Information Security Program (like most everything else that happens in the Agency .) SEC-501 assigns the ISO a significant number of responsibilities, but they're all performed under the agency head's authority. Successful ISOs have found it helpful to set up a standing appointment on their agency head's calendar, monthly at a minimum, more frequently in the larger agencies or where the information security program requires greater attention from the agency head.

There are a number of topics that should be brought to the agency head's attention periodically; including the status of information security audits and the resolution of any audit findings; pending requests for exception to the provisions of SEC-501, including new exceptions that need to be submitted, exceptions that are about to expire and need to be renewed; and security-related incidents. Other topics could include major new software developments, major modifications to extant applications and the annual security awareness update training.

The active involvement of the agency head is one of the keys to the success of an agency 's information security program. Give your agency head bullet points to mention when he/she speaks with senior manager or the staff at large.

C. Attend the ISO Orientation.

Commonwealth Security presents the ISO Orientation at least quarterly. The class lasts about 2 hours and provides a broad overview to the Commonwealth's Information Security program. It is usually conducted at VITA's headquarters and has, in the past, been presented via webinar. Attending in person is an excellent way to meet fellow ISOs and commiserate about your appointment and agency's information security program.

Initial completion of the orientation and the biennial repeat are requirements for the ISO Certification process which is a criteria reported by Commonwealth Security in the Annual Information Security Report to the Governor. Plan to attend as soon as you learn that you're going to be appointed and put a tickler on your calendar a month or two before your ISO appointment is due for renewal, so you can repeat the course and stay in compliance with SEC-501. The following is the link to register for the ISO Orientation: http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

D. Review the agency's information systems architectures.

The agency IT Director should maintain a set of diagrams that depict the agency's information architecture. This includes the hardware infrastructure (networks, servers and such) and the software applications that the agency uses and where those applications and their data reside. Developing an understanding of the relationships between the hardware and software assets that the agency uses is an excellent place to start your orientation to your responsibilities as the ISO. Look for the points where data enter and leave the agency and how it moves between applications and servers. Identify where data are "in use" in the agency, where data is "at rest," and how data "in motion" flow through the agency. Section 8. Sensitive IT System Inventory and Definition and Appendix F: IT System and Inventory and Definition Document have more in-depth information related to this activity.

E. Review the System Inventory and Data Sensitivity Analysis.
From the BIA, the ISO should distill a list of systems that are in use in the agency. Ensure that this inventory stays up to date, adding new applications as they are implemented in the agency and deleting those that are no longer in use.

Each information system in use in the agency should be analyzed for sensitivity in three areas; confidentiality, integrity and availability. According to SEC-501, Confidentiality refers to the system's/data's sensitivity to unauthorized disclosure; Integrity refers to sensitivity to unauthorized modification; and availability refers to sensitivity to outages. Keep in mind that "sensitive data is any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled." Working with the system owners and data owners, the ISO performs this analysis and documents its findings. SEC-501 allows the ISO to define the terms "low," "medium" and "high" relative to these criteria, a helpful guide has been included as an appendix to this section. Any system assessed as "high" in any one of the criteria categorizes the system as "sensitive" and subjects it to additional controls and audit requirements. There is additional information on sensitive systems in section seven of this manual.

The ISO, system owners and data owners should pay special attention to systems that have external regulations and requirements related to confidentiality, integrity or availability; for example, the Health Insurance Portability and Accountability Act. We have also provided an example of the Commonwealth Security template, IT System and Inventory and Definition Document in Appendix F of this manual.

F. Review the agency's Business Impact Analysis (BIA).
The BIA should identify the agency's Mission Essential Functions (MEF) and the Primary Business Functions (PBF). The BIA should be updated as changes in agency missions, functions and information systems occur. Each agency ISO shall submit the results of the review and revision of the agency BIA annually to Commonwealth Security and Risk Management. We have also provided more information for preparing and maintain an agency's BIA is located in section eight of this manual.

When looking at your agency's BIA, also review the Commonwealth Enterprise Technical Repository (CETR). The agency's information technology team should be maintaining this listing of systems and databases. The ISO should ensure that all of the systems listed in CETR are also listed in the BIA and should report any discrepancies to the agency's IT Director. Together, they should decide whether an update is required to CETR, the BIA or both. Comparing the systems listed in the BIA and CETR is one of the ways that Commonwealth Security evaluates the BIA. You can get to your CETR information as identified at the end of section 15 of this manual.

G. Meet the System and Data Owners.
The system owner is generally the manager responsible for the business function that a system supports. With the possible exception of a system used to monitor or ensure compliance with information security requirements, the ISO should not be the system owner for any agency system. The system owner established the policies and procedures for system operation; including topics like security, training and other procedures. The system owner also appoints the data owner (or performs that duty himself/herself) and appoints system administrators. A system owner can be responsible for multiple systems, as can a data owner.

The ISO will find it valuable to meet with the system owners and data owners to discuss any security concerns surrounding sensitive data, Continuity of Operations and Disaster Recovery. Several activities recommended in this "top ten" will require interaction with system owners and data owners. In addition, establishing a relationship with the user community will also be beneficial before a security incident occurs.

H. Review the System Risk Assessments.
Systems identified as sensitive require further analysis regarding the risks facing them. The risk assessment should establish the following:

- Potential threats to the system, its data and the environment in which it operates;
- The likelihood that one of these threats may materialize;
- The vulnerabilities that these threats and their likelihood of occurrence present to the agency; and
- The impact that the agency would experience if one or more of the vulnerabilities are exploited.

A full risk assessment must be performed at a minimum every three years, but annually a risk assessment plan is required to add new systems, risks or vulnerabilities and remove systems that are no longer in use. The risk assessment plan shall be based on the Business Impact Analysis (BIA) and data sensitivity classification performed by the agency. Each agency head shall submit the agency risk assessment plan to the CISO, annually.

The system risk assessment should include actions taken to remediate the risk. There are generally controls (safeguards and/or countermeasures) applied to the systems. SEC-501 includes an exhaustive list of controls that Commonwealth Security recommends. A system that has a "high" sensitivity rating should employ additional controls to provide "defense in depth." There is more detailed documentation for the risk assessment in section nine of this manual.

I. Review Information Security Audit Reports.
One of the fastest ways to assess the status of an agency's information security program is to review audit reports. Each sensitive information system is required to be audited every three years. In addition, the Auditor of Public Accounts (APA) frequently assesses an agency's information security program as part of their annual or biennial agency audits. Larger agencies and those with special requirements have internal audit units that may also look at the security of individual systems and the information security program at large.

In addition these entities may look at other agency-wide programs that are also components of the agency's information security program. For example, they may look at the agency's Business Impact Analysis (BIA), Continuity of Operations Plan (COOP), and/or IT Disaster Recovery Plan.

Examine the audit reports for an assessment of where the agency stands with respect to these plans and programs. In addition to the findings, pay attention to the methodology that the auditors used to evaluate those programs and the positive feedback that the auditors provided the agency. Naturally, you'll also want to look at the Correction Action Plan (CAP) to determine what has been done to correct the findings and because the odds are that you'll be involved in any corrective actions that haven't yet been completed.

The audit reports will also give you an idea of what wasn't covered in the audits. This will help direct your further investigation into the status of the agency's security program and may help you uncover some hidden or previously unexplored problems.

While most managers run and hide from auditors, befriending an auditor might pay dividends, especially internal agency auditors as noted in section 15 of this manual. They have a unique opportunity to see how the agency and its programs operate at a high level, provide perspective on the interrelationships between agency programs and can help identify potential shortfalls in the agency's information security program.

J. Review the agency's Continuity of Operations (COOP) and Disaster Recovery plans.
The agency is required to have a Continuity of Operations (COOP) plan that describes how it will continue to function if a disaster occurs that makes its facilities become unusable. It is also required to have an IT Disaster Recovery plan to describe the reactivation and recovery of information systems, should they be damaged or become unusable. These are, or should be, separate plans and there is frequently confusion about them, because the titles are used interchangeably.

The COOP plan, which should be based on the BIA, focuses on the business operations of the agency. It may include references to information technology, because computers and networks are key operational tools. The COOP plan is usually (but not always) based on the loss of a physical facility by fire, flood or some similar reason.

The agency head is required to appoint an Emergency Coordination Office (ECO) who is responsible for the development of the COOP plan. In some cases, the agency head appoints him/her to this role. In other cases, the person responsible for "facilities" is given this additional responsibility. The COOP Plan must be updated annually. The ISO should determine who has responsibility for the plan and obtain a copy of the most recent version.

The IT Disaster Recovery plan is usually the responsibility of the agency 's IT director. It focuses on the catastrophic loss of systems (as opposed to operations) and the processes and procedures to bring those systems back online and restore their functionality. The IT Disaster Recovery plan should identify the sequence of system restoration, the time that it should take to return those systems to operation (Recovery Time Objective) and the amount of data that the agency can afford to have to recreate (Recovery Point Objective). The IT Disaster Recovery plan should also identify the regimen of system backups that are performed, including the location of the media used for backups and how the backed-up applications and data are returned to the data center and restored.

In becoming conversant with the BIA, COOP and Disaster Recovery plans, the ISO should compare them to ensure that systems identified the BIA are also covered by the COOP and Disaster Recovery Plans. Any discrepancy should be brought to the attention of the agency head, ECO and IT Director.

A new ISO may encounter some resistance to requests for these documents, but they are within the portfolio of your responsibilities and you should insist on the opportunity to review them.

Using the Manual

The remaining sections in this manual provide greater detail on many of the above subjects. The manual is designed to be read topically, but users may read it from cover-to-cover, if they so choose. Remember that the Commonwealth Information Security Standard, SEC-501, is the authoritative source for the direction on the agency's information security program.

