REPORT OF THE
AUDITOR OF PUBLIC ACCOUNTS

A Review of Information Security in the Commonwealth of Virginia

TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA

SENATE DOCUMENT NO. 24

COMMONWEALTH OF VIRGINIA
RICHMOND
2006

EXECUTIVE SUMMARY

The information security programs in the agencies and institutions of the Commonwealth are generally inadequate and do not address the business needs to adequately control information as well as risks associated with not controlling information. The Commonwealth, however, has several agencies and institutions, such as the Departments of Taxation and General Services and the three largest institutions of higher education, University of Virginia, Virginia Commonwealth University, and Virginia Polytechnic Institute and State University, which provide working models of the best practices of information security programs.

All state agencies and institutions have some type of security over their information technology infrastructure and systems. The security, in most cases, provides coverage over information existing within the agency. Further, almost all agencies and institutions have at least some plan to recover from a disaster; however, this plan does not always extend to how and under what circumstances.

The Auditor of Public Accounts has been conducting security reviews of financial system for over a decade and reporting our findings. This review's results are consistent with our previously reported findings. With the exception of smaller agencies without financial systems, we have previously issued or commented on all the agencies with either no or inadequate information security programs.

In reviewing the results, the reason for inadequate information security programs in the larger agencies, when considering either number of employees or agency budget, appears to center around the resolution of who has responsibility for the infrastructure between the Virginia Information Technologies Agency (VITA) and the agency. The large institutions of higher education with inadequate programs typically do not have the managerial placement of the program at the appropriate level for the organization, although this does occur in other agencies.

Overall, the Commonwealth's standards address most of the components found in the best practices. The difference between the Commonwealth's standards and the best practices, to the most part, occurs within the processes of the components.

We believe the large agencies and institutions can address our recommendations without significant operational changes. However, the Commonwealth will need to develop and implement a process to provide information security programs for smaller agencies and institutions.

Finally, the General Assembly may wish to amend the Code of Virginia to provide for the audit of information security programs, rather than focusing on databases and data communications. The current statute does not address the real risk to the Commonwealth.

-TABLE OF CONTENTS-

CITIZEN'S PERSPECTIVE

Citizens are regularly entrusting significant amounts of personal and other information to state agencies and institutions. From filing tax returns with social security numbers of the filer and spouse to income, employer and bank account information for a tax refund to buying a fishing license. In many cases, citizens are voluntarily entering information on-line in real time over the internet including providing key financial information such as credit card numbers.

Citizens expect that state agencies and institutions are taking measures to properly secure and protect their information from misuse by hackers or employees. Citizens using these services make no distinction in the protection of their personal information when they give it to the Commonwealth.

While citizens understand that they may have to deal with different agencies and institutions, they expect the same level of service and security of their personal information at each agency. If the Commonwealth cannot assure citizens of this level of security, citizens may lose faith in the Commonwealth's ability to protect information and not be willing to provide electronic information in the future.

This report cannot and does not predict how citizens will respond to security failures. The report does analyze the state of the Commonwealth's information security programs, and whether they have the fundamental process to secure citizen information. What we can tell citizens is that the large agencies such as Taxation, Motor Vehicles, and others have sound working security programs, which protect their personal information.

Should a security breach occur, these large agencies also have, as part of their information security program, a plan to notify and assist citizens affected by the breach. However, these larger citizen-oriented agencies and institutions do not constitute the whole picture of information security in the Commonwealth.

A number of small and medium size agencies require significant improvement to their overall information security programs. The lack of information security programs in these small and medium size agencies creates an environment, which can create risks for the larger agencies and citizens because of our interconnectivity infrastructure.

INTRODUCTION

The 2006 General Assembly passed Senate Joint Resolution No. 51, directing the Auditor of Public Accounts to report on the adequacy of the security of state government databases and data communications from unauthorized uses. This report summarizes our findings on the current state of information security programs implemented at state agencies and institutions of higher education in the Commonwealth of Virginia.

In order to conduct this review, we evaluated the Commonwealth's information security programs against the best practices of the industry. In planning our work, we recognized that both the Resolution and the Code of Virginia do not provide a sufficiently broad definition of data security.

Focusing data security efforts on only databases and data communications does not consider the amount and nature of information held by the Commonwealth; nor does it consider the various methods of storing and using potentially sensitive information.

As this report will discuss in detail later, the Commonwealth's level of security represents a mixed picture of concerns, vulnerabilities, sophistication, and awareness. In many agencies and institutions, security programs have typically been an evolutionary process instead of a systematic, risk-based approach. A risk-based approach should align with business objectives and consider the amount and nature of information maintained by the agencies and institutions.

While VITA and its predecessor agencies have provided standards for the assessment, methodology, and development of security programs, it has been three outside influences that have led to the development of most agencies' and institutions' security programs. Those three outside influences were the Y2K concerns, Health Insurance Portability and Accountability Act (HIPAA), and the reactions to having the need to recover after disasters similar to 9/11.

While these outside influences have provided an awareness of the need for information security programs, their effectiveness on program development and completeness have yielded mixed results. Generally, agencies and institutions are aware of the need to have security programs; however, what the security programs should address and how remains an unanswered question in many organizations.

Several other factors affect the development of security programs and present risks associated with security programs in the Commonwealth. For example, current state policies make the agency or institution head responsible for security. While this policy clearly establishes who has responsibility for security, it ignores three important factors.

First, the lack of information provided to the agency head from the service provider that will enable the agency head to establish a proper information security program. Second, the lack of expertise to help the agency head understand his or her information security environment and risks and develop the program. Finally, the lack of resources may prohibit the development of a plan or even a simple assessment.

For most executive branch agencies, the Commonwealth structurally separates responsibility for software systems and applications from the technology infrastructure, except in institutions of higher education. For applicable agencies, VITA, along with Northrop Grumman (NG), are responsible for the technology infrastructure while agencies are responsible for their applications and data that reside on this infrastructure. The separation introduces a level of complexity into the Commonwealth security structure, since different parties may play various roles in protecting the same information, but at different points in the process.

As an example, a citizen may apply on-line for a license at a state agency. VITA and NG would have responsibility for the internet connection, firewall, router, and server and its associated operating system, which stores the citizen's license data and runs the licensing software application. The state agency would have responsibility for developing and maintaining the licensing software, screening the data submitted on-line, organizing and maintaining the data, and determining who has access to the license software and its associated data.

In this example, the shared responsibilities require that VITA, NG, and the licensing agency completely understand their role in providing this service to the citizen and work together to ensure the security of the information. Within the Commonwealth, these relationships are part of an evolutionary process, which began with the creation of VITA, and continues with the introduction of the NG contract.

Security of information and systems within the Commonwealth does exist; however, whether the appropriate level of security exists is not normally a well-reasoned or documented process. Security implementations have occurred in equal measures to respond to actual or perceived events, or have occurred when new or updated software have required increased security in order to access specific systems or information.

Our report will address the reasons for security and the methods we used to develop what we consider industry best practices. Our report will also discuss our audit procedures and processes and our findings and recommendations.

INFORMATION SECURITY PROGRAM OBJECTIVES AND ISSUES

A well-defined, clear, and documented information security program will minimize unauthorized uses of information contained within databases and transmitted through data communication lines. A lack of consistent or sufficient policies, procedures, and standards creates a highly diversified information security environment, which limits an organization's ability to govern information security at an enterprise level.

The Power of Information

This report focuses on the policies, procedures, and standards that control how the Commonwealth and its agencies access, store, and transmit electronic information. For the purposes of this report, there is an important distinction between the terms "data" and "information."

Generally, the term information means data that is useful or meaningful. The reason we make this distinction is because data is everywhere. Even though all data has a purpose and requires protection to some extent, the identification of data versus information is important in establishing an information security program.

The expression "one man's trash is another man's treasure" easily translates into the information security realm and can be rephrased as "one man's data is another man's information." In other words, data from location A and data from location B may independently not have any meaning. However, if combined, the two elements of data may become information. It is therefore important that an information security program considers and controls all possibilities of data usage. In addition to the distinction between information and data, further classification of information based on its sensitivity and/or criticality may be necessary. The following example will elaborate on the difference between data and information.

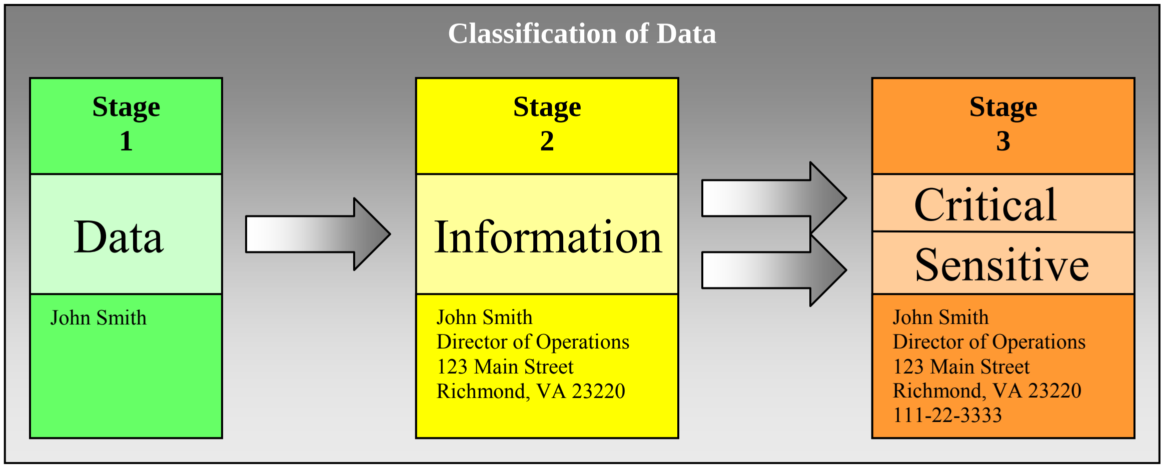


Figure 1 – Classification of Data

The illustration in *Figure 1* has three stages, Stage 1 - Data, Stage 2 – Information, and Stage 3 – Critical and Sensitive Information. Each stage represents a particular classification of data. Assuming a file containing a word processing document only contains the following: “John Smith,” the file classification is most likely “Stage 1 – Data,” as it contains data that has no meaning or context.

However, if someone applies additional data to the document, such as “Director of Operations, 123 Main Street, Richmond, Virginia 23220,” the file now contains a document with information. The collection of the first data element, “name,” with the additional data elements “title” and “address,” have reclassified the file into “Stage 2 – Information.” The file now contains information that is useful or meaningful.

Furthermore, if this document becomes an element of processing payroll, then the user organization may consider it “critical,” thus moving the file into “Stage 3 – Critical and Sensitive Information.” In addition, if the user organization adds another data element, such as social security number, the information in the file will change the classification to “sensitive.”

It is important to note that information is not exclusively stored in databases and transmitted over data communication lines. For example, a user may copy information from a database on a network, controlled by policies and procedures, onto an uncontrolled portable storage device, such as a Jump drive, which the individual carries out of a building in his or her pocket. The incredible speed at which information technologies have developed throughout the past 30 years, allows us today to keep millions of documents and spreadsheets, or information from a database, on a storage device, such as a Jump drive, that can attach to our key chains.

Granted, the human factor is the most unpredictable variable in an information security program. The implementation of a strong information security program, guided by well-documented policies, procedures and standards, minimizes the risks of information distribution to unauthorized users. Unfortunately, even the best information security programs cannot prevent the deliberate act of an authorized individual to disclose information to unauthorized parties. Additionally, information can become easily transportable and therefore highly subject to risk of loss and misuse. Following are classic examples that illustrate the ease of information portability outside the confines of an organization.

Case Examples

Identity theft is probably one of the most publicized aspects of poor information security controls today. There are frequent reports in the media that underline this point and demonstrate that the lack of information security controls exists in corporations as well as government agencies.

Public Organization

On May 22, 2006, the U.S. Department of Veterans Affairs issued a statement that one of their analyst's laptops was stolen containing 26.5 million names, social security numbers, dates of birth, and health records of active and retired veterans and spouses.

Private Organization

Financial services company ING had a laptop stolen from the Washington home of one of its employees on June 12, 2006 containing sensitive data, such as social security numbers, of 13,000 District of Columbia employees and retirees.

Information sensitivity/confidentiality is only one of many concerns of information security. Information does not need to be sensitive or confidential in order for an organization to consider the information critical to its mission. Even though most information stored by the Commonwealth is public information and is available to the public upon request, its unauthorized alteration or inaccurate disclosure of public information may greatly impair the efficiency and effectiveness by which the agency conducts its mission. For example, unauthorized alteration of accounting information may lead to inaccurate financial statements that, in turn, lead to inappropriate resource allocation and budgeting.

All organizations need to analyze and determine what data and information they have. This determination, coupled with a consideration of whether the data is critical and/or sensitive, becomes the cornerstone of an effective information security program. Understanding the nature of data and information is also necessary to develop a security program that looks beyond the controls that exist only within the physical confines of the organization.

We have already discussed the classic problem of identify theft and financial misstatement. However, organizations need to realize they may be holding other data, such as proprietary information obtained in conjunction with a bid proposal that may compromise the corporation that submitted it. Addressing safeguards of information is the primary purpose of an information security program.

Definition of Information Security

An information security risk is any activity or event that threatens the achievement of identified business objectives by compromising the confidentiality, integrity, or availability (CIA) of data. Organizations are vulnerable to many kinds of information risks inflicting various types of damage, which can result in significant losses. This damage can range from errors harming data integrity to fires destroying entire computer centers. In more detail, an information security program seeks to minimize risks in the following information security areas.

- Confidentiality provides assurance that sharing information occurs only among authorized persons or organizations. Breaches in confidentiality can occur when organizations do not handle or protect data in a manner adequate to safeguard the confidentiality of the information. Such disclosure can take place by e-mailing, creating documents or data files, printing, copying, or word of mouth. The classification of the information should determine its confidentiality and hence the appropriate safeguard.

- Integrity provides assurance that information is not only "correct," but also whether the information can be trusted and relied upon. Users frequently use the term integrity when discussing the primary indicators of information security as to whether a system has or does not have security. For example, consider an application developed by an organization that processes employee travel payment reimbursements and directly deposits the payment into their bank account. Without proper change controls in place, someone could change the program of the application to transfer the travel reimbursement payments to fraudulent bank accounts.

- Availability provides assurance that the systems responsible for delivering, storing, and processing information are accessible when needed, by those who need them. In ensuring the continuous operation of the organization, it is important that the information security program plans for contingencies and documents the critical infrastructure components, such as financial, document management, and e-mail systems necessary to ensure those operations.