2. What is the Commonwealth's Information Security Governance Structure?

In general, the commonwealth has designated the Virginia Information Technologies Agency (VITA) as the oversight agency for consolidated, centralized information technology including, but not limited to: documenting and providing information security program requirements, operation of the commonwealth's IT infrastructure, related personnel, for the executive branch agencies (in-scope), support of the Information Technology Advisory Council (ITAC) and the Chief Information Officer for the Commonwealth; and, procurement technology. For more information regarding these, see the latest SEC519 ITRM Information Security Policy, ITRM Standard SEC520 Information Technology Risk Management Standard and SEC501 ITRM Information Security Standard found on VITA's website at the following link: http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs

We can also utilize some applicable COBIT Five principles regarding information security governance structure:

1. Meeting stakeholder needs
2. Covering the enterprise end-to-end
3. Single integrated framework
4. Holistic approach
5. Separating governance from management

By utilizing these principles, this allows the optimization of information and technology. We have also provided an example of a RACI model that by definition is a model used to help define who is responsible or accountable for a variety of IT services. Please refer to Appendix A for the RACI example.

This provides for each individual ISO, being responsible to leverage the best possible support, security policy and presence, for their respective agency overall, by complying with VITA's governance, these individual ISOs represent collectively, a centralized security effort to protect the commonwealth. We have provided the Commonwealth of Virginia Information Security Program Framework in Appendix B of the ISO Manual.

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

We have just gotten a wake-up call from the Nintendo Generation (Hackers 1995)

It's a scary world out there. We should be constantly looking for IT security weaknesses and comparing them against prominent threats to obtain our risk. But you can't stop there. You have to reduce the risk by fixing the vulnerabilities. How you ask?

What about completing a security audit? Security audits, which imply a (hopefully) rigorous check against a list of security controls. A checklist comprised from controls from security control documents such as SEC-501 or NIST 800-53 might be a great start for this. You might also do a security assessment, which could include a review of policies and procedures along with some technical scanning of the environment.

Let's get a little more techie. A vulnerability assessment can be conducted in many forms including network, desktop, and wireless, application, and web application. And on top of all that, we have the granddaddy of evaluating our security posture. . . the mighty penetration test. This, too, can be focused on different areas, such as wireless, network, or web application. It can be open book or closed book, white box or black box, whatever you want to call it. That means you decide how much information (diagrams, credentials, etc.) you want to give your testers. Typically, the more information you provide, the cheaper it is since they don't have to do as much work to own your box (or not!! Yay!!). Don't be too discouraged if they get root access. Better the tester gets in than the bad guy.

Software isn't an install it and forget it deal. You need to know where your holes are – how the enemy can exploit you. To find out, all equipment, servers, desktops, networking equipment and appliances should be periodically scanned to determine the current status of the firmware and software. It's required by SEC-501 for a reason: it drives vulnerability patching.

Over time, vulnerabilities and bugs are discovered by the manufacturer or the public for the operating system and enterprise and desktop applications as well. The manufacturer will often create a software update or patch to address these vulnerabilities (note to self: It takes a while for patches/updates to come out, so I may want to think of some compensating controls in the meantime).

Depending on the setting and capabilities of the scanner, we can be alerted to other vulnerabilities such as open ports and unnecessary services. Tighten that up as much as your business processes allow.

The good news for those included in the partnership is that this type of vulnerability scanning is included in the service fee you're already paying. However, it's your responsibility to review the reports. Check them out periodically on the PSO website.

But don't stop there! You need to scan your web applications too! Web technologies are getting more sophisticated, often include application servers, two and three tier configurations, and frequently serve up data from a back end database.

If your Web pages are static and don't contain any sensitive information, they are a fairly low risk. However, many agencies now have dynamic websites. These involve data input and/or pages that generate unique content each time they're loaded. Put this together with today's Web vulnerabilities and sensitive citizen, financial data or critical infrastructure information, and your risk increases exponentially.

This is typically focused on public facing Web-based applications, but it could easily apply to internal browser based applications with sensitive data serving trusted users. These are really intranet websites and should be evaluated as well. We need to protect ourselves from us too!

This type of security assessment looks for common Web-based vulnerabilities using both automated and manual scanning techniques. For a list of the top ten vulnerabilities, an excellent site to check out is OWASP (www.owasp.org). Each year, the Open Web Application Security Project puts out the top ten web vulnerabilities to let you know how hackers are getting to your data. The crazy thing is some of the vulnerabilities are the same year after year, but organizations still aren't fixing their websites. Lesson? Know what is out there.

While this type of testing is not part of the basic partnership scanning service, it is still required by SEC-501. Any state entity can obtain Web application scanning services from Commonwealth Security or external providers.

Last, but not least, is penetration testing. The NG security team performs a network penetration test, which can include any agency, but usually includes the larger agencies and covers a wide scope of things over a few months each year. This process includes a recon phase (let your agency staff know that Facebook and LinkedIn and many other sites are considered attack fuel by Pen testers), a mapping and discovery phase, an exploitation phase and a reporting phase.

The scope can include wireless networking and application security as well as the network. Testers not only find the vulnerabilities, they try to exploit them to see what the evil doers can do. While we can limit what the penetration testers find by implementing a robust OS, application, Web application and wireless network scanning a good penetration test will uncover some vulnerabilities or weakness. If client side testing is allowed, testers are virtually guaranteed a successful attack. Pen testing is not required by SEC-501, but is required by the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability Accountability Act (HIPAA) which may apply to your agency. It's something that is really worth looking in to.

Bottom line – Getting unauthorized access to confidential data has gone from simple bragging rights to big money. Help your agency minimize its attack surface area before it's too late. It's not if you get compromised, it's when.

P.S. If you're an ISO for an out-of-scope entity, pay attention to what the partnership is doing regarding vulnerability testing. If they're doing something specific, chances are you should be doing it, too.

4. The agency's Information Security Program (The View From 50,000 Feet)

The IT security program is designed to minimize the risk for your systems that contain sensitive data. We wanted this section to give you a means to navigate the IT security program at a high level. Appendix B also has a flowchart that will help you visualize the process to implement an IT security program. This section is a narrative that will help explain some of the IT security program processes which are:

- Documenting the Business Impact Analysis (BIA).
- Identifying sensitive systems.
- Formulating the risk assessment.
- Preparing an IT security audit plan.
- Performing IT security audits.
- Submitting Correction Action Plans (CAPS).

The starting point for the Information Security Program is documenting your Business Impact Analysis (BIA). The information to help you prepare your BIA is in Section six of this manual. The good thing about the BIA is you will be able to work with other members of your agency in order to provide the necessary information for the assessment. Conduct periodic review and revision of your agency's BIAs, as needed, but at least once every three years. Now that you have your BIA documented you will want to identify your sensitive data and systems.

Section seven of this manual provides the information that will help enable you to identify your sensitive data. Once you have identified your sensitive data you will want to reconcile the information with the data in the reporting database the Commonwealth Enterprise Technology Repository (CETR). You can get to your CETR as identified in section 15 of this manual.

Now that you have completed your BIA and know which systems are sensitive you will want to prepare your Risk Assessment (RA). The RA can provide you with a variety of information that can help you to identify controls to put in place to minimize the risks you have identified in the assessment. This process should be conducted at a minimum of once every three years or whenever there are changes in the system to warrant an update. The information to help you prepare your RA is identified in section nine of this manual.

The information from your RA will help your prepare your IT Security Audit Plan. The template for the IT Security Audit Plan can be found at the following link:

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

You can use the Word or an Excel format that is located in the section named "Tools and Templates" on the VITA website. Using your RA you can identify your highly risky systems to schedule the audits. You will need to ensure that you schedule your sensitive systems audits to be completed in a minimum of once every three years. Using the audit plan template will be helpful since it is set up to list your audits over a three year time frame.

The next key component is identified at the conclusion of your IT security audit. You may have provided adequate controls to the system being audited so as not to have any audit findings for your sensitive system. In this case you would want to continue to assess you systems by performing your BIA and RA to ensure you are have identified ongoing and potential new risks. However, if your audit has identified findings you will want to prepare a corrective action plan to remediate the control weaknesses that were documented. There is a Corrective Action Plan template in Word or Excel that can be found at the following VITA link:

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

The Corrective Action Plan template helps organize the information that will enable you to provide a corrective action for the weaknesses identified in the audit. Filling out the template during your audit process can also save you time after the audit when you submit the CAP to Commonwealth Security. You will also want to notify Commonwealth Security if there are no audit findings related to the IT security audit.

Continuous monitoring of your sensitive systems by completing the above noted assessments and audits will enable you to provide an IT security program that will minimize the probability that identified risks will impede system data confidentiality, integrity or availability.

5. The Supporting Cast - Security Roles and Responsibilities

Who (or what) is a System Owner and what do they do?

The system owner is the agency business manager responsible for having an IT system operated and maintained. With respect to IT security, the system owner's responsibilities include the following:

1. Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
2. Manage system risk and developing any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
3. Maintain compliance with COV Information Security policies and standards in all IT system activities.
4. Maintain compliance with requirements specified by data owners for the handling of data processed by the system.
5. Designate a system administrator for the system.

Who (or what) is a Data Owner and what do they do?

The data owner is the agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following:

1. Evaluate and classify sensitivity of the data.
2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
3. Communicate data protection requirements to the system owner.
4. Define requirements for access to the data.

What is the role of the Commonwealth's Information Security Officer?

The Commonwealth's Information Security Officer (CISO) role includes defining and administering the COV Information Security Program, including policies and standards. The CISO is also responsible for the administering the COV Information Security Program and periodically assesses whether the program is implemented in accordance with COV Information Security policies and standards.

The CISO establishes agency information security program requirements with agency service providers, reviews exception requests to COV policy, and provides guidance and expertise in IT security. The CISO also collects data relative to the state of IT security within the commonwealth that is reported to the Governor on an annual basis.

The CISO facilitates effective implementation of the COV Information Security Program, by:

a. Preparing, disseminating, and maintaining information security, policies, standards, guidelines and procedures as appropriate;

b. Collecting data relative to the state of IT security in the COV and communicating as needed;

c. Providing consultation on balancing an effective information security program with business needs.

The CISO also provides networking and liaison opportunities to Information Security Officers (ISOs) such as the monthly Information Security Officer's Advisory Group (ISOAG) meeting. To register for the monthly ISOAG meetings send a request to Commonwealth Security and request to be added to the ISOAG e-mail list. To register for the monthly ISOAG meeting please use the following:

http://vita2.virginia.gov/registration/

We have also provided other roles and responsibilities in the supporting cast in Appendix C of this manual that will help provide information on who to turn to when issues regarding the system arises. We have also included in Appendix C an Account Approval Quick Reference Guide that provides the approval areas for the user's manager, ISO, AITR Authorized Approver and Commonwealth Security and Risk Management.

6. Business Impact Analysis (Or Finding Out What Your Agency Really Does)

What is a Business Impact Analysis?

1. The Business Process Analysis (BIA) delineates the steps necessary for agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions and the primary business functions.

2. The ITRM Standard SEC520 Information Technology Risk Management Standard and SEC-501 ITRM Information Security Standard provides guidance on the requirements that address the IT and data aspects of a BIA. The standard does not require agencies to develop a BIA separate from the BIA that could be used to develop an agency's COOP plan (previously referred to as Continuity of Operations Plan). Agencies should create a single BIA that meets both the requirements of the standard and can also be used to develop the agency continuity plan.

3. This can be a time savings if a BIA is developed to address agency's continuity plan as required by Virginia Department of Emergency Management (VDEM) as well as the requirements identified by the standard. One thing to be aware of is in the VDEM's guidelines the Business Impact Analysis (BIA) is identified as the Business Process Analysis (BPA).

4. The following is the link to VDEM's State Continuity Planning Resources website: http://www.vaemergency.gov/em-community/plans/coop

   i. The below are the templates that are provided on VDEM's website:
      1. VDEM Continuity Plan template
      2. VDEM Guide to Identifying Mission Essential Functions
      3. Mission Essential Function Identification worksheets

   ii. Of course to get the full benefit of the templates they should be prepared in the following sequence:

      1. VDEM Guide to Identifying Mission Essential Functions
      2. Mission Essential Function Identification Worksheets
      3. VDEM Continuity Plan Template

Now the real fun begins - providing information for your agency's business functions. You will want to schedule time with the key personnel in the functional areas identified in the mission essential functions and in the primary business function areas. The process owners will need to provide some of the critical information regarding the BIA.

One of the key areas that relates to the BIA in the VDEM Continuity Plan Template is the Appendix D – Business Process Analysis. Preparing the information for the business process analysis will be helpful in identifying the necessary information and how the processes relate to your IT systems. We have also provided a template in Appendix D of this manual that will help provide the necessary information for your agency's business functions.

Each agency ISO shall submit the results of the review and revision of the agency BIA annually to Commonwealth Security and Risk Management. An online template will be provided to capture the required information that will need to be provided annually. The following data will be needed to be provided annually:

- Document the required Recovery Time Objective (RTO) based on agency and COV goals, objectives, and MEFs, as outlined in the agency continuity plan.
- Document the Recovery Point Objectives (RPO) as outlined in the agency continuity plan. For each MEF and PBF, the BIA should identify the following:

- Business function name.
- Business function owner.
- Date BIA completed.
- Person completing the BIA.
- Primary objective of the business function.
- Business function internal customers, commonwealth agency customers, government entity customers, public customers and other types of customers, for example vendors.
- Description of the data used as input to the business function.

- The source of the data used by the function, internal, external or external and internal to the agency.
- The destination of the data provided by the function, internal, external or external and internal to the agency.
- The internal agency IT systems required by the function.
- The external agency IT systems required by the function.
- Identify Mission Essential Functions (MEFs).
- Indicate whether the business function uses sensitive data.

You will want to ensure that all of your systems identified in CETR (check out the end of section 16 for information on CETR) are also associated with a mission essential function or a primary business function that is identified in your BIA.

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

Data protection is the effort of determining whether or not data requires security safeguards when processing and storing data. There are defined methods outlined in SEC519-00 ITRM Information Security Policy, Section 2.2.5 Data Protection. See the latest of this policy, on the VITA website.

As part of data protection, it is important to determine the data sensitivity classification levels applicable to the type of data processed and stored. Sensitive data is any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled.

Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to confidentiality, integrity and/or availability. Agencies must classify each IT system by sensitivity according to the most sensitive data that the IT system stores, processes, or transmits. For more information, see the latest version of SEC-501 ITRM Information Security Standard, which includes a section on IT System and Data Sensitivity Classification.

IT System and Data Sensitivity Classification requirements include:

- Confidentiality: addresses sensitivity to unauthorized disclosure
- Integrity: addresses sensitivity to unauthorized modification
- Availability: addresses sensitivity to outages.

In order to start the process of data sensitivity classification, the agency ISO will:

a. Have the data owner identify the types of data within each IT system.
b. Have the data owner determine if the data is subject to any regulatory requirements.

> **Example:** Some IT systems may handle data subject to legal or business requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); IRS Publication 1075; the Privacy Act of 1974; Payment Card Industry (PCI); the Rehabilitation Act of 1973; or § 508, Federal National Security Standards, etc.

c. Have the data owner determine the potential damages to the agency if a compromise of confidentiality, integrity or availability of data handled by an IT system, and classify the data sensitivity accordingly.

Example: Data owners may construct a table similar to the following table. Data owners must classify sensitivity requirements of all types of data. The following table is only an illustration of one way to accomplish this.

System ID: ABC123	Sensitivity Criteria		
Type of Data	**Confidentiality**	**Integrity**	**Availability**
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Juvenile Criminal Records	High	High	High

Table 1: Sample Sensitivity Analysis Results

For data classification, example below (lifted out of VITA SEC-501 Security Standard):

System name:	Sensitivity Criteria		
Type of Data	**Confidentiality**	**Integrity**	**Availability**
HR Policies	Low	High	Moderate
Public Information	Low	Low	Low
Personnel Records	High	High	High
Agency Confidential	High	High	Moderate
Privacy Records (HIPAA)	High	High	Moderate
Medical Records, PHI (HIPAA)	High	High	High

Note: For example, agency classifies applications or data as **sensitive** even if a *type* of data handled by an IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability. Certain applications housed within an IT system are considered "sensitive," even if their classification is low, due to the "confidentiality" of the material.

1. Data classifications are to be reviewed and documented for the defined classifications.
2. Confirm that all agency IT systems and data have been reviewed and classified appropriately for sensitivity.
3. Communicate approved IT system and data classifications appropriately.
4. Prohibit posting any agency data classified as sensitive with respect to confidentiality on a public website, FTP server, or any other publicly accessible platform.

5. Use the information documented in the sensitivity classification as a primary input to the information system security plans for each IT system, RA processes, and agency IT security audit plans.

There is a table at Appendix E that will help provide one method to classify sensitivity requirements of all types of data. The table is only an illustration of one way to accomplish the classification process.

8. Sensitive IT System Inventory and Definition

Sensitive IT system inventory and definition requirements identify the steps in listing and marking the boundaries of sensitive IT systems in order to provide cost-effective, risk-based security protection for IT systems, for the agency as a whole, and for the COV enterprise. For more information, see the latest SEC-501 ITRM Information Security Standard, which includes a section on, IT System and Data Sensitivity Classification.

Agency ISOs and designated system owners are responsible for documenting an information system security plan. Each ISO or designated sensitive system owner(s) shall:

1. Document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur.

   Note: Data and homogeneous systems, belonging to a single agency, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc. Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as system owner for the purposes of this standard, upon request, the CIO of the Commonwealth will determine the system owner. A sensitive IT system may have multiple data owners, and/or system administrators, but must have a single system owner.

2. Maintain or require that its service provider maintain updated network diagrams.

   Note: There is a template at Appendix F that provides guidance on the necessary information for IT systems inventory and definition documentation.

9. Risk(y) Assessment (Business)

Now that you have the BIA and system and data sensitivity, you know your risky business!

Pick the most risky systems first:

a. The information from the BIA, system and data sensitivity and this risk assessment work will be gathered for the RA planning phase.
b. If the system is a “support” system – it is used by more than one system - each subsystem should be assessed separately.

i. Each system will be audited separately.
ii. System inventory and definition - what is it made of??

c. Who – agency system and data owners, system administrators, AITR, CAM and NG OAM will all be helpful, as well as any power users.
d. What – Agencies are required, unless otherwise approved by the CISO, to use the Risk Assessment Plan template found at: http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs
e. Each agency head shall submit the agency risk assessment plan to the CISO annually. The risk assessment plan must include the following:

i. The agency name, agency abbreviation and agency number,
ii. The contact information of individual submitting the plan,
iii. The date of submission,
iv. The system full name and abbreviation,
v. The planned assessor,
vi. The date the last risk assessment was conducted for the system, and
vii. Scheduled assessment completion date.

Note: Scheduled assessment completion date is the planned date of the completion of the future risk assessment covering a three year period from the submission date.

f. Boundary Description and Diagram – may need a visit to the server room
    1. Components - Hardware - NG will provide network details – switches, routers, servers, etc – and agency should have software (app, operating sys, protocol) (example diagram)
    2. System Interfaces – including purpose and relationships- information flow diagram will be helpful here as well as the other system owner information. (example diagram)
    3. Interoperability security and agreements - if the systems have different owners, and sensitive data, a formal signed agreement should be developed.
g. When – Conduct and document a RA of the IT system as needed, but not less than once every three years. Document and report updates to CISO using the risk assessment template.
h. Also will need to conduct and document an annual assessment to determine the continued validity of the RA. Send updates to the annual assessment to CISO.
i. Risks identified in the risk assessment with a residual risk rating greater than a value of low create a risk finding. Note: residual risks are calculated based on the data from the risk assessment.

k. For each risk finding, a risk treatment plan shall be created using the risk treatment plan template.