Often considered as the three pillars of information security; confidentiality, integrity and availability provide a strong foundation upon which organizations, including the agencies of the Commonwealth, should build sound policies, procedures, and standards that together establish an information security program.

Internal and External Threats

Internal and external threats are events or actions that compromise the confidentiality, integrity, or availability of electronically stored information. Specifically, internal threats are those events or actions taken by staff and employees that often have authorization to access the agency's information in their normal course of business. External threats, on the other hand, are those events or actions involving individuals outside the organization that generally attempt to gain access without permission. Law enforcement agencies classify these attempts as "attacks," although they are similar to burglaries. We discuss these two types of threats in more detail below.

In the 2006 CSI/FBI Computer Crime and Security Survey, conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, approximately one third (32 percent) of the participants in the survey believe that no loss is caused by insider threats to information security. The remaining participants, approximately two thirds (68 percent), believe that insider threats are to blame for a certain percentage of loss. For example, 29 percent of the participants believe that 20 percent or less of threats to their information security environment come from insiders. Whereas seven percent of the participants believe that 81 percent to 100 percent of threats to their information security environment come from insiders. These numbers are represented in the following figure, "Percentage of Losses that Come from Insider Threats," below.

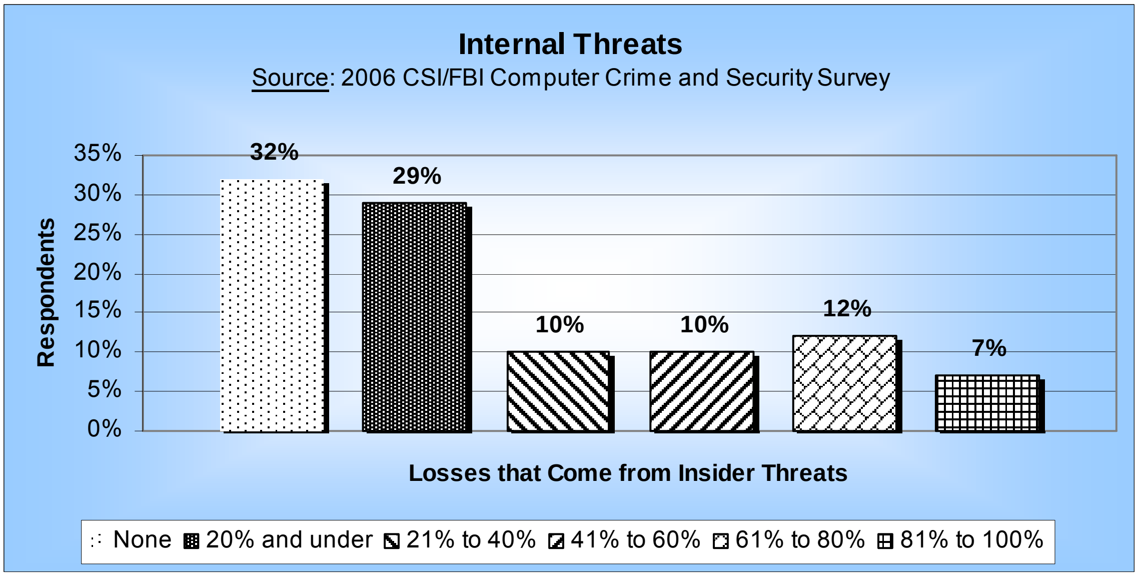


Figure 2 – Percentage of Losses that Come from Insider Threats

As mentioned earlier, an internal threat is an action or event initiated by an employee or staff that has valid access to agency information as part of performing his or her job duties. This type of threat is the most difficult to predict or protect against. Many groups also classify internal threats as intentional or unintentional.

Intentional internal threats include employees gathering information kept by the agency and selling it for personal gain, disgruntled employees seeking revenge, or simply employee curiosity. As an example, a crime organization could approach an employee with access to the information surrounding credit cards issued to employees. The crime organization offers the employee a handsome reward in exchange for a copy of the database containing all the information needed to use the credit cards.

Using a portable storage device, the employee copies the information and conducts the transaction with the crime organization. If there are no controls or audit trails surrounding the electronic storage of the credit card information, the theft is undetected until the credit card statements arrive. By this time, it will be difficult to prove who stole the information, unless at a later date, someone catches an individual in the crime organization and that person testifies against the employee that sold the credit card information.

Unintentional internal threats include employees that have inadequate security awareness training and initiate an action or event inadvertently. For example, a graduate teaching assistant receives an assignment to analyze student enrollment over a certain period. Instead of analyzing this information directly against the data repository at the college, the graduate student downloads the information (consisting of 250,000 student social security numbers and names) onto his laptop computer in order to use the advanced analysis features of a spreadsheet application.

Since the graduate student also uses his laptop computer in his dormitory with an active wireless connection, this situation would allow another person to access the student's laptop unless the graduate student has a well-protected laptop with the latest security patches and firewalls. Another person could use widely available "hacking" tools to access and copy the social security numbers and names.

Lastly, external threats are those actions or events initiated by someone outside of the organization who is attempting to compromise the organization's information or systems. For example, someone has released a new virus in the form of an internet worm. The purpose of the worm is to find and infect as many computers as possible and wait idle for a particular time before becoming active. When the worm activates, on a particular date, every computer infected with the worm makes a simultaneous transaction request to a particular on-line computer system. This method of attack is a denial-of-service attack, which overloads the on-line system with requests and makes it unavailable to legitimate system users who need access to the system in order to conduct business.

Other external threats include natural disasters, such as earthquakes, fires, hurricanes, and floods. Even though these threats are unpredictable, a well documented continuity of operations plan and disaster recovery plan will minimize downtime.

Policies, Procedures and Standards

Legal and regulatory requirements can and should affect an organization's information security program. Although there are many state and federal requirements, three of the most common requirements are the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Freedom of Information Act (FOIA). Laws and regulations such as these must become part of the standards, guidelines, procedures, and practices that collectively comprise the information security program. Additionally, the information security program needs to address industry best practices, as discussed later.

Both FERPA and HIPAA have requirements that restrict the distribution and dissemination of information. FOIA, on the other hand, seeks to make information about government operations easily available to the public, so that the public can monitor government activities. It is not unusual that laws and regulations appear to have conflicting purposes and implementation requirements; however, organizations need to know of these conflicts and decide how to deal with them in their information security program.

In another example, FERPA prevents parents from obtaining a college student's grades without the student's permission. However, students often demand that professors provide grades as quickly as possible after grading tests. Often the professor posts these grades on a class web site, which may or may not have appropriate restrictions under FERPA.

Figure 3 below illustrates the information flow model for policies, procedures, and standards:

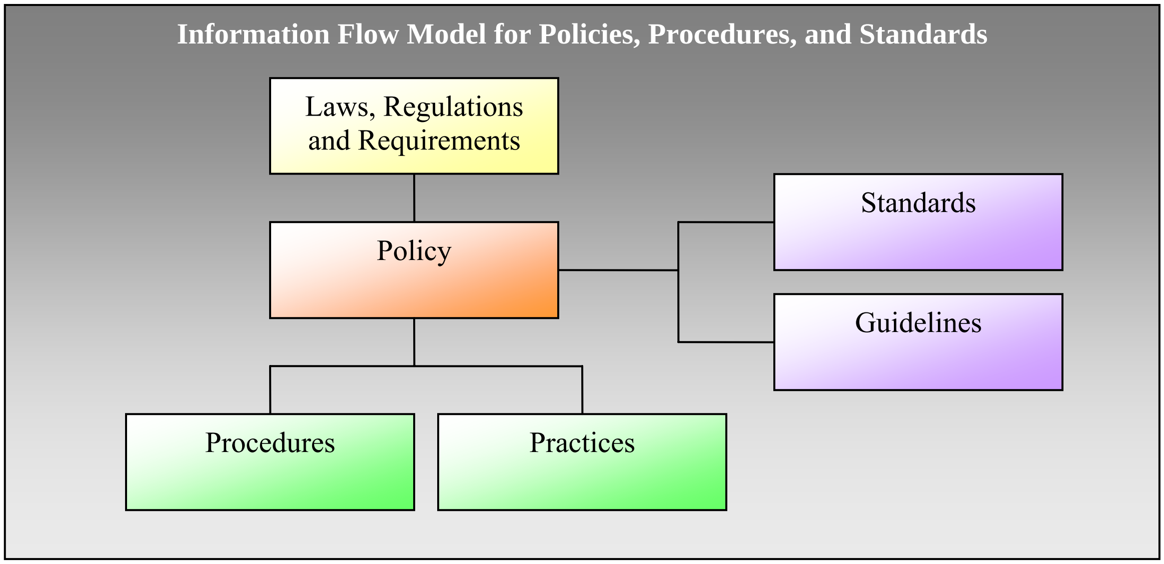

Information Flow Model for Policies, Procedures, and Standards
Laws, Regulations and Requirements
Policy
Standards
Guidelines
Procedures
Practices

Figure 3 – Information Flow Model for Policies, Procedures, and Standards (Peltier 2004)

In the figure above, laws, regulations and requirements flow into the policy. A policy states information security goals in general terms. As companions to a policy, standards and guidelines will define what action an agency must accomplish in specific terms. Finally, the procedures and practices document how to meet the standards and guidelines. The development of an information security program with complete policies, procedures, and standards is one method that data owners and management can use to demonstrate that they have implemented reasonable and appropriate information security measures to protect its information.

Industry Best Practices

As part of this review, we compiled from available sources the industry identified best practices for an information security program. We compared the Commonwealth's Information Security Program against the best practices as a means of completing our review checklist, which we discuss later. We highlight the best practice generating organizations and the specific standards we compiled.

The organization recognized for setting the standards for sound internal controls is the Committee of Sponsoring Organizations (COSO). The Sarbanes-Oxley legislation governing public corporate operations and internal controls recognized COSO's activities by its inclusion in the regulations implementing the law. While this organization provides general guidance regarding what internal control systems should address and how these systems control financial compliance and other transactions, their guidance does not specifically address the information security program. COSO does provide a list of organizations that provide more detailed guidance.

There are several nationally recognized best practice standards, each of which provides varying levels of guidance and detail. The following are the major organizations that have developed and contributed to the development of Information Technology Security Standards.

- International Organization for Standardization (ISO)
- US National Institute of Standards and Technology (NIST)
- Information Systems Audit and Control Association (ISACA)
- US Government Accountability Office (GAO)

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) seeks to develop operating standards that commercial organizations and governments can use to do business internationally. The ISO standards allow entities to provide their customers and government regulators assurance that the operating entity meets international expectations for operating compliance with regulation and quality assurance of production standards. The ISO has expanded its standard setting to include certain organizational and managerial activities, such as information security.

Information security standards are *ISO/IEC 17799, 13335* and *15408*. ISO/IEC 15408 has a narrow focus of Evaluation Criteria for Information Technology Security. ISO/IEC 13335 deals with guidelines for the management of information technology security, while ISO/IEC 17799 addresses the Code of Practice for Information Security Management. The Commonwealth's information security standards reference this last standard, ISO/IEC 17799, as the best practice standard.

US National Institute of Standards and Technology (NIST)

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the United States' economy and public welfare by providing measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national-security-related information in federal information systems. Also known as the *Special Publication 800 series, or SP 800 series of documents*, they report on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

These SP 800 series reports provide general guidance and some detail on various parts of an information security program. Each different SP 800 report deals with a specific topic, for example, SP 800-18 addresses Developing Security Plans for Federal Information Systems, SP 800-30 addresses Risk Management for IT Systems, and SP 800-26 is a Security Self-Assessment for IT Systems.

Information Systems Audit and Control Association (ISACA)

Information Systems Audit and Control Association (ISACA) is an organization of information security professionals that promotes the development of sound internal controls and security measures in automated environments. ISACA has issued a companion document to the COSO guidance that specifically addresses information security programs. This document is a comprehensive IT security standard, known as the Control Objectives for Information and related Technology (COBIT).

COBIT provides both a framework for the information security program, and also provides specific details of what constitutes a sound program. We provide below some the general information on the structure of COBIT.

COBIT Governance Issues

For many enterprises, information and the technology that supports it represent their most valuable, but often least understood assets. Successful enterprises recognize the benefits of information technology and use it to drive their stakeholders' value. These enterprises also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on IT. Many enterprises now understand the need for assurance about the value of IT. The management of IT-related risks and increased requirements for control over information are key elements of enterprise governance. Value, risk, and control constitute the core of IT governance.

IT governance is the responsibility of executives and the board of directors and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.

Furthermore, IT governance integrates and institutionalizes good practices to ensure that the enterprise's IT supports the business objectives. IT governance thus enables the enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities and gaining competitive advantage. These outcomes require a framework for control over IT that fits with and supports the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control—Integrated Framework*, the widely accepted control framework for enterprise governance and risk management, and similar compliant frameworks.

Organizations should satisfy the quality, fiduciary, and security requirements for their information, as they do for all assets. Management should also optimize the use of available IT resources, including applications, information, infrastructure, and people. To discharge these responsibilities, as well as to achieve its objectives, management should understand the status of its enterprise architecture for IT and decide what governance and control it should provide.

COBIT Objectives

COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's practices represent the consensus of experts and strongly focus on control and less on execution. These practices will help optimize IT-enabled investments, ensure service delivery, and provide a measure against which to judge when things do go wrong.

For IT to be successful in delivering against business requirements, management should put an internal control system or framework in place. The COBIT control framework contributes to these following needs.

- Making a link to the business requirements
- Organizing IT activities into a generally accepted process model
- Identifying the major IT resources to be leveraged
- Defining the management control objectives to be considered

COBIT Process

The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners.

COBIT is a process model, which subdivides IT into 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help to identify those resources essential for process success, i.e. applications, information, infrastructure, and people. In summary, to provide the information that the enterprise needs to achieve its objectives, a set of naturally grouped processes will manage its IT resources.

US Government Accountability Office (GAO)

The United States General Accountability Office (GAO), Accounting and Information Management Division issued the *Federal Information System Controls Audit Manual (FISCAM)* in January 1999. Federal agencies, Congress, and the public rely on computer-based information systems to carry out agency programs, manage federal resources, and report program costs and benefits. The methodology outlined in FISCAM provides guidance to auditors in evaluating internal controls over the integrity, confidentiality, and availability of data maintained in these systems. The Manual focuses on evaluations of general and application controls over financial information systems that support agency business operations. It also assists in evaluating the general and application controls over computer-processed data from agency information systems, as called for in *Government Auditing Standards: 1994 Revision* (GAO/OCG-94-4), Paragraph 6.62, "Validity and Reliability of Data From Computer-Based Systems."