The agency head or designee shall submit to the CISO the following information:

1. A record of all completed IT Risk Assessments conducted by or on behalf of the agency.
2. Agencies are required unless otherwise approved by the CISO to use the RA template found at: http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs
3. Each risk identified in the risk assessment template must contain:
   a. IT System Name
   b. Risk ID
   c. Sensitivity rating (e.g. Confidentiality, Integrity and availability)
   d. Date of risk assessment
   e. Risk vulnerability family (e.g. SEC-501 control)
   f. Vulnerabilities
   g. Threats
   h. Risk summary
   i. Magnitude of impact (e.g. low, moderate, high, critical)
   j. Controls in place (brief description)
4. For each risk identified, a risk treatment plan must be submitted to the CISO. The risk treatment plan shall include the:
   a. IT system affected
   b. Authoritative source (e.g. SEC-501, enterprise policy, operating instruction)
   c. Control ID (e.g. AC-1)
   d. Date risk identified
   e. Risk summary
   f. Risk rating (Low, Med-Low, Med, Med-High, High, and Critical)
   g. Status
   h. Status date
   i. Planned resolution;
   j. Resolution due date
5. The risk treatment plan for completed risk assessments must be submitted within 30 days of issuing the final risk assessment report. An updated risk treatment plan must be submitted quarterly (at the end of the quarter), until all resolutions are completed. All risk treatment plans and quarterly updates submitted must have evidence of agency head approval. This can be done by copying the agency head on the email sent to Commonwealth Security.

   You should be “audit ready” now!

10. Information Security Training

As an ISO, it is your responsibility to develop and maintain a formal information security awareness and training program. All employees at your agency, including contractors, interns, and temporary staff are required to complete this training on an annual basis, when there are system changes or more often if necessary.

There are requirements you have to include as part of your training program to comply with the VITA security policy:

1. Your agency's policy for protecting IT systems and data, with an emphasis on sensitive IT systems and data.
2. The concept of separation of duties.
3. The prevention and detection of information security incidents, including those caused by malicious code.
4. Proper disposal of data storage media.
5. Proper use of encryption.
6. Access control, including creating and changing passwords (including keeping them confidential).
7. Agency acceptable use policy.
8. Agency remote access policy.
9. Intellectual property rights, including software licenses and copyright issues.
10. Responsibility for the security of COV data.
11. Phishing and social engineering.

Based on specific roles within the organization, such as those of a system or network administrator of a sensitive system, additional specific security awareness training must be provided based on these operational responsibilities. Your program is going to need to have an auditable way to ensure users participated in the program. Local auditors as well as APA (Auditor of Public Accounts) will always ask for this documentation at some point. Be sure to maintain these records in accordance with your agency's retention policy.

There are also some things you can do as part of your training program such as: provide users with security awareness email tips, posters, supplies inscribed with security reminders (like pens or post-its), log-on messages and conducting awareness events.

This might seem overwhelming, but there is some relief! You do not necessarily have to do this on your own. Several companies, including VITA do have a training program you can purchase, for a fee.

11. Agency Level Security Policy (The ISO's Opportunity to be King/Queen for a Day)

Policies, Standards, Guidelines, and Procedures – oh my!

In order to ensure that agency data is secure, controls need to be implemented to protect the data and the IT systems that store and process this data. Information security policies, standards, guidelines, and procedures are the documents used to define these controls. The agency level security policy is the cornerstone of the information security program.

The ISO is responsible for developing and managing the agency's information security program beginning with a well defined agency level security policy. IT security policies and procedures help identify the critical aspects of an agency's security framework that is in place for users to follow regarding business and technology issues that may occur.

For those agencies that have not developed all their IT security policies and procedures, Commonwealth Security and Risk Management (CSRM) will have approximately 30 policies and procedures they will be able to share with agencies in the near future. Some examples of the 30 policies and procedures that will be shared with agencies are:

- Information Security Program Policy,
- Information Security Roles and Responsibilities Policy,
- IT Configuration Management Policy,
- IT Contingency Planning Policy,
- Risk Assessment Policy,
- Emergency Response Damage Assessment Procedure, and
- Information Security Incident Response Procedure.

These policies and procedures prepared for CSRM will be helpful for those agencies that may have limited resources to prepare the needed IT security policies. The IT security policies that will be shared with agencies establish the controls for protecting the confidentiality, integrity, and availability of the agency's data and the information systems that store and process the data. Once these policies have been undergone the CRSM review they will be made available to agency ISOs.

12. Responding to Security Incidents

Over 90% of all data breach victims learn of the compromise from third party notification, not from internal security personnel. The level of impact suffered from a data breach is very much determined by detection of and response to the incident.
A successful Information Security Incident Response Process starts long before the incident ever occurs. When developing the Information Security Incident Response Process, keep the following principles in mind:

1. Prepare
2. Identify
3. Contain

4. Eradicate
5. Recover
6. Learn

Prepare – designate agency personnel who have expertise dealing with information security incidents to be members of an Incident Response Team. Develop an Incident Response Plan so that the members of the Incident Response Team know what they are supposed to do when an incident occurs. Make sure that the Plan includes categories of information security incidents that are prioritized based on the immediate and potential adverse effect that the incident could have and how it could affect the IT system(s) and data.

Identify – the type, severity and source of the compromise in order to determine the categorization level of the incident so that the appropriate course of action can be taken.

Contain – the damage and minimize the risk to the agency with an appropriate response. Take measures to contain and control the incident to prevent further unauthorized access to of use of personal information including shutting down servers, applications, or third-party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.

Eradicate – the threat. Eliminate vectors of attack and mitigate exploitable vulnerabilities.

Recover – the IT system(s). Take needed actions to restore essential systems to functioning status, either in the original or in a repaired environment, or determine that the recovery activities must cease or be suspended until a different or rebuilt environment can be configured.

Learn – from the incidents and incorporate the lessons learned into the Incident Response Plan and Process. It is helpful to include an Incident Response Template in the Incident Response Plan so that it can be filled in during the incident and reviewed later to ascertain lessons learned and incorporate changes into the Incident Response Plan.

Establish a process for reporting information security incidents to the COV CISO. Executive Branch agencies must establish a reporting process for information security incidents in accordance with §2.2-603(F) of the Code of Virginia so as to report "to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence…all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities."

It is very important that you thoroughly test the Incident Response Plan before an actual incident occurs. Without thorough testing, you cannot be confident that the measures you have put in place will be effective in responding to incidents.

Where do I go for help? Refer to the NIST SP 800-61 Computer Security Incident Handling Guide.
This publication provides guidelines for incident handling with emphasis on analyzing incident-related data and determining the appropriate response to each incident.

It has a good Incident Handling Checklist as well as several really good incident handling scenarios which could be used for testing the Incident Response Plan.

13. Disaster Recovery ≠ Continuity of Operations

What is the difference between Disaster Recovery (DR) and Continuity of Operations (COOP)? They are not the same, though many people tend to put them together. Disasters basically fall into two (2) categories. Either you can take the blame or you can't:

- Natural: weather, wildfire, health related (epidemic), floods, earthquakes, volcanic, space
- Man-made: war, arson, crime, terrorism, power, structural, transportation, hazardous material

The goal of Disaster Recovery is to minimize the effects of a disaster and take the necessary steps to ensure that resources, personnel and business processes are able to resume operations in a timely manner. Another way to think about it is to consider that DR is carried out while everything is still in "emergency mode." This plan is to get the most critical systems on line right away.

Continuity of Operations is more along the lines of "OK, so the sky fell, how do we stay in business until someone can put it back?" This plan is much broader and involves getting the critical systems moved to another environment while repair of the original facility takes place and performing business in a different mode until regular conditions are back in place. COOP provides methods and procedures for dealing with long term outages and continuing operations until recovery is complete.

Having your systems up and running doesn't do any good if your people have no place to work and no process to get the job done.

As the ISO, you have a responsibility to review and approve the agency's Continuity Plan (previously called a Continuity of Operations Plan (COOP)), and Disaster Recovery Plan, if applicable. Whew, that's a mouthful!

14. Exceptions, Exceptions, Exceptions

Contrary to what you may have been told, you can't ignore SEC-501 requirements just because you can't comply with them or you think they're ridiculous. Putting your hands over your eyes and saying "I can't see you! I can't see you!" doesn't make them go away.

Take a deep breath and keep a few things in mind. First, the standard is written to cover a wide range of environments from social services, to universities, to tourism and can sometimes be pretty vague or painfully detailed. Certain entities have more tolerance for risk than others or have fewer industry regulations to comply with. Look at how the standards apply to your organization and start from there.

Second, Rome wasn't built in a day. VITA understands that certain things may take longer than others. You may a legacy system that doesn't allow for the requisite password settings or event logging, but that doesn't mean a whole lot.

Get that exception form out and start thinking compensating controls and future plans. With the current system, what can you do to mitigate the risk? Get creative. If password complexity can't be enforced, can the length of the password be increased? Can you run periodic scans with a password checker to test password strength? (Note to self: Don't crack them without your 'get out of jail free' card). Do you send out security awareness reminders? If logs aren't read only, can someone write a script that shows the log checksum, so you'll know if the log was modified? Can logs be automatically sent to someone outside of IT for review?

Exceptions may be given if compensating controls are adequate to reduce the risk or if extra time is needed to put controls or a new system in place. Exceptions are useful in several ways:

- They allow VITA to know where the risks are throughout the commonwealth and where to add extra resources, if possible.
- They give you a temporary pass when an auditor says you're not complying with commonwealth standards in a particular area.
- They help you and management better plan for the future, especially if a new system needs to be developed or acquired. Exceptions don't last forever, so it helps keep the issue from falling through the cracks.
- They help provide acknowledgement of understanding the risk if your worst nightmare comes to pass and you wake up to your agency getting slammed in the newspaper for a security breach.

The Exception Form template can be found under the Templates for Download on the ITRM Policies, Standards and Guidelines Web page at the following link:

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

15. Audits Can Be Your Friends

Are you struggling to get management to implement some of your security recommendations and hitting a brick wall? Discussing the issue with your auditor can benefit you in several ways.

First, the auditor can include the finding in the audit report, which adds legitimacy to your concerns. Management will assume the auditor found the problem. Because the report goes to the Governor and General Assembly, you may find that management suddenly wants to address the issue. Or if the lack of money was the reason your pleas were ignored and the issue is enough of a security risk, there's a chance that extra appropriations could be added to the budget. If not, perhaps management will surprise you and decide it's necessary to reallocate funds to ensure the finding is not repeated in the next audit report.

Second, it helps the auditor by reducing the effort needed to find the control weakness on their own. You will learn that a happy auditor is a good thing. Why? Some issues come down to 'auditor judgment.' If a particular issue can swing either way (verbal recommendation vs. management point) and you'd prefer to fix the problem without it going into the audit report, what do you think your chances are of that happening if you've fought the auditor the whole time?

A good working relationship is essential. If you ask an auditor what the #1 rule is, the 'clean' response will be, "don't make the auditor mad."

16. Obtaining Information Security Reports from the Partnership (Who from and What)

Reports From Your Service Provider

Your agency Customer Account Manager (CAM), Customer Relationship Management, Virginia Information Technologies Agency (VITA), can provide a variety of reports. Reports Include:

a. Detailed information regarding the work being completed at your agency from the work request system, the following link is to the: https://ssl01.apps.vita.virginia.gov/WorkOrderRequest/default.aspx
b. Your CAM can also provide reports regarding the exceptions and significant issues using the VCAST system which can be found at the following link: https://xrm.virginia.gov/VITA/main.aspx
c. Partnership Asset Reporting Server (PARS) is found at https://covsmices-msq01.cov.virginia.gov/Reports/Pages/Folder.aspx

The Partnership Asset Reporting Server (PARS) imports information from Altiris (our source for electronic inventory collected from computers) and Asset Center (our tool for managing all assets) to provide interested parties with insight into the assets located within the VITA/NG partnership. PARS provides a variety of reports. There are reports such as listings for desktop, laptop and server that includes the asset tag number, user name and user e-mail account. Also, there are reports on the top applications in use by your agency, refresh service activity, CISCO VPN profiles, and computers with encryption. There are approximately 30 reports related to computers, servers and services.

- To gain access to the Partnership Asset Reporting Server you need to have the following to access PARS:

  An active COV domain account
  Your COV domain account must be a member of one or more of these security groups
  A136-AC-PARS Agency Access
  A136-AC-PARS Internal Access
  A136-AC-PARS Asset Team Access
  Your COV domain user id must be added to PARS

- As an agency employee of the Commonwealth of Virginia, your id needs to be added to the appropriate tables within PARS associated with the agencies for which you have been approved.

- For the **VITA IT Comprehensive Goods and Services (Online Billing)** application try VIM at: http://vita.virginia.gov/resources/default.aspx?id=13002

    - Inventory billing is monthly and shows billing for all agency asset-based services; e.g. desktops, laptops, printers, servers, etc. Below are step-by-step guidelines to help validate your inventory billing.
    - Step 1 – Log in to billing site
    - Go to the Comprehensive IT Goods and Services
    - Access and log in using your COV credentials
    - Select your agency, then select the month for the billing cycle you wish to view.
    - Your view of the agencies will show only your agency or any sub-agencies.
    - You can download the billing in a PDF format or in Excel.

- For CTP - Oracle Primavera Portfolio Management (OPPM) instructions for setting up the account are found at: http://www.vita.virginia.gov/oversight/projects/default.aspx?id=505
    - The CTP provides monthly and quarterly information regarding current projects for your agency.
    - Reports are set up for project managers or application development managers.
    - The reports provide the status of projects using the red, yellow and green color codes for problem status, caution status and on time status.

Reports and Requests from Websites and Customer Care Center

We also have a listing that was provided by the Commonwealth Security and Risk Management (CSRM), Virginia Information Technologies Agency (VITA) at Appendix G of this manual.

Another reporting database is the **Commonwealth Enterprise Technology Repository** (CETR). To access CETR you will need for your AITR to send a request to the VITA Customer Care Center (VCCC). Once you have been granted access go to the website using the following link:

https://ssl01.apps.vita.virginia.gov/cetr/

CETR houses information, maintained by Executive Branch agencies, on agency components: applications, data assets, data exchanges and software tools. CETR has also been called the Commonwealth's Enterprise Applications Portfolio. Authorized agency users may:

- Add and maintain information
- View agency information
- Certify agency information
- Maintain the relationships between components
- Extract information for analysis

The information in CETR is related to your agency systems and identifies which systems are considered sensitive. Information also includes when audit plans were submitted, overdue audit findings and your sensitive systems missing IT security audits.

CETR is now being used to populate the Enterprise Governance Risk and Compliance application that is used for the VITA annual Data Points (which may soon be highlighted on a quarterly basis).

17. Big Iron – Mainframe Security

I. TSO STEPS for Mainframe to CREATE NEW ACCOUNT

A. To access the online forms from VITA go to this website: http://www.vita.virginia.gov/misforms/forms/VITA03_001.cfm
B. The UID is the agency name abbreviation + department/location + employee's 3 initials
   1. xxxxxxxx
C. Under special considerations for a new person put:
D. Please add TCP and xxxxxxxxxxxxxx
E. A request will automatically be sent to VITA who creates a ticket. They will let you know when it is done. Once you fill out the form for add or delete, press submit and it will send the request to VITA. Save a copy of the request you sent to VITA in an on-line folder. When they send you an email back stating your request has been processed, save that email as well.
F. FYI- Once the account is created – go in a un-suspend the account and make up a password of 8 characters and at least 1 has to be a number. Press enter
G. Send an email to your Accounting Mainframe Representative to notify him that the request has been processed.
   1. Save a copy of the VITA notification in an on-line folder.
   2. Send an email to the user giving them their new logon and password.

II. TO LIST AN ACCOUNT:

list XXXXXX

III. UNSUSPEND AND ACCOUNT:

Change XXXXXX nosuspend
*** (hit enter)

If a person has PWP-VIO (3) that means they had 3 password violations and you need to do the nosuspend command and change their password.

IV. CHANGE A PASSWORD:

Change XXXXXX password (america1) (hit enter)

V. LIST EVERONE WHO HAS AN ACCOUNT:

List like (XXX-) AGENCY abbreviation

VI. TO GET OUT OF TSO TYPE:

end
l (to logoff)

Additional TSO COMMANDS

Settings:
Verbose: SET Verbose (full list of ACF2 id)
Terse: SET LID TERSE (only lists first and second line of ACF2 id)

ACF2 COMMANDS for Security Group and Related Actions

ALL MAS: SET LID TERSE, L LIKE(MAS-) to go back to full List, SET VERBOSE
SPECIFIC PRIVILEGE: List Ids with specific session (example CICSP1): LIST IF(CICSP1)
ALL IN ONE FIPS: l like(e6-) if(fips='760 acs')
Lids ids not signed in within specified time(NON-USAGE REPORT): L like(MAS-) if(acc-date le u'11/01/10')

(keep for information purposes only - the commands are ACF2 commands but DMAS ids may not have the same structure)

List ids with specific scope list (Security Officers' code for UID3): LIST IF (SCPLIST='MASABD')
List ids in one specific office/agency : LIST UID(MASCSE ABD) or LIST IF(UID3='ABD')
Update UID string: Examples- CHANGE MASJZD UID4(ABD) or CHANGE MASJZD UID5(ABC)
Resetting password on ids with NON-EXPIRING passwords: CHA *(MUST BE 8 CHARACTER PASSWORD) NOPSWD-EXP
List Location: LIST UID(MASCSE HEN) OR L UID(MASCSE HEN)
List wild character in MAScode: LIST LIKE(MASJ*D) OR L LIKE(MASJ*D)

QUICK REFERENCE FOR COMMANDS

VIEW COMMANDS:
List an id(know MAScode): LIST MASJZD OR L MASJZD

CHANGE COMMANDS:
Password Change: CHANGE MASJZD PASSWORD(MASCOME1) OR CHA MASJZD PASSWORD(MASCOME1)
Remove Violations: CHANGE MASJZD PSWD-VIO(0) OR CHA MASJZD PSWD-VIO(0)

Remove Suspend: CHANGE MASJZD NOSUSPEND OR CHA MASJZD NOSUSPEND
Suspend: CHANGE MASJZD SUSPEND OR CHA MASJZD SUSPEND
Name change: CHANGE MASJZD NAME(JOHN Z. DOE SR.) OR CHA MASJZD NAME(JOHN Z. DOE SR.)
Phone number change: CHANGE MASJZD PHONE(804-692-1580) OR CHA MASJZD PHONE(804-692-1580)

SIGN IN
Type: **TSO1 (enter)**
Enter your MAScode: **MASAAA (enter)**
Enter your password: **xxxxxxxx (enter)**
Always enter when you see 3 asterisks: **(enter)**
Type: **ACF (enter)**
TO SIGN OFF:
Type: END (enter)
At the READY prompt enter LOGOFF (enter)

ACT ACCOUNTS:

DOA contact is Wayne Gabbert (804) 371-0199 (w).

Email above request to Wayne Gabbert at DOA…. wayne.gabbert@doa.virginia.gov

Wayne will set up the account and email you back what the full account name will be. Follow the same steps as above to reset the password, e-mail your Accounting Mainframe Representative, and email the user.

18. COV Certification for ISOs

The goal is to make commonwealth IT systems more secure by assuring that the individuals who manage IT security understand and can apply the appropriate IT security controls and standards.

Currently there are two methods for obtaining a COV ISO Certification. The first method would be for the ISO to send an email to CSRM indicating the professional security certification that they currently hold. CSRM will follow Department of Defense Directive 8570 (DoDD 8570) for recognizing certifications. What is DoDD 8570? Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. The table that lists the certification providers associated with each approved certification is located at Appendix H of this manual.