The first volume is comprised of four chapters, an introduction chapter, a chapter on planning the audit, and two chapters that deal extensively with evaluating and testing general controls and evaluating and testing application controls. The chapter on evaluating and testing general controls has six categories, which closely parallels with COBIT and ISO 17799. The following is a listing of the categories.

- Entity wide security program planning and management
- Access controls
- Application software development and change controls
- System software controls
- Segregation of duties
- Service continuity

For each of these six categories, FISCAM identifies several critical elements that represent tasks that are essential for establishing adequate controls. If the controls for one or more of each category's critical elements are ineffective, then the controls for the entire category are not likely to be effective, putting the audited system's confidentiality, integrity, and availability of data at risk.

Development of Best Practices

As stated earlier in this report, an information security risk is any activity or event that threatens the achievement of identified business objectives by compromising the confidentiality, integrity, or availability (CIA) of data. Organizations are vulnerable to many kinds of information risks inflicting various types of damage, which can result in significant losses. This damage can range from errors harming data integrity to fires destroying entire computer centers.

Therefore, with this objective in mind, we reviewed the information from the four organizations setting standards for information security programs. We found that one issue with the standard setting bodies is the inconsistency of the level of detail in their standards. The level of detail covered all the ground from general strategic planning to questionnaires by process. The graph below, Figure 4, shows the array of how we view the detail and completeness of the various standards.

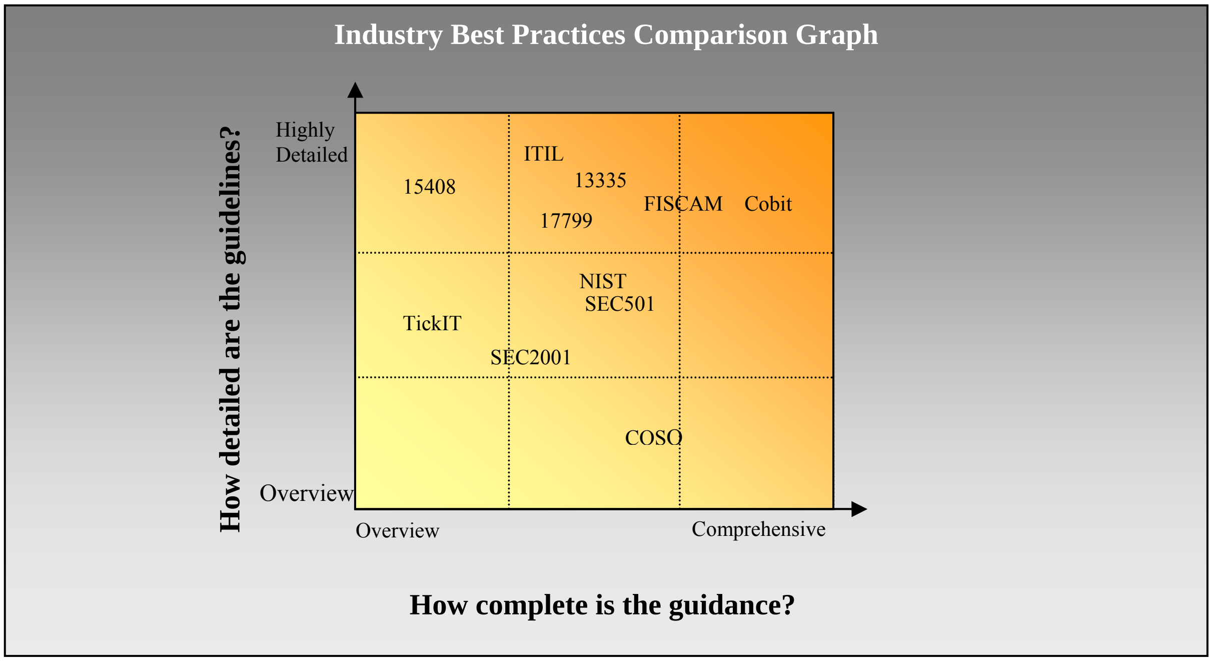


Figure 4 – Industry best practices comparison graph

In order to maximize the usefulness of these standards, we determined that they generally envisioned an information security program that had four general components. We divided each of the general components into more specific areas. We used this classification for two purposes. The first is a detailed analysis of the existing best practices with the Commonwealth standards and secondly, a checklist to evaluate the Commonwealth information security program.

We will discuss the results of our comparison of the best practices with the Commonwealth's standards later in this report. The review checklist is Appendix B.

The following are the four components that the best practices indicate should comprise a sound information security program. Security Management Structure addresses the strategic organizational risks, vulnerabilities, and framework of the program. Data Protection, Integrity, Availability, and Confidentiality are the processes of classification, access, safeguarding, and control of information. Configuration and Change Management address the infrastructure and application process of handling information within the program over time. Monitoring and Logging is the final component of review, follow through and management response.

- Security Management Structure
- Data Protection, Integrity, Availability and Confidentiality
- Configuration and Change Management
- Monitoring and Logging

Under each component are the processes that a good information security program includes. The following has a brief discussion of the processes that occur within these components.

Security Management Structure

- The Security Roles and Responsibilities determine that a security management organizational structure exists within each agency and institution and that proper security oversight and separation of duties exists.

- Security Awareness Training provides instruction to new and current employees and contractors on topics such as the importance of properly protecting and handling sensitive information, the need for password policies and system access controls, and workplace security.

- Data Classification categorizes agency and institution information according to the level of sensitivity with respect to confidentiality, which addresses sensitivity to unauthorized disclosure, to integrity, which addresses sensitivity to unauthorized modification and to availability, which addresses sensitivity to outages.

- Information Assets Inventory determines that each agency and institution maintains a detailed list of their hardware and software as well as a current network diagram.

- A Risk Assessment (RA) verifies that each agency and institution has identified potential threats to the organization as well as its information technology assets, including its data, and the probability and impact of occurrence and the mitigation of these risks.

- A Business Impact Analysis (BIA) identifies each agency's and institution's business functions and supporting resources, delineates those functions considered to be essential, verifies the acceptable loss over time when information systems are inoperable or unrecoverable due to a disaster, and specifies when the Disaster Recovery Plan should be activated.

- A Business Continuity Plan (BCP, also known as Continuity of Operations Plan or COOP) verifies that each agency or institution has identified the steps necessary to plan for and execute resumption, recovery and restoration of business functions and information technology resources and data in the event that an emergency or disaster occurs that renders them unavailable.

- A Disaster Recovery Plan (DRP) verifies that in the event of a natural or man-made disaster, each agency and institution has identified the steps necessary to recover and restore business functions and information technology resources and data on a schedule that supports the mission requirements of that organization.

- Incident Response Procedures (IRP) verify that each agency and institution has identified the steps necessary to properly respond to and resolve suspected or known breaches to established information security safeguards.

Data Protection, Integrity, Availability, and Confidentiality

- Authorization includes each agency's and institution's policies and procedures to control access to their information technology resources that allows use of such resources to only internal and external users that have authority to use them.

- Authentication is the process by which each agency and institution attempts to verify the digital identity of the sender of a communication such as a request to log in to an information system.

- Password Controls include those policies and procedures developed by each agency and institution that establish a set of rules designed to protect information technology resources and data by encouraging their internal and external users to employ strong passwords and use them properly.

- Physical Access includes those policies and procedures established by each agency and institution that identify the controls necessary to safeguard the physical facilities that house information technology resources, data, and personnel.

- Interfaces and Interoperability include those policies and procedures developed by each agency and institution to establish the controls needed to protect data shared with other information systems.

Configuration and Change Management

- Change Management includes those policies and procedures each agency and institution has to identify the controls needed to properly document proposed changes to information system configurations, assess the impact, cost, benefit and risk of these changes, develop justification, obtain approval and manage the testing, implementation and reviewing of the changes.

- Software Change Management includes those policies and procedures established by each agency and institution to identify the controls needed to properly document, manage and maintain the integrity and traceability of the development of the software throughout its life cycle (from project definition through disposition).

- Standard Configurations define and document lists of security settings employed by each agency and institution to safeguard their information systems against potential intrusions.

- Systems Development Life Cycle (SDLC) Security includes the security requirements into each phase of the development life cycle (planning, analysis, design, development, testing, implementation and maintenance) to safeguard the agency and institution's information systems and for each modification proposed to an agency's or institution's information systems.

- Asset Management includes those policies and procedures each agency and institution has to identify the controls to manage and secure the physical information technology assets and the data stored on them and guard against the use of computer software in violation of applicable laws.

Monitoring and Logging

- Monitoring and logging includes those policies and procedures of each agency and institution to identify the controls needed to manage and record the activities that occur on information systems including normal daily activities as well as suspicious or malicious activities.

SECURITY IN THE COMMONWEALTH

Legislation passed in 2003 created the VITA and called for the appointment of a Chief Information Officer (CIO) to oversee the operations of VITA. This legislation requires that the CIO and VITA formulate standards, guidelines, policies, and procedures "for assessing security risks, determining the appropriate security measures, and performing security audits of government databases and data communications" and "for managing information technology by state agencies and institutions."

The CIO has designated a Chief Information Security Officer (CISO) to be responsible for the development of policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth's information systems. In addition, the CIO is required to consider the advice of the Council on Technology Services when developing these policies.

The Commonwealth's IT Security Standards

As of July 1, 2006, VITA issued a new IT security standard (COV ITRM SEC501-01) that requires agency and institution compliance by July 1, 2007. All executive branch state agencies and institutions of higher education must comply with this standard. However, academic information systems used for purposes of research and instruction are exempt from the requirements of this standard. However, these research and instructional systems are not exempt from other state and federal laws.

The Commonwealth standards describe the minimum level of security for information technology in the Commonwealth. Agencies must maintain a security program that meets all aspects of these standards.

Roles and Responsibilities for IT Security in the Commonwealth

VITA and those agencies following the standards each have individual roles in ensuring that the systems have proper security. For this section of the report, the term "state agency" or "agency" is any agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch listed in the appropriation act as defined in the Code of Virginia. However, University of Virginia Medical Center is excluded from these standards.

Role of the Virginia Information Technologies Agency

As previously discussed, the CIO has appointed a CISO to develop standards for IT security. The CISO has the following responsibilities outlined in the Commonwealth's information security policy, ITRM Policy SEC500-02.

- Administer the Commonwealth's IT security program and periodically assesses whether the program's implementation is in accordance with COV IT Security Policies and Standards.
- Review requested exceptions to IT security policies, standards and procedures.
- Provide solutions, guidance, and expertise in IT security.
- Maintain awareness of the security status of sensitive IT systems.
- Facilitate effective implementation of the state's IT Security Program, by accomplishing the following:
    - Preparing, disseminating, and maintaining IT security, policies, standards, guidelines and procedures as appropriate
    - Collecting data relative to IT security in the Commonwealth and communicating as needed
    - Providing consultation on balancing an effective IT security program with business needs
- Provide networking and liaison opportunities to Information Security Officers (ISOs).

Role of Agencies

Agency heads play a large role in ensuring that agencies have sufficiently secured the collected and stored data. ITRM Policy SEC500-02 has the following definition of the IT security responsibilities for agency heads.

- Designate an Information Security Officer (ISO) for the Agency, and provide that person's name, title and contact information to VITA no less than biennially. The Agency Head is strongly encouraged to designate at least one backup for the ISO, as well.

- Determine the optimal place of the IT security function within the Agency hierarchy with the shortest practical reporting line to the Agency Head.

- Maintain an IT security program that has sufficient documentation and communicated to staff to protect the Agency's IT systems.

- Review and approve the Agency's Business Impact Analyses (BIAs), a Risk Assessment (RA), and a Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable.

- Accept residual risk.

- Maintain compliance with IT Security Audit Standard (COV ITRM Standard SEC507-00). This compliance must include, but is not limited to:

    - Requiring development and implementation of an Agency plan for IT security audits, and submitting this plan to the CISO;

    - Requiring that the planned IT security audits are conducted;

    - Receiving reports of the results of IT security audits;

    - Requiring development of Corrective Action Plans to address findings of IT security audits; and

    - Reporting to the CISO all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.

- Facilitate the communication process between data processing staff and those in other areas of the Agency.

- Establish a program of IT security safeguards.

- Establish an IT security awareness and training program.

- Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

The Information Security Officer (ISO) is responsible for the most critical aspects of the agency's security program. The ISO responsibilities include the following:

- Develop and manage an IT security program that meets or exceeds the requirements of the Commonwealth's IT security policies and standards in a manner commensurate with risk.

- Develop and maintain an IT security awareness and training program for Agency staff, including contractors and IT service providers.

- Coordinate and provide IT security information to the CISO as required.

- Implement and maintain the appropriate balance of protective, detective, and corrective controls for agency IT systems commensurate with data sensitivity, risk, and systems criticality.

- Mitigate and report all IT security incidents in accordance with Section 2.2-603 of the Code of Virginia and VITA requirements and take appropriate actions to prevent recurrence.

- Maintain liaison with the CISO.

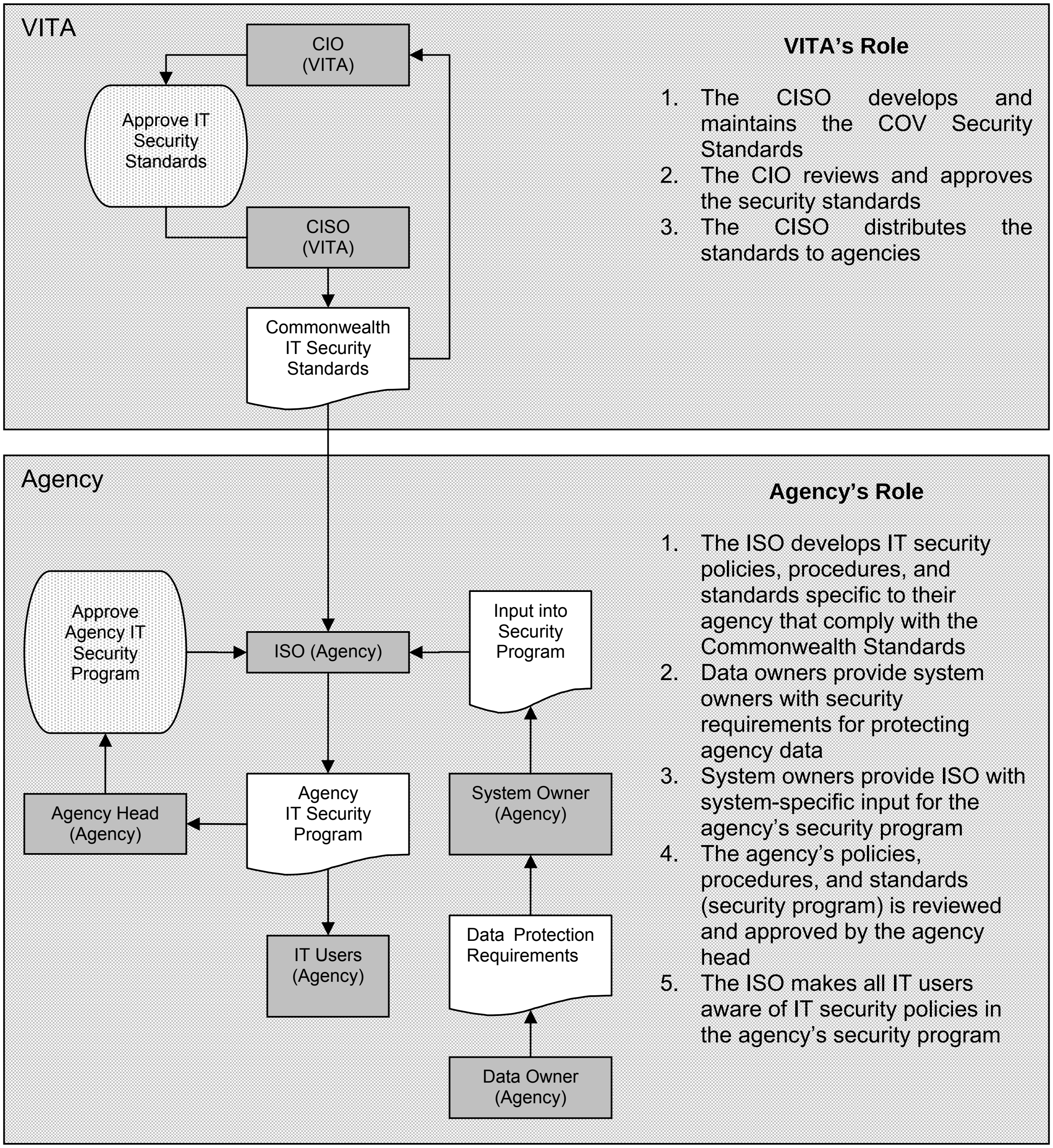
The following responsibilities are also the duty of the ISO unless the agency appoints a Privacy Officer as required by the Health Insurance Portability and Accountability Act (HIPAA). The Privacy Officer has the following responsibilities:

- Meet the requirements of state and federal privacy laws.

- Prevent disclosure of and access to sensitive data.

- Meet security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Figure 5 summarizes the Commonwealth's process of developing statewide standards and agency policies.


VITA
CIO (VITA)
Approve IT Security Standards
CISO (VITA)
Commonwealth IT Security Standards
Agency
Approve Agency IT Security Program
ISO (Agency)
Input into Security Program
Agency Head (Agency)
Agency IT Security Program
System Owner (Agency)
IT Users (Agency)
Data Protection Requirements
Data Owner (Agency)

VITA's Role

1. The CISO develops and maintains the COV Security Standards
2. The CIO reviews and approves the security standards
3. The CISO distributes the standards to agencies

Agency's Role

1. The ISO develops IT security policies, procedures, and standards specific to their agency that comply with the Commonwealth Standards
2. Data owners provide system owners with security requirements for protecting agency data
3. System owners provide ISO with system-specific input for the agency's security program
4. The agency's policies, procedures, and standards (security program) is reviewed and approved by the agency head
5. The ISO makes all IT users aware of IT security policies in the agency's security program

Figure 5 – Policies and Standards development process in the Commonwealth

Exceptions to the Commonwealth IT Security Standards

Agencies and institutions of higher education are required to comply with all standards issued by the CISO. However, in certain business environments, agencies and institutions may require exceptions to these standards. In those cases, an agency head must submit an exception request to the CISO. This exception request must include the following information for the exception:

1. The business need
2. The scope and extent of the exception
3. The controls in place to mitigate the risk of not following the standard
4. The specific duration of the exception
5. Agency head approval

CISO evaluates the need for the exception and either approves or denies the exception. If CISO denies the exception, there is an opportunity to appeal the decision to the CIO via the CISO. Some agency systems are automatically exempt from the IT Security Standards. Those systems have the following characteristics:

- Systems under development or experimental systems not in use in the daily business processes

- Surplus or retired systems no longer used in the daily process

- Systems for instruction or research

- University of Virginia Medical Center systems

The Commonwealth's Approach to Information Security

Currently, the Commonwealth takes a "silo" approach to information security. The executive, legislative, and judicial branches do not have a high-level Commonwealth (or enterprise) wide information security program. As a result, each branch, and in turn, each agency, interprets and implements information security differently. This approach leads to an inconsistent implementation of information security across the Commonwealth's agencies and institutions.

In particular, the Commonwealth does not mandate a basic information security program for the judicial and legislative branches. The agencies and institutions within these branches establish their own information security programs without any guidance or minimum requirements. These agencies and institutions for the most part, however, do use the standards set by the CIO as a baseline.

Commonwealth Statistic
Surveyed agencies and institutions with an adequately documented information security program:
20%

The Commonwealth mandates the Information Technology Investment Board (ITIB) and CIO, whom in turn have directed VITA, to establish policies, procedures, and standards for executive branch agencies. Figure 6 illustrates the entity responsible for the development and implementation of information security programs in each of the branches of Virginia state government.

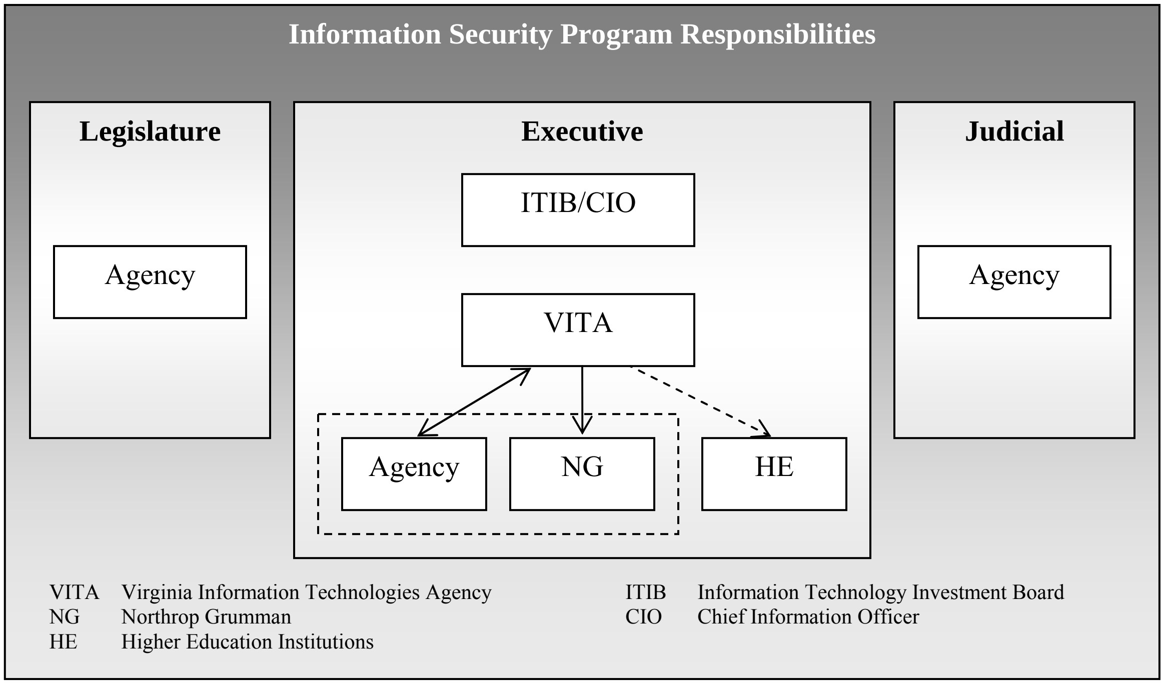

Information Security Program Responsibilities
Legislature
Agency
Executive
ITIB/CIO
VITA
Agency
NG
HE
Judicial
Agency
VITA Virginia Information Technologies Agency
NG Northrop Grumman
HE Higher Education Institutions
ITIB Information Technology Investment Board
CIO Chief Information Officer

Figure 6: Information Security Program Responsibilities

The agencies within the legislature and judicial branches have responsibility for both the infrastructure layer (hardware) and the application layer (software) of information security. These agencies' direct oversight of their own infrastructure, which is limited to the equipment directly under their control, however, these agencies are also extensive users of the Commonwealth's infrastructure managed by Northrop Grumman and their application. This approach makes it more difficult for these agencies to manage their information security programs.

In the executive branch, the Code of Virginia mandates the ITIB and the Commonwealth's CIO to "direct the development of policies, procedures, and standards for assessing security risks, determining the appropriate security measures and performing security audits." The CIO has charged VITA with the task of developing the information security program for the executive branch. The executive branch includes most Commonwealth agencies and institutions of higher education.

Unlike the legislature and the judicial branches, the executive branch agencies are only directly responsible for part of the application layer of information security. However, in a public-private partnership, the Commonwealth has outsourced the management of the infrastructure layer and parts of the application layer to Northrop Grumman. This introduces another level of complexity for the Commonwealth in creating and maintaining its information security programs, since a third party, Northrop Grumman, manages the executive branch agencies' infrastructure layer of information security.

Layers of Information Security

An information security program should also consider the layers of information security. The "layers of information security" refers to the co-dependency between the infrastructure and application layers in an information systems environment. It is important that an information security program address information security risks associated with each layer of information security, in a holistic and detailed level, in order to prevent a security risk in one layer from impacting another layer.

The infrastructure, or physical, layer consists of the hardware that allows users to access, store and transfer information. Hardware includes personal computers, servers, network cabling, routers and switches. The application, or logical, component consists of the software that allows users to interact with the information that is stored or transferred throughout the infrastructure.

There is a clear co-dependency between the two layers. Applications cannot function without an infrastructure, and vice-versa. Thus, it is essential to consider both layers in an information security program. This means that insufficient information security controls around the infrastructure inherently introduces an information security weakness in the application component.

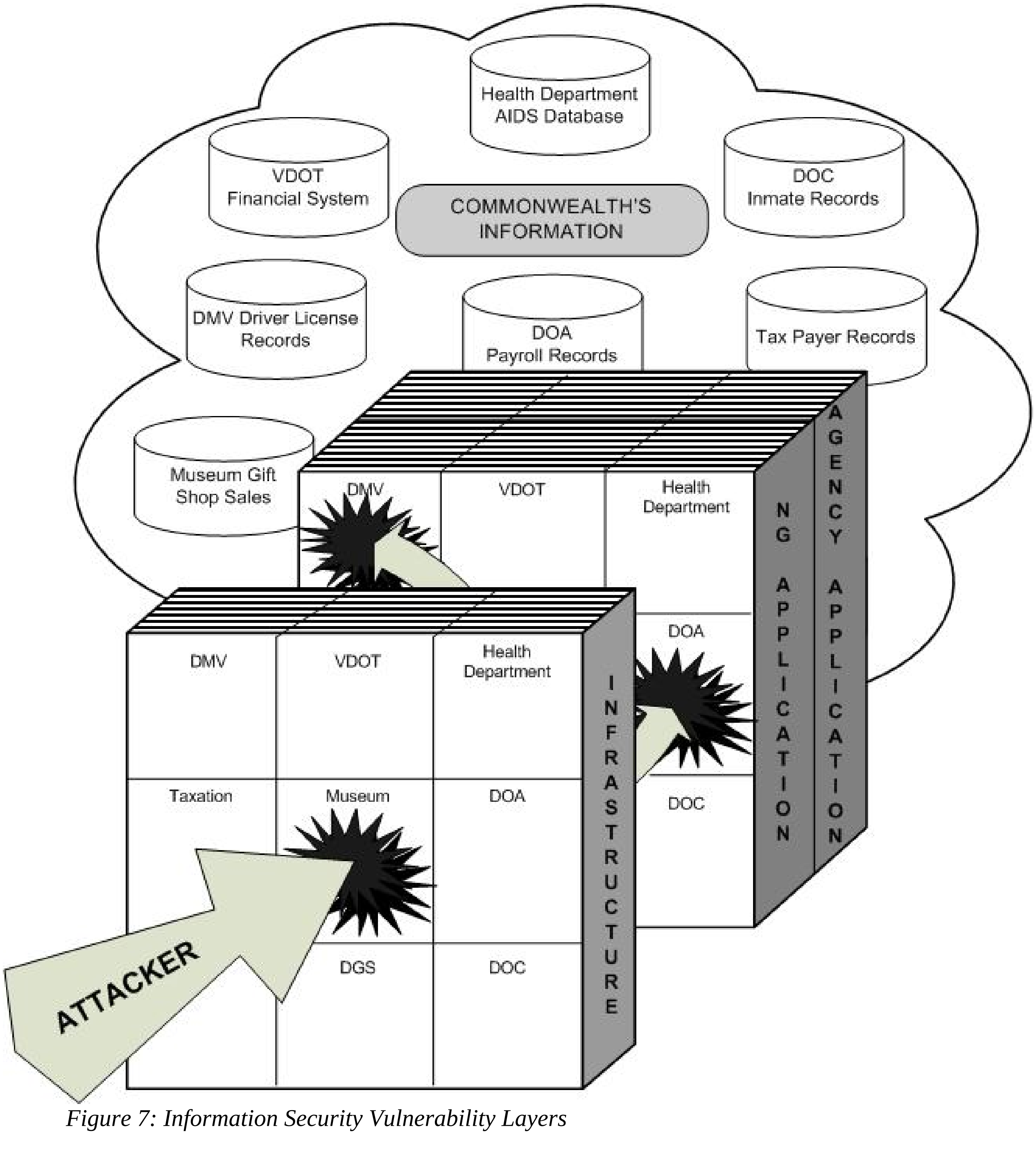


Figure 7: Information Security Vulnerability Layers

The preceding figure illustrates how an attacker can gain access to information by taking advantage of poor information security controls at either of the two layers. In this hypothetical example, an attacker breaks through a poorly configured information system at a museum. Once the attacker has gained access to the Northrop Grumman network that hosts the museum's IT applications, the attacker can use trusted relationships between the museum and other state agencies, for example, the Department of Accounts. Thus, the attacker can use weaknesses in the infrastructure and application controls managed by Northrop Grumman in order to open the front door to applications and information controlled by executive branch agencies.