The ISO with a certification would also need to attend ISO Security Orientation at least once every two years. Successfully complete at least one course in the KC ISO Academy at least once a year. Attend at least one ISOAG meeting per year (currently the designated ISOAG October meeting is mandatory). Maintain compliance with the continuing educational requirements of the professional IT security

certification body (by obtaining at least 20 additional hours of training per year). The following are the current ISO courses available in the Knowledge Center:

System Owner Training
Sensitivity Analysis
Facilities Security (SEC517-00)
IT Data Protection Guideline (SEC507-00)
Contingency Planning (SEC508-00)
Systems Security: System Security Planning (SEC515-00)
Systems Security: Malicious code Protection (SEC515-00)
Systems Security: System Hardening (SEC515-00)
Threat Management: Threat Detection (SEC510-00)
Threat Management: Incident Handling (SEC510-00)
Threat Management: Logging and Monitoring (SEC510-00)
Logical Access: Account Management (SEC509-00)
Logical Access: Password Management (SEC509-00)
Logical Access: Remote Access (SEC509-00)
Personnel Security (SEC513-00)
Removal of Data (SEC514-03)
IT Asset Management (SEC518-00)
Use of Non-COV Equipment to Telework (SEC511-00)

The second method to obtain ISO Certification if the ISO does not currently hold a recognized professional IT security certification would include the following:

a. Attend ISO Security Orientation at least once every two years.

b. Successfully complete at least three courses in the KC ISO Academy at least once a year.

c. Attend at least one ISOAG meeting per year (preferably the October meeting).

d. Starting in 2014 obtain an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to three hours each).

There is a summary of the COV ISO Certification requirements in Appendix I that will be very helpful in making sure you maintain your COV ISO Certification.

This is the last topic of the ISO Manual. The following areas are the appendices that will provide examples for the information we have provided in the manual. We hope the manual will be helpful for the areas you are working with as an agency ISO.

Appendix A: An example Governance RACI Chart:

Definition: *a model used to help define who is responsible / accountable;*

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Service Manager
Create a framework for defining IT services.			C	A	C	C	I	C	C	I	C	R
Build an IT service catalogue.			I	A	C	C	I	C	C	I	I	R
Define SLAs for critical IT services.		I	I	C	C	R	I	R	R	C	C	A/R
Define OLAs for meeting SLAs.				I	C	R	I	R	R	C	C	A/R
Monitor and report end-to-end service level performance.				I	I	R		I	I		I	A/R
Review SLAs and UCs.		I		I	C	R		R	R		C	A/R
Review and update IT service catalogue.			I	A	C	C	I	C	C	I	I	R
Create service improvement plan.			I	A	I	R	I	R	C	C	I	R

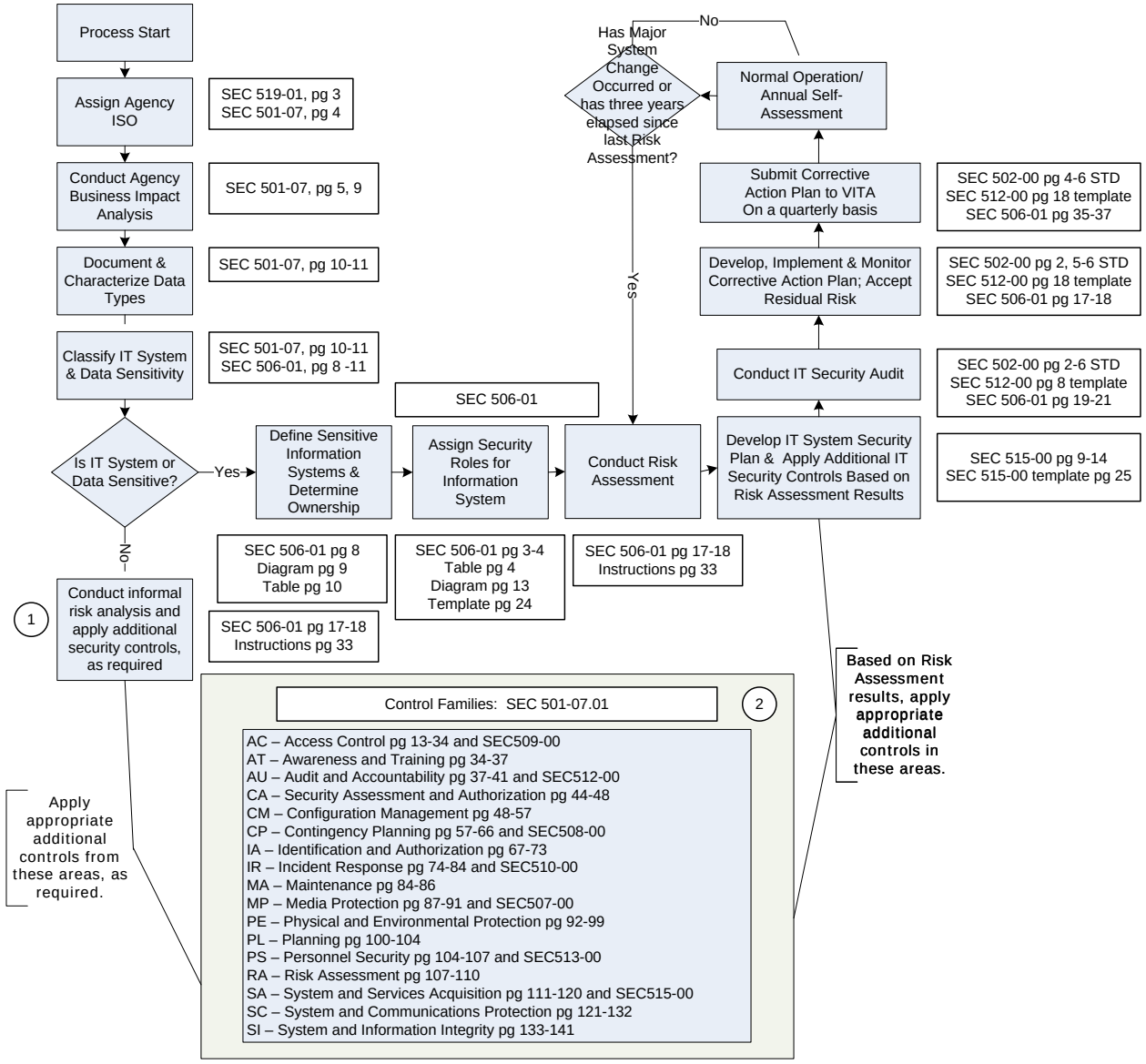
The RACI model is built around a simple 2-dimensional matrix which shows the 'involvement' of Functional Roles in a set of Activities. 'Involvement' can be of different kinds: Responsibility, Accountability, Consultancy or Informational (hence the RACI acronym).

The model is used during analysis and documentation efforts in all types of Service Management, Quality Management, Process- or Project Management. A resulting RACI chart is a simple and powerful vehicle for communication.

Defining and documenting responsibility is one of the fundamental principles in all types of Governance (Corporate-, IT-Governance). Reference: http://www.continentalsoftware.com/raci-model/

Appendix B: Commonwealth of Virginia Information Security Program Framework

The diagram below, illustrates the interaction of the component areas of the COV Information Security Program that enables COV agencies to accomplish their missions in a safe and secure environment when creating, maintaining, using, or disposing electronic records and processing such records with automated information systems.



Legend:

[1]Agency responsibility with technical assistance/information from IT Partnership

[2]Applicable documentation provided in NG Enterprise Infrastructure Security Practices Document (EISP) from Service Provider

Appendix C: The Supporting Cast - Security Roles and Responsibilities

Other roles include:

Roles and Responsibilities as defined by SEC-501 and SEC506 For more information regarding these, see the latest SEC501-07.01 ITRM Information Security Standard found on VITA's website.	
Role	Responsibility
Agency head	Oversee Agency IT Security Program • **Agency head designates ISO biennially to VITA**
Information Security Officer (ISO)	Overall security of Agency IT systems and liaison to the CISO of the commonwealth • Must be a COV employee • Must not be a system or data owner • Should not exercise (or report to an individual who exercises) operational IT or IT security application or infrastructure responsibilities Responsible for developing and managing the agency's information security program. **Works with the AITR. In some cases, ISO and AITR are the same position.** • **VCCC and AAO requires ISO and/or AITR approval for COV account administration, firewall changes, etc.**
Privacy Officer	Provide guidance on privacy laws • At agency head's/ ISO's discretion • An agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required. Otherwise, these responsibilities are carried out by the ISO.
Agency 's Information Technology Resource (AITR)	Acts as liaison between their agency and VITA • Serves as primary point of contact regarding agency concerns, working with VITA to resolve issues • Ensures the agency Strategic Plan (IT) accurately reflected in ProSight System along with agency IT investments such as projects/procurements
System Owner	Responsible for the overall security of an IT system (hardware or application). • Accountable to the agency head • Required for all sensitive IT systems • Must be a COV employee • Must not be ISO or system administrator for system owned
Data Owner	Spreads IT security awareness to data users. Develops any additional local requirements, procedures needed to protect the data.

	• Required for all sensitive IT systems • Must be a COV employee • Must not be ISO or system administrator for system owned
System Administrator	Day-to-day administration of the IT system. Implements requirements of the IT Security Management Program. • Required for all sensitive IT systems • Must not be ISO • The System Administrator may be an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the system owner, data owner, and/or data custodian. • Implements security controls and other requirements of the agency information security program on assigned IT systems.
Data Custodian	Protects data from unauthorized access, alteration, destruction, or usage and in a manner consistent with COV IT security policies and standards. • May be an individual or an organization (COV or partner) • Must not be ISO • Responsible for protecting the data in their possession from unauthorized access, alteration, destruction or usage.
IT System Users	Reads/complies with agency IT security requirements All users of COV IT systems including, but not limited to, employees and contractors are responsible for the following: • Complying with agency information security program requirements. • Reporting breaches of IT security, actual or suspected, to their agency management and/or the CISO. • Protecting the security of accessible IT systems and data.

Account Approval Quick Reference Guide

Use the Online COV Account Request Form		COV	AA	RR	YY	ZZ	Comments Required	Required Approvals				
COV								Manager	ISO	AITR	Authorized Approver	CSRM
	A Basic User Account	☐							☐	☐	☐	
	Admin Agency		☐						☐	☐	☐	
	Admin NG					☐				☐		
	HP Service Center	☐					☐		☐	☐	☐	
	Knowledgebase	☐							☐	☐	☐	
	Local Admin User Rights	☐						☐	Informed		IT Staff	non-IT Staff
	Local Power User Rights	☐						☐	Informed			

	PARs	☐					☐	☐				
	Resource Account			☐					☐	☐	☐	
	Service Account				☐				☐	☐	☐	
	SharePoint Access	☐					☐		☐	☐	☐	
	Single Sign-on VPN	☐							☐	☐	☐	

Appendix D: Business Impact Analysis Template

The best way to use the below is to copy each row below into one row in an Excel spreadsheet. Then copy row the single row to the rows below in the spreadsheet for each process you are documenting.