Without clearly written and communicated policies, procedures, and standards this hypothetical scenario could become a future case study. Agencies have a responsibility to communicate their information security needs to VITA, which in turn will ensure that Northrop Grumman meets those responsibilities. VITA should also work with agencies to ensure compliance with the Commonwealth's policies, procedures, and standards.

The Northrop Grumman Partnership

On July 1, 2006, Northrop Grumman took responsibility for the operations and management of all IT infrastructure components, such as desktops, servers, mainframes, and routers for agencies that VITA serves. VITA, the CIO, and the Information Technology Investment Board (ITIB) continue to retain responsibility for the Commonwealth's IT security governance as required by the Code of Virginia.

VITA's contract with Northrop Grumman clearly recognizes the CIO, ITIB, and VITA's responsibility for IT security. The contract includes language noting that VITA will give Northrop Grumman clear direction regarding the security standards and controls that the Commonwealth needs and requires. Northrop Grumman will use that information to ensure their operations and management meets the Commonwealth's security standards and controls. The contract also provides for Northrop Grumman to submit to an annual infrastructure audit, periodic security audits, and other audits as deemed necessary by VITA. These audits will include an examination of whether or not Northrop Grumman is meeting the security standards and controls that VITA has set.

We have issued several reports on VITA since they took over the management and operations of the Commonwealth's infrastructure in 2003. These reports expressed concerns that VITA had little understanding of the IT security requirements beyond the old Department of Information Technology data center. Our recommendations to VITA encouraged them to collect information about agency specific security needs.

Once collected, our reports encouraged VITA to analyze the information and set minimum-security configurations for the equipment they managed. We recommended VITA communicate those minimum configurations to agencies so they could assess how the configurations would impact the security they required. In addition, we recommended that VITA improve their communication with agencies regarding what security areas VITA was responsible for and what areas the agency controlled.

With the exception of a few large agencies such as the Departments of Taxation and Transportation, VITA had collected little information about agency security requirements. Most recently our April 2006 report titled, "Review of Information Technology Governance and Virginia Information Technologies Agency Operations," continued to note concerns that VITA did not have adequate IT security information beyond their data center. We were concerned that the operations and management of the infrastructure would transfer to Northrop Grumman on July 1, 2006, without any formal communication of the Commonwealth's security requirements.

Since issuing our report, Northrop Grumman took over the Commonwealth's infrastructure management and operations and VITA initially provided them only minimal information on the security requirements beyond the VITA data center. Since transition, VITA and Northrop Grumman have been working together to collect security information and set minimum-security standards. For example, in early spring 2006, VITA sent an information security template to agencies requesting them to identify sensitive/critical applications and provide a variety of information such as specific laws surrounding data collected by the application. Although not every agency responded to VITA's request, and many did so after the additional deadline, the collection of this type of information by VITA is a starting point to understanding the security requirements of applications that run on the Northrop Grumman infrastructure.

Recently, Northrop Grumman set out an initial list of 10 infrastructure standards that they will follow such as server backup, virus protection, and system patches. We believe these security standards are a start and encourage their continued development. We are concerned, however, that VITA has not communicated these standards to agencies, nor have they developed a plan to communicate them.

Under the Commonwealth's IT Security Standard, agencies are responsible for developing an information security program. Agencies need information about Northrop Grumman's infrastructure and standards to fully evaluate and consider infrastructure risks and vulnerabilities on which their applications and sensitive information runs. Without considering the infrastructure, agency-based information security programs will be incomplete and may be inadequate.

RECOMMENDATION 1:

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

Comparing Commonwealth's Standards to Best Practices

Overall, the Commonwealth's standards do address most of the components found in the best practices. The difference between the Commonwealth standards and the best practices, for the most part, occurs within the processes of the components.

As stated earlier we have developed a *Best Practices Information Security Program* using the resources noted earlier in the report. We have just discussed the development of the Commonwealth's Information Security standards. Following is a discussion of the difference between the Commonwealth Standards and Best Practices. The comparison in this report uses SEC 501 and industry best practices. As of July 1, 2007, SEC 501 will become the Commonwealth's standard and the ITIB and the CIO will have the opportunity to decide whether to address some of these differences in amendments to SEC 501.

Policy Consideration

Historically, the Commonwealth, like other governmental entities, has a constitutional separation of powers between the Executive, Judicial, and Legislative branches. In Virginia, this separation includes independent agencies and institutions of higher education.

Best practices assume a single authority has overall responsibility for the information security programs. The CIO's authority for security includes only executive branch agencies and institutions of higher education. While the CIO does not have explicit authority over the legislative and judicial branches, these agencies have elected to comply with the Commonwealth's information security program.

The other issue the comparison could not address is the organizational issue that divides information security programs within the Commonwealth between the agencies and VITA. The division of responsibilities does create both confusion and risk in evaluating individual information security programs. In order to resolve this issue, VITA and the agencies must develop joint mutually dependent information security programs that merge into one program within the agency and an information security program addressing all the concerns of protecting information.

RECOMMENDATION 2:

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

We found fifteen processes that best practices indicate should exist within the information security program, but were not found in the Commonwealth's security standards. Below, we discuss the detailed differences between the best practices and the Commonwealth's security standards. Please refer to Appendix B for a comparison of the best practices in matrix form. Following, we provide the process difference and explain its purpose within the information security program.

1. The Commonwealth's standard does not have a requirement that the agency has an organizational chart that lays out the reporting structure of its employees involved with information security.

   Purpose: To ensure the appropriate reporting structure of an agency's information security officers.

2. The Commonwealth's standard does not have a requirement that each agency has a committee that oversees the security plan.

   Purpose: To ensure that the management and the information security officer(s) of an agency communicate changes and periodically evaluate their security program to review the effectiveness of its implementation.

3. The Commonwealth's standard does not empower the agency Information Security Officer (ISO) to deny requests that do not fall in-line with the security plan.

   Purpose: The agency Information Security Officer should have the authority to formally assume responsibility for operating an information system at an acceptable level of risk to the agency operations, assets, or individuals. As such, the ISO should have the following responsibilities related to the agency's information security plan.

   - Approve system security plans
   - Authorize operation of an information system
   - Issue interim authorization to operate an information system under specific terms and conditions
   - Deny authorizations to operate the information system if unacceptable security risks exist

4. The Commonwealth's standard does not require that an agency's senior management approve data classifications, review them periodically, or communicate them to the data owners or end-users.

   Purpose: Periodic review of data classifications is necessary as risk assessments and business impact analyses change._ The senior management shall review, approve, and communicate data classifications, as they are ultimately responsible for the security of information in their possession.

5. The Commonwealth's standard does not require that agencies document and periodically review a list of its hardware and software assets.

   Purpose: To ensure that the agencies have information technology hardware and software assets documented in the event of a disaster.

6. The Commonwealth's standard does not require updated network diagrams or the designation of a network administrator responsible for updating such diagrams.

   Purpose: Updated network diagrams ensure identification of possible infrastructure vulnerabilities and identification and location of equipment.

7. The Commonwealth's standard does not require the involvement of the data and systems owners in the Business Impact Analysis (BIA) process.

   Purpose: Involvement of the data and systems owners in the BIA process is necessary to ensure that the data and system owners' concerns are considered.

8. The Commonwealth's standard does not require agencies' disaster recovery plans to include the manual processing procedures for critical functions that users can follow until the agency restores operations.

   Purpose: Manual-processing procedures ensure continued operation of agencies' functions and processes after a disaster.

9. The Commonwealth's standard does not require agencies to have policies and procedures that approve and remove authorization for vendors and third parties.

Purpose: Policies and procedures that approve and remove authorization for vendors and/or third parties are necessary to lessen the risk of unauthorized access to information.

10. The Commonwealth's standard does not require the documentation or review of employee job descriptions that accurately reflect assigned duties and responsibilities.

Purpose: Accurate reflection and review of assigned duties and responsibilities in an employee's job description ensures accurate segregation of duties.

11. The Commonwealth's standard does not require the documentation of requests and approvals of emergency or temporary access on a standard form and maintained on file, approved by appropriate manager, security communicated to the security function, and automatically terminated after a predetermined period.

Purpose: Formalization of granting emergency or temporary access lessens the risk of unauthorized access.

12. The Commonwealth's standard does not require vendor supplied (default) passwords be changed immediately after installation.

Purpose: Changing vendor supplied (default) passwords immediately after installation lessens the risk of unauthorized access.

13. The Commonwealth's standard does not require management to periodically review the list of persons allowed physical access to sensitive resources.

Purpose: Access to sensitive resources should be limited to personnel with legitimate need for access to perform their job duties.

14. The Commonwealth's standard does not require authorization and logging of deposits and withdrawals of all media that is stored off-site.

Purpose: Authorization and logging of deposits and withdrawals lessens the risk of third party compromising information.

15. The Commonwealth's standard does not require documented security agreements between two parties (agencies) to include any mandated requirements, such as HIPAA, if applicable.

Purpose: The Commonwealth is required to follow federal information security laws, such as HIPAA.

RECOMMENDATION 3:

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

Evaluation of the Commonwealth's Information Security Programs

In order to evaluate and analyze the state of information security programs in the Commonwealth, we developed a comprehensive Information Systems Security Checklist (see Appendix C). This checklist was our tool to determine the level of information security implemented by agencies and institutions.

The checklist consists of the four components of a sound information security program from our best practices work. Within each of the components, a series of detailed questions addressed each of the processes.

- Security Management Structure
- Data Protection, Integrity, Availability, and Confidentiality
- Configuration and Change Management
- Monitoring and Logging

In developing the checklist, as stated earlier, we were aware that differences existed between best practices and the current Commonwealth security standard (SEC 501-01); however, we included the missing items in our checklist, but excluded them from our evaluation of the agency's and institution's overall evaluation in Appendix A.

We planned for agencies to use the checklist as a tool in gathering information on their information security program. The checklist would serve as a guide for reviewing the information, since it followed the components of the best practices for information security programs. Finally, the checklist would provide a more uniform mechanism for reviewing and evaluating the individual programs and comparing those programs among the various agencies and institutions.

We selected a small number of agencies and institutions that served as a pilot group. The pilot group consisted of agencies and institutions of varying budget size, number of employees, computer systems, and sensitivity of information. The pilot agencies executed the checklist and our personnel reviewed and evaluated the results. Based on the comments and recommendations made by the pilot group including both agency personnel and our auditors, we refined the checklist for use during the review.

We determined that, statewide, there were 104 agencies and institutions in the executive, legislative, and judicial branches that should have control of information security programs. Certain agencies manage their information security programs centrally for their affiliated agencies. For example, the Department of Corrections centrally manages and provides information security governance of all Corrections' facilities. In these cases, only the agency providing governance completed the checklist.

Analyzing the Checklist Results

Information security programs are generally inadequate and do not address both the business needs and risks associated with not controlling that information. The Commonwealth, however, has several agencies and institutions such as the Departments of Taxation and General Services and the three largest institutions of higher education, University of Virginia, Virginia Commonwealth University, and Virginia Polytechnic Institute and State University, which provide working models of the best practices of information security programs.

All state agencies and institutions have some type of security over their information technology infrastructure and systems. The security in most cases provides coverage over information existing within the agency. Further, almost all agencies and institutions have at least some plan to recover from a disaster; however, this plan in many cases does not extend to how and under what circumstances.

The Auditor of Public Accounts has been conducting security reviews of financial system for over a decade and reporting our findings. This review's results are consistent with our previously reported findings. With the exception of smaller agencies without financial systems, we have previously issued or commented on all the agencies with either no or inadequate information security programs.

Critical Evaluation Factors

Fundamental to an effective information security program is having conducted the Risk Assessment, Business Impact Analysis, and Business Continuity Plan. If these three items have either not been performed or are out of date, the entire information security program will not function, since it will not address the entity's needs.

These assessments identify the critical information and risks to the agency and help management set priorities on how to fund and protect information. Regardless of all the planned and unplanned security measures taken, these assessments direct management's attention to developing the proper controls.

As stated above, we have a number of state agencies, which have instituted some security controls, but have not done any assessments or have outdated assessments. Some experts compare this approach to security to being the equivalent of paying for a home alarm system, but leaving your valuables in the open back yard. You have security, but you are not protecting your valuables.

Another major factor in evaluating an information security program is the emphasis management places on the information security program. Management's emphasis can take numerous forms, but the most important issues are the placement within the organization, commitment to training, a commitment to problem resolution, and finally the commitment of resources to maintain the program.

If management is not committed to the information security program or is overriding the controls then any program would be truly ineffective. We placed high emphasis on management's commitment to information security in our overall evaluation of the checklist results.

Our final critical evaluation factor was the information security program and management's steps to minimize human failure. No workable system can prevent human failure that overrides the entire system. As stated Virginia Commonwealth University has one of the best information security programs in the Commonwealth, however, students have failed to follow the program and sensitive information has been inappropriately released. We considered how the program addressed these issues and management's commitment to resolve these actions in a timely and direct manner.

Rating the Information Security Programs

We compiled the results of all the Checklists and our review into a database for analysis. We have analyzed the results of the checklist and classified each agency's information security program as "None," "Inadequate" or "Adequate."

Below is our discussion of the evaluation rankings.

- No Information Security Program Criteria:

  The agency or institution did not have any of the basic documents required to perform a security assessment. If none of the four security assessment documents, (the business impact analysis, the risk analysis, the continuity of operations plan, or the disaster recovery plan) are available, the agency cannot correctly establish an information security program.

- Inadequate Information Security Program Criteria:

  If an agency has begun the process of evaluating their state of security, they have an inadequate information security program. An agency must have at least one of the four security assessment documents, (the business impact analysis, the risk analysis, the continuity of operations plan, or the disaster recovery plan), in order to be considered inadequate.

- Adequate Information Security Program Criteria:

  In order for an agency to have an adequate security program, they must have performed a full security analysis of the information within the agency as well as have some security controls over the information. The full security analysis must include completion of the four security assessment documents, (the business impact analysis, the risk analysis, the continuity of operations plan, and the disaster recovery plan). The additional security controls come from selected questions within the security survey. At a minimum, the agency or institution needed the following.

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

Analyzing the Checklist

Overall, we found 83 of the 104 agencies and institutions had effectively either no or an inadequate information security program. However, almost all of the agencies and institutions, which regularly accumulate information from citizens, have adequate information security programs such as the Department of Taxation.

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

General Observations

In reviewing the results, the reason for the inadequate programs in larger agencies, when considering either number of employees or agency budget, appears to center around the resolution of who has responsibility for the infrastructure between VITA and the agency. The larger institutions of higher education with inadequate programs typically do not have the proper managerial placement of the program at the appropriate level for the organization, although this does occur in other agencies.

In reality, the role of the Information Security Officer throughout agencies in the Commonwealth is highly diverse. Largely due to resource restraints, the requirement of the Commonwealth's security standard to designate an agency's resource as an ISO often forces small to medium-sized agencies to assign a staff member that does not necessarily have the correct training, expertise, qualifications, or authority to perform the duties described above effectively.

The development and maintenance of an information security program requires expertise and significant training. In addition, it is not feasible for small to medium-sized agencies to train one of their own staff members to perform this duty. Therefore, the expertise and trained IT professionals at VITA can greatly help in leveraging the cost in the development of agencies' information security programs.

Expertise and Resources

In determining the reason for the lack of an information security program or its inadequacies, we have concluded that an agency's size and resources directly impact its ability to complete an adequate information security program. Below are three analyses that compare number of employees, whether the agency is under VITA's infrastructure, and the agency operation budgets.

Number of Employees

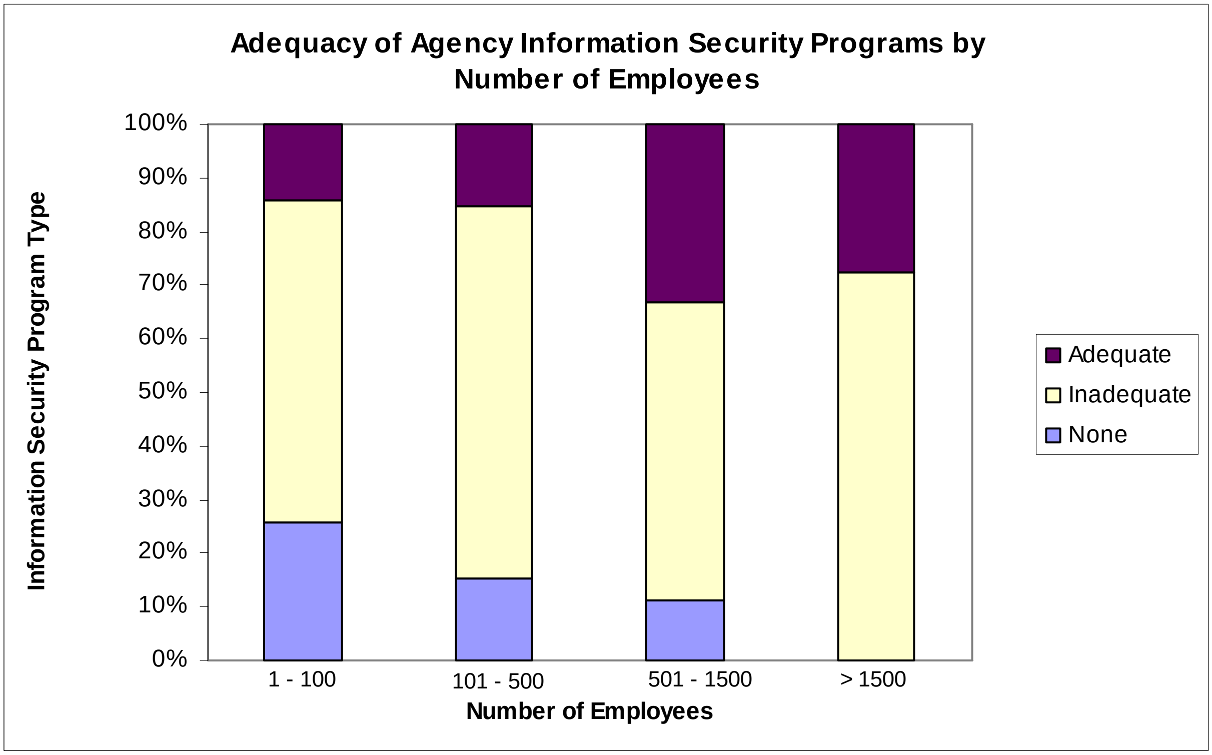
We have compared whether the number of employees within the agency could affect the adequacy of the information security program. We grouped the agencies and institutions results into the following categories.

1. Less than 100 employees
2. 100 to 500 employees
3. 501 to 1500 employees
4. More than 1500 employees

Historically, agencies and institutions with a higher number of employees have provided direct services to citizens and, therefore, have a history of having information systems to gather data. Even with the creation of VITA, these agencies and institutions have continued to maintain their internal information technology systems. These agencies therefore have internal staff, which understand the need for an adequate information security program and can consult with internal management on the program.

The results indicated agencies and institutions with more employees generally have stronger information security programs. After considering the VITA infrastructure and managerial placement of the information security program, we believe most of the larger agencies and institutions would move from inadequate to adequate.

Information Security Program	**Agency Employee Count**			
	< 100	**100 to 500**	**501 to 1500**	**> 1500**
None	26%	15%	11%	0%
Inadequate	60%	70%	56%	72%
Adequate	14%	15%	33%	28%

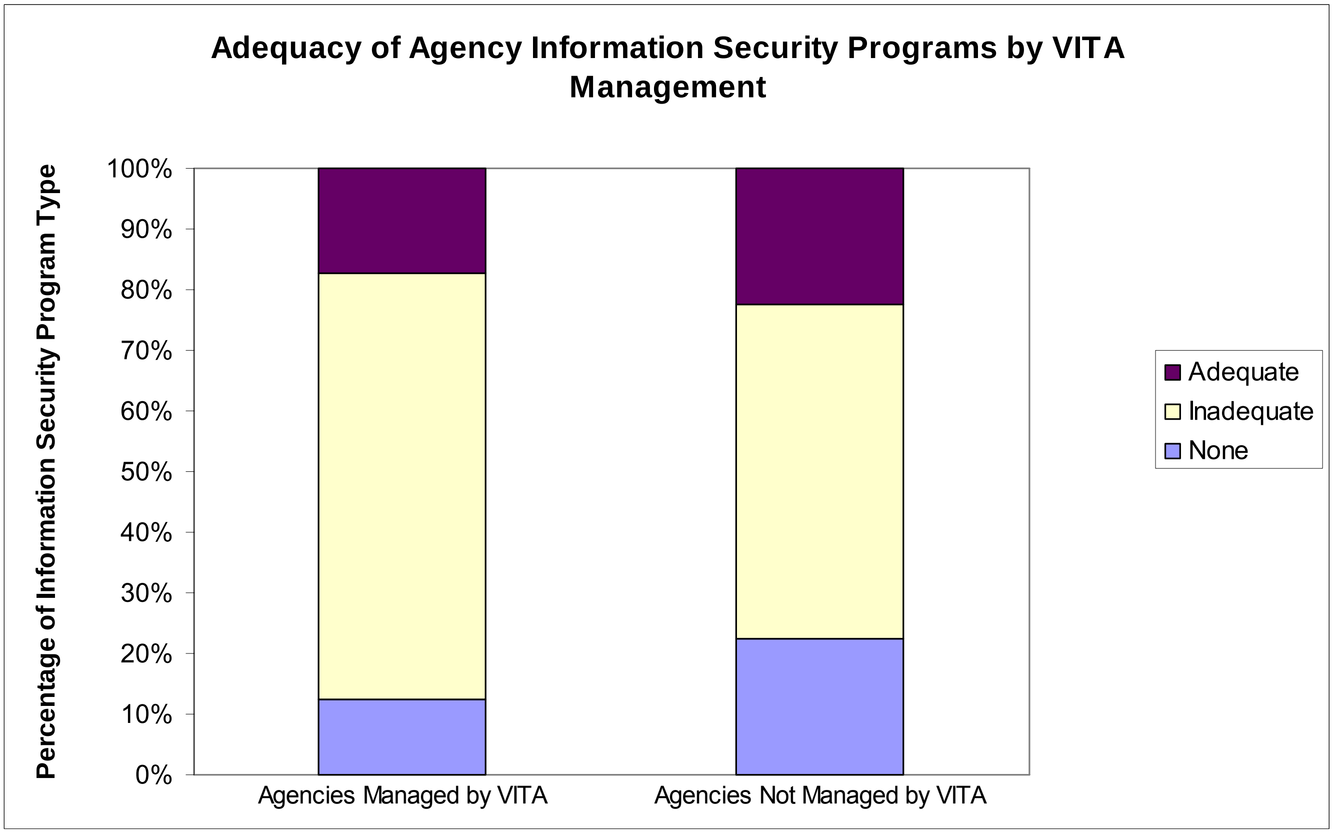


Infrastructure Managed By VITA

A comparison of the adequacy of information security programs of VITA and non-VITA managed agencies and institutions showed no significant difference. Managing an information security program without a third, party should make implementing and controlling the program simpler. However, as shown by the information below there is no significant difference.

We believe that as VITA and the agencies resolve the issue of infrastructure security responsibilities that the comparison in the future will show that these agencies will have improved security programs.

Information Security Program	Agency Managed by VITA	Agency Not Managed by VITA
None	13%	23%
Inadequate	70%	55%
Adequate	17%	22%

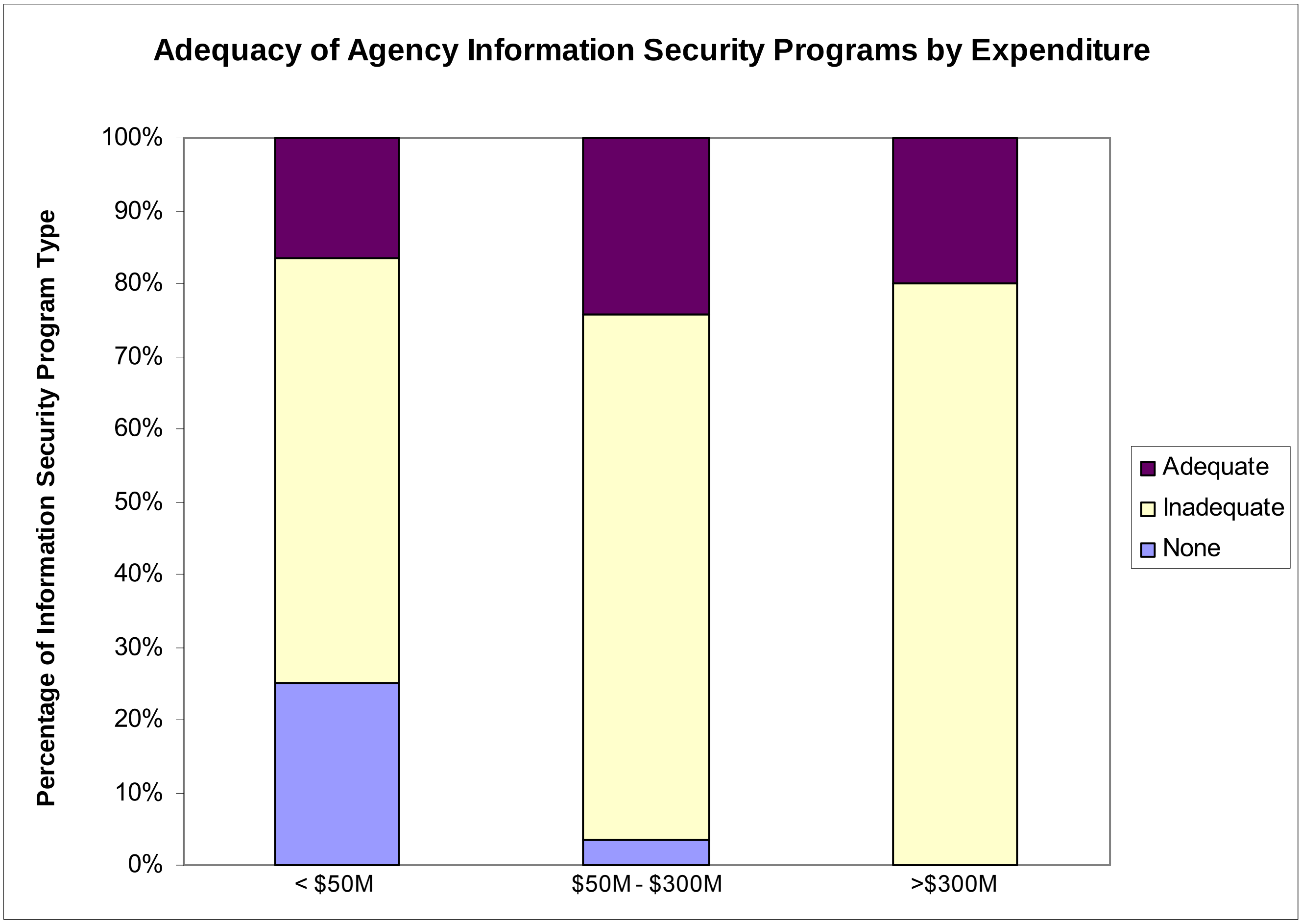


Total Budget

The final analysis compares the adequacy of agency information security programs to its available resources. Like the comparison with number of employees, those agencies and institutions with larger budgets are regularly providing services directly to citizens and may have more complex computer systems to support them. In addition, since they have had this experience, their information security programs would be stronger.

Again, as with the employee analysis, the inadequacy of programs in larger budget agencies is not a resource issue generally, but the broader issue to VITA and the management structure. Our analysis again indicates that the resolution of the two broader previously mentioned issues are likely to move the inadequate programs to adequate.

Information Security Program	Expenditures		
	< $50 M	$50M to $300M	> $300M
None	25%	4%	0%
Inadequate	58%	72%	80%
Adequate	17%	24%	20%



What prevents the larger agencies and institutions from having adequate information security programs are structural issues of infrastructure responsibilities and managerial placement of the program within the organization. However, the same is not the case for the smaller agencies. These agencies and institutions do not have the internal resources or expertise to either develop or maintain an adequate information security program.

Providing these agencies and institutions with the expertise and resources on an individual basis is neither cost effective nor prudent. These agencies and institutions individually cannot attract and retain the quality of staff to do this work. Providing resources would create an expectation that management could redirect funding in the future.

As shown earlier in this report, these agencies not having adequate information security programs could place the entire Commonwealth system at risk. An independent group should assume responsibility for the information security programs and have the authority to implement them within the agencies and institutions. We believe this is the most cost effective approach to minimizing this risk.

RECOMMENDATION 4:

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

OVERALL CONCLUSION

Information security programs are generally inadequate and do not address both the business need and risk associated with not controlling information. The Commonwealth however has several agencies and institutions such as the Department of Taxation and General Service and the three largest institution of higher education, University of Virginia, Virginia Commonwealth University and Virginia Polytechnic Institute and State University, which provide working models of the Best Practices of Information Security Programs.