Agency	Primary Business Function	Primary Function Objective	Internal Customers	Commonwealth Agency Customers	Other Government Customers	General Public Customers	Other	If Applicable Describe Other Customer	Describe Data Used as Input
			Yes or No	Yes or No	Yes or No	Yes or No			
Internal or External Source of Data	Are External Systems Required	If Applicable Describe External Systems	Are Internal Systems Required	If Applicable Describe Internal Systems	Mission Essential Function or Supports Mission Essential Function	If Mission Essential Provide RTO in days	System Stores Sensitive Data that is Confidential	Describe the Confidential Elements for System	Provide the number of Confidential records processed or stored
External to the Agency Internal to the Agency Internal & External to Agency	External to the Agency Internal to the Agency Internal & External to Agency	Yes or No	Yes or No		Yes or No		Yes or No		
Life	Safety	Finances	Legality	Regulation or Compliance	Customer Service and Publicity	Privacy Impact on Agencies or Citizens	Additional Comments	Business Function Owner's Name	Business Function Owner's Phone Number
0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3	Yes or No			
Date BIA Completed	Name of Person Completing BIA								

Appendix E: Information System Security Plan

Agency Name
Information System Security Plan
Standard Assignment for Access by Office, Division, Section, Group

An **Information System Security Plan for each Sensitive Security System** is required by VITA SEC-501 Information Security Management Standard, Family 8.12 Planning, Section PL-2 System Security Plan, page 100, and VITA SEC515 Information Technology Systems Security Guideline.

Standard Access Assignment by Office, Division, Section, and Group Identified Below:
(name)

Data Information Owner & other Designated Contacts (key Point of Contact (POC) (*Name, title, Agency, address, email address, & phone #s) :*

Data Owner:
____, Director
Agency Name (abbreviation)
Office, Division, Section, Group (abbreviation)
Street Address
Richmond, VA 23219
_____@agencyname.virginia.gov
804-_____

Agency Information Security Officer:
name, Information Security Officer (ISO)
Office, Division, Section, Group
Agency abbreviation
Street Address
Richmond, VA 23219
First.lastname@agencyname.virginia.gov
804-_____

Authorizing Official (*Name, title, agency, address, email address, & phone # of the official designated as the authorizing official, such as the agency head or ISO):*

Name, Information Security Officer (ISO)
Office, Division, Section, Group
Agency abbreviation
Street Address
Richmond, VA 23219
First.lastname@agencyname.virginia.gov
804-_____

Operational Status *(Indicate the operational status of the data. If more than 1 status is selected, list which part of the system is covered under each status)**:***

Operational	Under Development	Major Modification

(system is in production)	(system is being designed, developed or implemented)	(system is undergoing a major conversion or transition)
X		

General System Description / Purpose ***(****Describe the function or purpose of the system & the information processes****):***

The network files are used by group staff to perform their daily work.

System Environment ***(****Provide a general description of the technical system. Include the primary hardware, software & communications equipment, as applicable****):***

Windows-Based Network, XYZservername
Oracle Databases as assigned

Standard Assignments:

Drive or share assignments, name of share:

Oracle Database:

Other, assumptions, etc.:

Related Laws / Regulations / Policies *(List any laws or regulations that establish specific requirements for the confidentiality, integrity or availability (CIA) of the data in the system)****:***

System ID:	Sensitivity Criteria		
Type of Data	**Confidentiality**	**Integrity**	**Availability**
	High Low	High Low	High Low

Classification: Sensitive*

*Treated as sensitive due to the nature of the data.

Plan to Implement Recommended Controls (reference Risk Assessment) *(Provide a description of how security controls recommended from the risk assessment are being implemented, or plan to be implemented, and who is responsible for the implementation)****:***

Formal Risk Assessment performed in _____.
Current controls are adequate based on Risk Assessment performed. No additional controls recommended.

Information Data Security Plan Completion Date ***(****Enter the completion date of the plan****):***

(date)

Information Data Security Plan Approval Date ***(****Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file and where on file****):***

June 17, 2013, authorization located within this document.

Review and Approvals

Recommended Date: (date)

Required Signature: _____
_____Director
_____ Office, Division, Section, Group (abbreviation)

*Reviewed by: _____
Name
Information Security Officer (ISO)
Office, Division, Section, Group

*may have multiple reviewers

Authorized by:

Required Signature: _____
Name
Information Security Officer (ISO)
Office, Division, Section, Group

Effective Date: (date) June 17, 2013

Review to occur every 3 years (per SEC-501, PL-2, page 101) from date of issue or sooner if major systems upgrade / change.

Appendix F: IT System and Inventory and Definition Document

IT System Inventory and Definition Document			
I. IT System Identification and Ownership			
IT System ID		**IT System Common Name**	
Owned By			
Physical Location			
Major Business Function			

System Owner Phone Number		**System Administrator(s) Phone Number**	
Data Owner(s) Phone Number(s)		**Data Custodian(s) Phone Number(s)**	
IT System Inventory and Definition Document			
IT System Inventory and Definition Document			
Other Relevant Information			
II. IT System Boundary and Components			
IT System Description and Components			
IT System Interfaces			
IT System Boundary			

III. IT System Operability and Agreements				
Agency or Organization	**IT System Name**	**IT System ID**	**IT System Owner**	**Interoperability Security Agreement Summary**

IV. IT System and Data Sensitivity			
Type of Data	**Sensitivity Ratings Include Rationale for each Rating**		
	Confidentiality	**Integrity**	**Availability**
Overall IT System Sensitivity Rating and Classification	**Overall IT System Sensitivity Rating** Must be "high" if sensitivity of any data type is rated "high" on any of the criteria		
	☐ **HIGH**	☐ **MODERATE**	☐ **LOW**
	IT System Classification Must be "Sensitive" if overall sensitivity is "high"; consider as "Sensitive" if overall sensitivity is "moderate"		
	☐ **SENSITIVE**	☐ **NON-SENSITIVE**	

Appendix G: Reports and Requests from Websites and Customer Care Center

The below listing was provided by Bill Freda, Security Analyst, Commonwealth Security and Risk Management, Virginia Information Technologies Agency (VITA).

Internet Activity	Blue Coat Link
SAS70 and Security Audit CAPS and POAM	Audit CC 136-VITA Site Link
SEC501 Self Assessment CAPS and POAM	PSO Site Link
Network Diagrams	VCCC ticket
Backup logs, evidence of daily backups	VCCC ticket
Backup Media logs, Evidence or off-site storage, labeling, act.	VCCC ticket
OS Level Vulnerability Scanning Reports	VCCC ticket
Malicious Code protection evidence reports	VCCC ticket
User list of users with access to sensitive systems	VCCC ticket
Remote Access Logs	VCCC ticket
Physical Access to Sensitive Systems (Where they are housed)	VCCC ticket
Security Awareness Training of ITP and Contractor Staff	VCCC ticket
IDS Logs, evidence that logs are reviewed and high risk events are addressed	VCCC ticket
Logs for User Access, successful logon, failed logon, brute force signatures	VCCC ticket
Data Destruction Verification Lists	VCCC ticket
Asset Management- Equipment Lists	VCCC ticket

Appendix H: ISO Certification Information

Certification Provider	Certification Name
Carnegie Mellon Software Engineering Institute CERT® *	Computer Security Incident Handler (CSIH)
Computing Technology Industry Association (CompTIA) *	A+ Continuing Education (CE)
CompTIA *	Security+ Continuing Education (CE)
CompTIA *	Network+ Continuing Education (CE)
CompTIA *	CompTIA Advanced Security Practitioner Continuing Education (CE)
EC-Council *	Certified Ethical Hacker (CEH)

International Information Systems Security Certifications Consortium (ISC)2 *	Certified Information Systems Security Professional (CISSP) (or Associate - this means the individual has qualified for the certification except for the number of years experience)
(ISC)2 *	Certified Secure Software Lifecycle Professional
(ISC)2 *	Certification Authorization Professional (CAP)
(ISC)2 *	Information Systems Security Architecture Professional (ISSAP)
(ISC)2 *	Information Systems Security Engineering Professional (ISSEP)
(ISC)2 *	Information Systems Security Management Professional (ISSMP)
(ISC)2 *	System Security Certified Practitioner (SSCP)
Information Systems Audit and Control Association (ISACA) *	Certified Information Security Manager (CISM)
ISACA *	Certified Information Systems Auditor (CISA)
Global Information Assurance Certification (GIAC) *	GIAC Certified Intrusion Analyst (GCIA)
GIAC *	GIAC Certified Enterprise Defender (GCED)
GIAC *	GIAC Certified Forensic Analyst (GCFA)
GIAC *	GIAC Certified Incident Handler (GCIH)
GIAC *	GIAC Security Essentials Certification (GSEC)
GIAC *	GIAC Security Leadership Certificate (GSLC)
GIAC *	GIAC Systems and Network Auditor (GSNA)

*From the approved IA baseline certification table on the DISA IASE website (http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html). Please review the website to ensure your certification is on the current listing of DoDD approved certifications for personnel performing IA functions that meet baseline requirements.