All state agencies and institutions have some type of security over their information technology infrastructure and systems. The security in most cases provides coverage over information existing within the agency. Further, almost all agencies and institutions have at least some plan to recover from a disaster; however, this plan in many cases does not extend to how and under what circumstances.

The Auditor of Public Accounts has been conducting security reviews of financial system for over a decade and reporting our findings. This review's results are consistent with our previously reported findings. With the exception of the smaller agencies without financial systems, we have previously issued or commented on all the agencies with either no or inadequate information security programs.

In reviewing the results, the reason for the inadequate program in the larger agencies when considering either number of employees or agency budget appears to center around the resolution of who has responsibility for the infrastructure between VITA and the agency. The large institutions of education with inadequate programs typical do not have the managerial placement of the program at the appropriate level for the organization, although this does occur in agencies.

Overall, the Commonwealth's standards do address most of the components found in the best practices. The difference between the Commonwealth standards and the best practices, for the most part, occurs within the processes of the components.

We believe the large agencies and institutions can address our recommendations without significant operational changes. However, the Commonwealth will need to develop and implement a process for provide information security programs for smaller agencies and institutions.

Finally, the General Assembly may wish to amend the Code of Virginia to provide for the audit of information security programs, rather than database and data communication. The current statute does not address the real risk to the Commonwealth.

RECOMMENDATION SUMMARY

RECOMMENDATION 1:

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

RECOMMENDATION 2:

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

RECOMMENDATION 3:

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

RECOMMENDATION 4:

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

Commonwealth of Virginia

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Walter J. Kucharski, Auditor

December 1, 2006

The Honorable Timothy M. Kaine
Governor of Virginia
State Capitol
Richmond, Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

We have completed our review of the **Security of State Government Databases and Data Communications from Unauthorized Uses** as required by Senate Joint Resolution No. 51 of the 2006 Acts of Assembly and submit our report entitled, "A Review of the Information Security in the Commonwealth of Virginia." We conducted our review in accordance with the standards for performance audits set forth in Government Auditing Standards, issued by the Comptroller General of the United States.

Objectives

We had three objectives for our review of Data Security. These objectives were:

1. To educate the reader about information security concepts and provide a common knowledge base that aids in the discussion of the current state of information security in the Commonwealth;

2. To document the current information security initiatives in the Commonwealth and determine whether such initiatives are adequate to ensure the security of information in the possession of Commonwealth agencies and institutions of higher education; and

3. To evaluate the information security programs implemented at the agencies and institutions of higher education throughout the Commonwealth and determine their adequacy.

Scope

Our study included agencies in the executive, legislative, and judicial branches of the Commonwealth as of October 2006. However, the study did not survey agency affiliates, such as the prisons managed by the Department of Corrections, whose information security programs are governed by their oversight agencies.

Methodology

Our review procedures included a comparison of the Commonwealth's information security standard to industry best practices, an evaluation of the information security programs implemented at agencies and institutions of higher education, interviews with Information Security Officers, and research of current federal and state information security laws.

Conclusions

The information security programs in the agencies and institutions of the Commonwealth are generally inadequate and do not address the business needs to adequately control information as well as risks associated with not controlling information. The Commonwealth, however, has several agencies and institutions, such as the Departments of Taxation and General Services and the three largest institutions of higher education, University of Virginia, Virginia Commonwealth University, and Virginia Polytechnic Institute and State University, which provide working models of the best practices of information security programs.

All state agencies and institutions have some type of security over their information technology infrastructure and systems. The security, in most cases, provides coverage over information existing within the agency. Further, almost all agencies and institutions have at least some plan to recover from a disaster; however, this plan does not always extend to how and under what circumstances.

The Auditor of Public Accounts has been conducting security reviews of financial system for over a decade and reporting our findings. This review's results are consistent with our previously reported findings. With the exception of smaller agencies without financial systems, we have previously issued or commented on all the agencies with either no or inadequate information security programs.

In reviewing the results, the reason for inadequate information security programs in the larger agencies, when considering either number of employees or agency budget, appears to center around the resolution of who has responsibility for the infrastructure between the Virginia Information Technologies Agency (VITA) and the agency. The large institutions of higher education with inadequate programs typically do not have the managerial placement of the program at the appropriate level for the organization, although this does occur in other agencies.

Overall, the Commonwealth's standards address most of the components found in the best practices. The difference between the Commonwealth's standards and the best practices, to the most part, occurs within the processes of the components.

We believe the large agencies and institutions can address our recommendations without significant operational changes. However, the Commonwealth will need to develop and implement a process to provide information security programs for smaller agencies and institutions.

Finally, the General Assembly may wish to amend the Code of Virginia to provide for the audit of information security programs, rather than focusing on databases and data communications. The current statute does not address the real risk to the Commonwealth.

AUDITOR OF PUBLIC ACCOUNTS

APPENDIX A – Checklist Survey Results

Based on our discussion in this report, this appendix contains a summary of the checklist survey results, broken out by agency, number of staff and adequacy of their information security program. The APA distributed the checklists to the Commonwealth's agencies and institutions during July 2006 through October 2006. Therefore, the adequacy rating of an agency represents a snapshot of their information security program at a particular moment in time.

Agency Name	Staff	No Program	Inadequate Program	Adequate Program
< 50 Employees				
Board of Accountancy	9		X	
Board of Bar Examiners	5	X		
Commonwealth's Attorneys' Services Council	9	X		
Compensation Board	24		X	
Department for the Aging	27	X		
Department for the Deaf and Hard-of-Hearing	13			X
Department of Aviation	32		X	
Department of Charitable Gaming	38		X	
Department of Employment Dispute Resolution	13	X		
Department of Historic Resources	43		X	
Department of Minority Business Enterprises	43	X		
Department of Rail and Public Transportation	44		X	
Division of Legislative Automated Systems	22		X	
Gunston Hall	28	X		
Innovative Technology Authority	N/A			X
Jamestown 2007	41		X	
Motor Vehicle Dealer Board	33		X	
Office of the Governor and Cabinet Secretaries	41		X	
Southwest Virginia Higher Education Center	27	X		
State Board of Elections	46		X	
Virginia Board for People with Disabilities	21			X
Virginia College Savings Plan	43			X
Virginia Commission for the Arts	7		X	
Virginia Office for Protection and Advocacy	34	X		
Virginia Racing Commission	34		X	
50 – 100 Employees				
Department of Business Assistance	53		X	
Department of Fire Programs	77		X	
Department of Human Resource Management	80		X	
Department of Planning and Budget	67		X	
Frontier Culture Museum of Virginia	79	X		
State Council of Higher Education for Virginia	59		X	
Virginia Museum of Natural History	61		X	
Virginia Port Authority	54			X
Virginia State Bar	96	X		
Virginia Tourism Authority	54		X	

Agency Name	Staff	No Program	Inadequate Program	Adequate Program
101 – 200 Employees				
Department of Accounts	107			X
Department of Criminal Justice Services	157		X	
Department of Emergency Management	194		X	
Department of Housing and Community Development	141		X	
Department of Labor and Industry	186		X	
Department of Professional and Occupational Regulation	172		X	
Department of the Treasury	123		X	
Marine Resources Commission	144		X	
Richard Bland College	113		X	
Supreme Court	145		X	
The Science Museum of Virginia	150		X	
Virginia Economic Development Partnership	118		X	
Virginia School for Deaf and Blind at Staunton	172	X		
201 – 300 Employees				
Attorney General and Department of Law	274		X	
Department of Forensic Science	299	X		
Department of Health Professions	243			X
Department of Mines, Minerals and Energy	233		X	
Department of Mental Health, Mental Retardation and Substance Abuse Services	278		X	
State Lottery Department	299		X	
The Library of Virginia	252		X	
Virginia Department for the Blind and Vision Impaired	217			X
Virginia Retirement System	225			X
Virginia School for Deaf, Blind and Multi-Disabled at Hampton	209	X		
Virginia Workers' Compensation Commission	229		X	
301 – 500 Employees				
Department of Education	434		X	
Department of Forestry	375		X	
Department of Medical Assistance Services	419		X	
Department of Veterans Services	341	X		
Indigent Defense Commission	436	X		
Jamestown-Yorktown Foundation	413		X	
University of Virginia’s College at Wise	330			X
Virginia Institute of Marine Science	468		X	
Virginia Museum of Fine Arts	406		X	

Agency Name	Staff	No Program	Inadequate Program	Adequate Program
501 – 1000 Employees				
Department of Agriculture and Consumer Services	619	X		
Department of Correctional Education	775		X	
Department of Environmental Quality	906		X	
Department of Game and Inland Fisheries	522		X	
Department of General Services	634			X
Department of Military Affairs	558		X	
Longwood University	901		X	
State Corporation Commission	613	X		
Virginia Military Institute	502			X
Virginia State University	680		X	
1001 – 1500 Employees				
Christopher Newport University	1290			X
Department of Conservation and Recreation	1337		X	
Department of Rehabilitative Services	1017			X
Department of Taxation	1241			X
Norfolk State University	1053		X	
Radford University	1189		X	
University of Mary Washington	1116		X	
Virginia Information Technologies Agency	1136			X
1501 – 3000 Employees				
Department of Juvenile Justice	2426		X	
Department of Motor Vehicles	2380		X	
Department of Social Services	1702		X	
Department of State Police	2878		X	
James Madison University	2751		X	
Old Dominion University	2992		X	
The College of William and Mary	2130		X	
Virginia Employment Commission	1574		X	
> 3000 Employees				
Department of Alcoholic Beverage Control	3399		X	
Department of Corrections	11181			X
Department of Health	4136		X	
Department of Transportation	9953		X	
George Mason University	7113		X	
University of Virginia Medical Center	5398		X	
University of Virginia - Academic Campus	8029			X
Virginia Commonwealth University	7181			X
Virginia Community College System	9832			X
Virginia Polytechnic Institute and State University	9096			X
TOTAL		**17**	**66**	**21**

APPENDIX B – Industry Best Practices Comparison

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
1.A	Does the agency have an organizational chart that lays out the reporting structure of employees involved with Information Security?	SP-3.1	6.1	SP 800-18	PO4	Not in standard.
1.A	Does the agency have a committee that oversees the security plan?	SP-2.1	6.1	SP 800-18	PO4	Not in standard.
1.B	Does the organizational structure include the assignment of an Information Security Officer (ISO)? If no, skip the “Information Security (ISO) Role” section.	SP-3.1	6.1	SP 800-18	PO4	Req: SEC 500-02 2.3b
2.B	Have separation of duties been established for system owners?	SP-3.2	10.1	SP 800-18	PO4	2.2.2
2.C	Have separation of duties been established for data owners?	SP-3.2	10.1	SP 800-18	PO4	2.2.2
2.cov	Have separation of duties been established for system administrators?	SP-3.2	10.1	SP 800-18	PO4	2.2.2
2.cov	Have separation of duties been established for security administrators?	SP-3.2	10.1	SP 800-18	PO4	2.2.2
3.A	Does the Information Security Officer (ISO) have input in writing the agency’s security plan?	SP-3.1	6.1	SP 800-18	PO4	Glossary
3.C	Does each location have a Security Administrator (SA) assigned?	SP-3.1	6.1	SP 800-18	PO4	2.2.2
3.D	Does the Information Security Officer (ISO) have the power to deny requests that do not fall in line with the security plan?		6.1	SP 800-18	PO4	Not in standard.
4.cov	Does the agency have a training program? If no, skip to the “Resource and Data Classification” section.	SP-2.1 SP-3.3 SP-4.2	5.1 8.2	SP 800-50	PO7	8.3.2
4.cov	Does the training program define an employee responsible for its implementation and maintenance?	OMB CIRC A-130 Appendix III	8.2	SP 800-50	PO7	8.3.2
4.cov	Does the training program define specific training requirements for employees?	OMB CIRC A-130 Appendix III	8.2	SP 800-50	PO7	8.3.2
4.cov	Does the training program state that attendance is monitored and tracked on annual basis?	OMB CIRC A-130 Appendix III		SP 800-50	PO7	8.3.2

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
4.cov	Does the training program define employees' understanding of 1) agency policy for protecting information assets, 2) separation of duties, 3) systems access restrictions, 4) password management, 5) monitoring, and 6) handling of information types?	OMB CIRC A-130 Appendix III	8.2	SP 800-50	PO7	8.3.2
4.cov	Does the training program state that system owners shall not approve access for users that do not meet training requirements?	OMB CIRC A-130 Appendix III		SP 800-50	PO4	8.3.2
4.cov	Does the training program require employees' signatures on acknowledgement letters?	OMB CIRC A-130 Appendix III		SP 800-50	PO7	8.3.2
4.B	Does a security administrator or information security officer provide the training?	OMB CIRC A-130 Appendix III		SP 800-50	PO4	8.3.2
4.C	Does the information security training cover the following topics: Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), Enterprise Security Policies, Procedures and Standards, Applications and Systems?	OMB CIRC A-130 Appendix III		SP 800-50	PO7	8.3.2
4.C	Do information security training requirements exist for vendors?	OMB CIRC A-130 Appendix III	8.2	SP 800-50		8.3.2
4.D	Are training programs designed for all organizational levels of employee training?	OMB CIRC A-130 Appendix III	8.2	SP 800-50		8.3.2
4.E	Are all employees required to attend security awareness training?	OMB CIRC A-130 Appendix III	8.2	SP 800-50		8.3.2
4.E	If an employee is exempt from attending security training, is this documented, including reason for exemption, and approved by management and the Information Security Officer?					

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
4.F	Does the technical staff have training requirements and a predetermined number of professional hours required to meet the agency's training program?	OMB CIRC A-130 Appendix III	10.1 10.3	SP 800-50		8.3.2
4.G	Is technical staff notified of security related events and technology changes?	OMB CIRC A-130 Appendix III	13.2	SP 800-12		In 9.3.2 but could be reworded.
5.A	Does the agency have established classifications and associated criteria? If no, skip to "Information Asset Inventory" section.	AC-1.1	7.2	SP 800-12	PO2 DS5	2.4.2
5.B	Has data classifications been documented by the Agency and approved by its senior management?	AC-1.2	7.2	SP 800-12	PO2	2.4.2 includes data classification but does not require management approval
5.C	Does the agency review the data classifications periodically?	AC-1.2	7.2	SP 800-12	PO2	Not in standard.
5.D	Are the classifications communicated to the resource data owners and end users?	AC-1.1	7.2	SP 800-12	PO2	Not in standard.
5.cov	Has each data owner categorized their data based on confidentiality, integrity, and availability? *For example: Mission critical, mission essential, non-essential*	AC-1.2	7.2	SP 800-12	PO2	2.4.2
5.cov	Have sensitivity requirements been examined? *For example: HIPAA, FOIA, etc*	AC-1.1	15.1	SP 800-66	PO2	2.4.2
5.cov	Has each data owner documented potential damages to the agency if security requirements are not met?	AC-1.2	4.1	SP 800-12	PO2	2.4.2
6.A	Does the agency have a documented and maintained list of its hardware and software? If no, skip to the "Risk Assessment (RA)" section.	SC-1.2	7.1	SP 800-12	PO5	2.5.2
6.B	Does the agency have a documented policy to periodically review and update the list of its software and hardware?	SC-1.1	7.1	SP 800-12	PO5	2.5.2 states it should be updated as changes occur but does not provide for periodic review
6.C	Does the agency have an updated network diagram?	SC-1.2	10.6		PO5	Not is standard.