Appendix I: Summary of Steps to obtain COV ISO Certification

For those who already have a professional security certification:

Possession of recognized professional IT Security Certification	CISSP, CISM, CISA, SANS (others identified in the above DoDD 8570 certificate listing)
VITA Training	Attend Information Security Orientation training
ISO Academy	Successful completion of at least one course in the Knowledge Center (KC) ISO Academy per year
ISOAG attendance	Attend at least one mandatory ISOAG meeting per year (preferably the October meeting)
Continuing Education	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 2 - 3 courses per year in the KC ISO Academy
ISOAG attendance	Attend at least one mandatory ISOAG meeting per year (preferably the October meeting)
Continuing Education	Starting in 2014 obtain an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to three hours each)

Appendix J: SEC-501 MAINTENANCE CALENDAR

Component	SEC-501 Section	Deliverables	Time frame
Security Awareness	AT-1	Security awareness training refresher	Annually
System Hardening / Security Configurations	CM-2-COVd	Review, update and approve security configurations	Annually
Least Functionality	CM-7 1	Reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.	Annually
Vulnerability Scanning	RA-5	Perform vulnerability scans for publicly-facing systems, sensitive systems, and hosted systems	Quarterly and as needed
Vulnerability Scanning	RA-5	Update list of information system vulnerabilities scanned	Quarterly and as needed
System and Services Acquisition	SA-1	Review and update system and services acquisition policies and procedures	Annually
Corrective Action Plans (CAPS)	SEC 502	Provide VITA with CAPS	Quarterly and after each audit report is issued
Account/Privilege Reviews	AC2j	Review accounts and user privileges	Annually
Continuous Monitoring	CA-7d	Report the security state of the information system to appropriate organizational officials	Quarterly
Security Authorization	CA-6c	Update system security authorizations	Annually
ISO Designation	2.4	Submit ISO name to VITA	Bi-annually
Business Impact Analysis (BIA)	3	Review and update BIA	Every three yrs and as needed
System Classification	4	Review and update system and classifications, regulatory requirements, changes in owners, and potential damages	Every three yrs and as needed
Risk Self-Assessment	6	Conduct and document annual self-assessment to determine continued validity of Risk Assessment	Annually
Risk Assessment (RA)Report	6	Prepare RA report	Annually
Risk Assessment (RA)	RA-3	Review RA	Annually and when needed
Media Protection	MP-1	Review and update media protection	Annually

		policies and procedures	
Physical and Environmental Protection	PE-1	Review and update physical and environmental protection policies and procedures	Annually
Physical Access Control	PE-3	Inventories physical access devices and verifies physical access authorizations	Annually
Physical Access	PE-6	Review physical access logs	Every other month
Access Records	PE-8	Review visitor access records	Quarterly
Risk Assessment	RA-1	Review and update risk assessment policies and procedures	Annually
System Maintenance	MA-1	Review and update system maintenance policies and procedures	Annually
Incident Response Reporting	IR-6-COV	Provide quarterly summary reports of IDS and IPS events to Commonwealth Security	Quarterly
Incident Response Training	IR-2	Provide training in incident response roles/responsibilities	Annually (or whenever IR procedures are changed)
Incident Response Plan	IR-8	Review and update the IRP	Annually
Disaster Recovery Plan	CP-1-COV-1	Test the DRP (including backups)	Annually
Disaster Recovery Plan	CP-1-COV-1	Review and update the DRP as needed	Annually and as needed
Go-Kit	CP-2	Update the Go-Kit	Annually
Contingency Plan	CP-4	Update and test the COOP	Annually and as needed
Information System Backup	CP-9	Test backup information to verify media reliability and information integrity	Monthly
Security Planning	PL-1	Review and update security planning policies and procedures	Annually
System Security Plan	PL-2	Review, update, and submit security plan to Agency head for approval	Every three yrs and as needed
Personnel Security	PS-1	Review and update personnel security policies and procedures	Annually
Access Agreements	PS-6	Review and update access agreements (acceptable use)	Annually (and as needed)
Hardware/Software inventory and usage	CP-1-COV 2	Review and update the hardware/software list and ensure that actual usage is appropriate	Annually

Appendix K: Commonwealth of Virginia Acronyms

Acronym	Representation
ADM	Agency Deployment Manager (Northrop Grumman term)
AIDE	Asset Information Data Entry (screen)
AITR	Agency Information Technology Resource
AOM	Agency Operations Manager (Northrop Grumman term)
AP	Accounts Payable
APM	Agency Performance Management (division)
ARRA	American Reinvestment and Recovery Act
BD	Business Development (directorate)
BI	Business Intelligence
BOS	Business One-Stop
BP&A	Budget, Planning & Analysis (division)
CAL	Client Access License
CAM	Customer Account Manager (directorate)
CAM	Customer Account Manager (person)
CAN	Change Agent Network
CAO	Chief Applications Officer
CAP	Corrective Action Plan
CARS	Commonwealth Accounting and Reporting System
CAT	Customer Account Team
CATSPA	Commonwealth Agency Technology Strategic Planning Application
CATT	Cabinet Technology Team
CESC	Commonwealth Enterprise Solutions Center (new VITA/NG

	location)
CETR	Commonwealth Enterprise Technology Repository
CI	Configuration Item
CIA	Comprehensive Infrastructure Agreement
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CM	Commercial Management (division)
CMDB	Configuration Management Database
CMOC	Centralized Management Operations Center
COIA	Conflict of Interests Act
CoIN	Community of Interest Groups
COLA	Cost Of Living Allowance
COMMS	Communications (directorate)
COOP	Continuity of Operations Plan
COTS	Commercial Off-The-Shelf (software)
COTS	Council on Technology Services
CPE	Continuing Professional Education
CPE	Customer Premise Equipment
CPU	Central Processor Unit
COV	Commonwealth of Virginia
COVA	Commonwealth of Virginia
COVANET	Commonwealth of Virginia Network (telco network)
COVITS	Commonwealth of Virginia IT Symposium

CSA	Customer Service Alert
CSRM	Commonwealth Security and Risk Management
CSPMO	Customer Service Project Management Organization
CVC	Commonwealth of Virginia Campaign
DASD	Direct Access Storage Device
DR	Disaster Recovery
EA	Enterprise Architecture
EAAS	Enterprise Applications and Architecture Solutions (division)
EAD	Enterprise Applications Division
EBARS	Enterprise Backup and Recovery System
EBD	Enterprise Business Director
ECP	Engineering Change Proposal
EE	Employee
ELA	Enterprise License Agreement
ERP	Enterprise Resource Planning
ES	Enterprise Security (division)
ESG	Enterprise Solutions & Governance (directorate)
EUS	End User Support
eVA	electronic procurement system
F&A	Finance & Administration (directorate)
F&A Div	Finance & Accounting (division)
FAC	Finance and Audit Committee
FAQ	Frequently Asked Question
FOIA	Freedom of Information Act

GL	General Ledger
GIS	Geographic Information System
HITSAC	Health Information technology Standards Advisory Committee
HR	Human Resources (division)
IA	Internal Audit (directorate, division)
IFA	Industrial Funding Adjustment
IFB	Invitations for Bid
IMAC	Inventory Move and Change
IMAR	Install, Move, Add, Remove (MyRequests)
IOPS	Internal Operations Per Second
IP	Internet Protocol
IV&V	Independent Verification & Validation
IS Council	Information Security Council
ISO	Information Security Officer
ISOAG	Information Security Officer Advisory Group
ISP	Integrated Services Program
IT	Information Technology
ITAC	Information Technology Advisory Council
ITCL	Information Technology Contingent Labor
ITIB	Information Technology Investment Board
ITIES	Information Technology Investment and Enterprise Solutions (division)
ITIL	Information Technology Infrastructure Library
ITIM	Information Technology Investment Management
ITP	Information Technology Partnership

ITRM	Information Technology Resource Management
ITSP	Information Technology Strategic Plan
JCOTS	Joint Committee on Technology and Science
JLARC	Joint Legislative Audit and Review Commission (VA)
JPEG	Joint Photographic Experts Group (photo compression format)
KC	Knowledge Center
LAC	Local Area Coordinator
LAN	Local Area Network
LLS	Legal & Legislative Services (division)
LUN	Logical Unit Number
M&O	Maintenance and Operations
MSP	Managed Service Provider
MEE	VITA Managed Employee
MIS	Management Information System
MITA	Medicaid Information Technology Architecture
MOAT	Managed Ongoing Awareness Tool
MOU	Memo of Understanding
MP3	audio specific compression format
MPLS	Multiprotocol Label Switching
NAS	Network Attached Storage
NASCIO	National Association of State Chief Information Officers
NOC	Network Operations Center
NG	Northrop Grumman
NG 9-1-1	Next generation 9-1-1

OC&C	Other Charges and Credits
ORCA	Online Review and Comment Application
P2P	Procure-to-Pay
PAM	Process Automation Manager
PDA	Personal Digital assistant
PIR	Post-Incident Report
PM	Project Manager
PMD	Project Management Division
PMDP	Project Manager Development Program
PMP	Project Management Professional
PP&A	Policy, Practice & Architecture (division)
PPEA	Public-Private Educational Facilities Infrastructure Act
PPRAT	Policy and Procedure Review Architecture Team
PSAP	Public Safety Answering Point
PSC	Public Safety Communications
PSO	Program Security Office
RCA	Root Cause Analysis
RFO	Reason For Outage
RFP	Request For Proposal
RFS	Request For Service
RSS	Really Simple Syndication
RTIP	Recommended Technology Investment Projects
RMM	Request Management Module (ServiceCenter)
RU	Resource Unit

SA	Staff Augmentation
SAN	Storage Attached Network
SCM	Supply Chain Management (division)
SDM	Service Delivery Management (division)
SLA	Service Level Agreement
SLD	Service Level Director
SME	Subject Matter Expert
SMO	Service Management Organization
SOC	Security Operations Center
SOR	Statement of requirements
SoTECH, SoTech	Secretary of Technology
SOW	Statement of Work
SRM	Storage Resource Management
SWaM	Small, Women, and Minority-owned businesses
STAR Award	yearly acknowledgement of outstanding agency employees
SWESC	Southwest Enterprise Solutions Center
T&T	Transition and Transformation (division)
TB	Terra Byte
TSS	Technology Strategy & Solutions
VAP	Vulnerability Assessment Program
VBMP	Virginia Base Mapping Program
VCAST	VITA Customer Account Support Tool
VCCC	VITA Customer Care Center (help desk)
VEAP	Virginia Enterprise Applications Program

VGIN	Virginia Geographic Information Network
VI	Virginia Interactive
VITA	Virginia Information Technologies Agency
VITA KC	VITA Knowledge Center
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VPSW	Virginia Public Service Week
VSDP	Virginia Sickness and Disability Plan
WAN	Wide Area Network