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
6.D	Does the agency have a designated network administrator responsible for maintaining the network diagram?	SC-1.1	10.6		PO5	Not in standard.
	Has the agency completed and documented a RA relating to its IT infrastructure? If no, skip to the "Business Impact Analysis (BIA)" section.	SP-1 OMB Circ A-130, III	4.1	SP 800-30	PO9 AI1	2.6.2
7.cov	Is the RA reviewed at least annually to check compliance with the Commonwealth of Virginia security standard?	SP-1				2.6.2
7.cov	Is the RA updated at least every three (3) years?	SP-1	4.1	SP 800-30	PO9 AI1	2.6.2
7.G	Does the agency require all components of its IT infrastructure to be rated in the RA?	SP-1	4.1	SP 800-30	PO9 AI1	This standard only requires those systems classified as "sensitive" to be included.
	Does the agency have a documented BIA? If no, skip to the "Business Continuity Plan (BCP)" section.	SC-1.1	14.1	SP 800-34		2.3.2
8.A	Is the BIA updated at least every three (3) years or when a new system is introduced, whichever is earlier?	SC-1.1	14.1	SP 800-34		2.3.2
8.B	Does the agency involve the Data and Systems owners in the BIA process?	SC-1.1	14.1	SP 800-34		Not in standard.
8.C	Does the BIA include and define all agency mission critical business functions and secondary business functions?	SC-1.1	14.1	SP 800-34		2.3.2
8.D	Are maximum allowable downtimes stated for those systems classified as critical?	SC-1.1	14.1	SP 800-34		2.3.2
8.E	Does the upper management make the final decision of allowable downtime?	SC-1.1	14.1	SP 800-34		2.3.2
8.cov	Has the agency designated one employee to be responsible for the BIA and is this employee coordinating his/her efforts with Virginia Department of Emergency Management (VDEM)	SC-1.1	14.1	SP 800-34		Covered in COOP
	Does the agency have a documented BCP? If no, skip to the "Disaster Recovery Plan (DRP)" section.	SC-3.1	14.1	SP 800-34	DS4	3.2.2
9.A	Is the BCP reviewed and updated at least annually?	SC-3.1	14.1	SP 800-34	DS4	3.2.2

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
9.A	Has the Agency designated one employee responsible for the BCP?	SC-3.1	14.1	SP 800-34	DS4	3.2.2
	Does the agency have a documented DRP? If no, skip to the "Incident Response Procedure (IRP)" section.	SC-3.1	14.1 10.3 10.4 10.5 11.7	SP 800-34	DS4	3.3.2
10.B	Does the plan include manual processing procedures for critical functions that users can follow until operations are restored?	SC-3.1		SP 800-34	DS4	Not in standard.
10.cov	Does the DRP reference the BCP?	SC-3.1		SP 800-34	DS4	3.3.2
10.cov	Does the DRP state the order of restoration?	SC-3.1		SP 800-34	DS4	3.3.2
10.cov	Does the DRP specify support teams and their members?	SC-3.1		SP 800-34	DS4	This standard does not go into enough detail to provide a comprehensive DRP
10.cov	Does the DRP specify responsibilities?	SC-3.1		SP 800-34	DS4	This standard does not go into enough detail to provide a comprehensive DRP
10.cov	Does the DRP specify an alternate site?	SC-3.2		SP 800-34	DS4	This standard does not go into enough detail to provide a comprehensive DRP
10.cov	Does the DRP include technical procedures for restoration?	SC-3.1		SP 800-34	DS4	3.3.2
10.cov	Does the DRP state procedures for returning to normal operations?	SC-3.1		SP 800-34	DS4	This standard does not go into enough detail to provide a comprehensive DRP
10.cov	Does the DRP include controls to ensure regular backups?	SC-2.1		SP 800-34	DS4	3.4.2
10.cov	Are backup media stored at a secure location off-site?	SC-2.1		SP 800-34	DS4	3.4.2
	Does the agency have a documented IRP? If no, skip to the "Confidentiality, Integrity, and Availability (CIA)" section.	SP-3.4 CC-1.3	13.2	SP 800-34	DS5	9.3.2

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
11.A	Does the IRP include the use of virus identification software, means for prompt centralized reporting and a response team that has the necessary knowledge, skills, and abilities?	SP-3.4 CC-1.3	10.4		DS5	This standard does not address virus identification software in the IRP. 9.3.2 does address an IRT properly expertise. Malicious Code Protection is included as part of 4.4.2
11.C	Does the IRP define controls that manage problems and incidents?	SP-3.4 CC-1.3	13.2	SP 800-83	DS5	9.3.2
11.E	Does the IRP include a problem or incident management contact list and is this list included in the BCP?	SP-3.4 CC-1.3	13.2	SP 800-83	DS5	9.3.2 does include an incident management list, only the CIO.
11.cov	Are the requirements for scanning, monitoring, removal, alerts, logs, and prevention stated in the IRP?	SP-3.4 CC-1.3	13.2	SP 800-83	DS5	9.3.2
14.A	Does the agency have policies and procedures for approving logical access? If no, skip to the "Authentication" part.	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	11.6	SP 800-12	DS5	5.2.2
14.B	Do data owners and security officers issue the final approval or denial of access request?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	11.1 11.2 11.3 11.4	SP 800-12	PO4	5.2.2
14.C	Does the Agency have policies and procedures that approve and remove authorization for vendors and/or third parties?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	11.1 11.2 11.3 11.4	SP 800-12	DS5 DS2	This standard does not address third party access and/or authorization
14.D	Does the agency have policies and procedures for removing logical access, including terminated and transfer employees?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	8.3	SP 800-12	PO7	5.2.2

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
14.E	Has the agency documented that it practices the philosophy of "least privileges" for granting access?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	11.2	SP 800-12	DS5	5.2.2
14.F	Do data owners and/or Information Security Officers periodically review access authorization listings to determine whether they remain appropriate?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	11.2.4	SP 800-12	DS5	5.2.2
14.G	Are there documented employee job descriptions that accurately reflect assigned duties, responsibilities and segregate duties?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	8.1	SP 800-12	PO4 PO7	Not in standard.
14.H	Have controls been implemented to mitigate possible segregation of duties risk?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	10.1.3	SP 800-12	PO4	8.2.2
14.I	Does the agency actively review employee activity to identify other possible segregation risks?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1		SP 800-12	PO7	Standard provides for review of user accounts (5.2.2) but not a review of employee activity.
14.J	Is the request and approval of emergency or temporary access documented on a standard form and maintained on file, approved by appropriate managers, securely communicated to the security function, and automatically terminated after a predetermined period?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1		SP 800-12	DS5	Emergency and/or temporary access is not addressed in this standard
14.K	Are inactive user IDs deactivated after a specific period of time?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	8.3	SP 800-12	DS5	5.2.2

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
14.L	Are users required to be authenticated for access to all systems and exceptions approved by management, and have risks of those exceptions been evaluated and accepted?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	11.2	SP 800-12	DS5	8.2.2
14.M	Are there policies and procedures regarding password controls?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	11.5			5.3.2
14.N	Are vendor supplied (default) passwords changed immediately after installation?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	11.2			Not is standard
14.O	Has the agency identified all critical and service resources (mainly tangible items), including servers, computers, data centers, and sensitive materials for lockup?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	7.1	SP 800-12	DS9	2.5.2
14.P	Have critical physical security points been identified?	AC-2.1 AC-2.2 AC-3.1 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9	SP 800-12	DS12	Not in standard.
14.Q	Has the agency reviewed physical risks associated with equipment and resources?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9	SP 800-12	DS12	7.2
14.R	Does all the critical and sensitive assets have the appropriate physical safe guards in place to protect against unauthorized access and is it documented who approves these controls?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9 10.8.3	SP 800-12	DS12	7.2

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
14.S	Does the agency have critical and/or sensitive resources, which are not under the control of the information systems department, and are appropriate physical security controls in place?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9.2	SP 800-12	DS12	7.2
14.T	Does the agency have policies and procedures in place for approving and removing physical access?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9	SP 800-12	DS12	7.2
14.U	Is physical access limited for specific personnel and are there controls in place?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9	SP 800-12	DS12	7.2
14.V	Does the agency have controls in place for visitors, vendors, 3rd parties with respect to physical access?	AC-2.1 AC-2.2 AC-3.2 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9	SP 800-12	DS12	7.2
14.W	Are entry codes used and changed regularly to control access to computer rooms and equipment?	AC-2.1 AC-2.2 AC-3.1 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9.1.2	SP 800-12	DS12	Not in standard.
14.X	Does the agency have emergency exit and re-entry procedures to ensure that resources are properly protected?	AC-2.1 AC-2.2 AC-3.1 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9.1.1	SP 800-12	DS12	Not in standard.
14.Y	Does management regularly review the list of persons allowed physical access to sensitive resources?	AC-2.1 AC-2.2 AC-3.1 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9.1	SP 800-12	DS12	Not in standard.

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
14.Z	Must all deposits and withdrawals of storage media located off-site be authorized and logged?	AC-2.1 AC-2.2 AC-3.1 SS-1.1 SD-1.1 SD-1.2 SD-2.1	9	SP 800-12	DS11	Not in standard.
14. cov	Has physical security safeguards been established for structures?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-12	DS12	7.2
14. cov	Has physical security safeguards been established for door/windows?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-12	DS12	7.2
14. cov	Has physical security safeguards been established for the perimeter?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-12	DS12	7.2
14. cov	Has physical security safeguards been established for environmental conditions?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-12	DS12	7.2
14. cov	Has physical security safeguards been established for electrical needs?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-12	DS12	7.2
14. cov	Has physical security safeguards been established for fire safety?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-12	DS12	7.2
14. cov	Has physical security safeguards been established for water damage?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-12	DS12	7.2
14. cov	Has physical security safeguards been established for anti-terrorism?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-61		Not in standard.
14. cov	Has physical security safeguards been established for emergency evacuation?	AC-3.1 AC-3.2 SC-2.2 SD-2.1	9	SP 800-12	DS12	7.2
14. cov	Are background investigations performed before granting access to systems?	SP-4.1	8.1		PO7	8.2.2
14. cov	Does the user have to sign non-disclosure and security agreements?	SP-4.1	8.1		PO7	8.2.2
14. cov	Do controls exist to ensure that physical objects (badges, keys, etc) are returned after termination or transfer?	SP-4.1	8.3		PO7	8.2.2

REF #	**Checklist Question**	**FISCAM**	**ISO 17799**	**NIST**	**COBIT**	**SEC 501**
14. cov	Does separation of duties exist when physical access is determined and approved?	SD-2.1	10.1	SP 800-12	DS12	8.2.2
14.α	Are there security agreements for sharing system information with other systems and/or data owners?	AC-2.1	6.1		PO2	4.3.2
14.β	Do any security agreements include any mandated requirements (i.e. HIPAA) and is it documented that both partied (agencies) have to abide by these requirements?	AC-2.1	6.1		ME3	Not in standard with regards to shared information
14. cov	Do password controls include secure delivery of initial password?	AC-3.2	11.2.3			5.3.2
14. cov	Do password controls include a requirement to investigate any unusual activities?	AC-2.2				Password management 5.3 does not require investigation of unusual activity
14. cov	Do password controls include existence of auditable records?	AC-4.1				No requirement for auditable records
14. cov	Do password controls include using groups for Access Control Lists (ACL)?	AC-3.2				5.2.2
14. cov	Do password controls include the masking of passwords?	AC-3.2				5.3.2
14. cov	Do password controls include not using guest/shared accounts?	AC-3.2				5.2.2
15.A	Are there written policies and procedures for change management? If no, skip to the “Software Change Management” part.	CC-1.1	10.1.2		DS9	Defer to COBIT
15.B	Does the agency have a change management committee to rank the priority of changes?	CC-1.2	10.1.2		DS9	Defer to COBIT
15.C	Does the agency have separate development, test, and productions areas?	CC-1.1	10.1.4		DS9	Defer to COBIT
15.D	Is programmer testing required to be documented and fully tested?	CC-2.1	10.1.4		DS9	Defer to COBIT
15.E	Are the results of the tests reviewed by the programmer’s manager?	CC-2.1	10.1.4		DS9	Defer to COBIT
15.F	Is there a test plan developed before end-user testing begins?	CC-2.1	10.1.4		DS9	Defer to COBIT
15.G	Does management approve such a test plan?	CC-2.1	10.1.4		DS9	Defer to COBIT
15.H	Is end-user acceptance required for all changes?	CC-2.1	10.1.4		DS9	Defer to COBIT
15.I	Are all changes documented so that they can be traced from authorization to the final approved code?	CC-2.1	10.1.4		DS9	Defer to COBIT

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
15.J	Is code secured from programmer alteration after testing so that changes during user testing and after user acceptance testing can be prevented?	CC-2.1	10.1.4		DS9	Defer to COBIT
15.K	Does someone other than the programmer move code changes into production?	CC-2.1	10.1.4		DS9	Defer to COBIT
15.L	Are emergency changes recorded, reviewed, and approved after the problem is resolved?	CC-2.2	13.2		DS9	Defer to COBIT
15.M	Are all risky impacts considered by a configuration management committee before a change is implemented?	CC-2.1	13.2		DS9	Defer to COBIT
15.N	Is a proper approval process implemented?	CC-2.1	13.2		DS9	Defer to COBIT
15.O	Does the agency have a policy for version control? If no, skip to the "Standard Configurations" part.	CC-3.1	10.1.4		DS9	Defer to COBIT
15.P	Does the version control policy include a cost-benefit analysis?	CC-3.1	10.1.4		DS9	Defer to COBIT
15.Q	Do any software packages fall outside the scope of the version control policy, and does it follow the agency's exception policy?	CC-3.1	10.3		DS9	Defer to COBIT
15.R	Are there policies in place to prevent users from installing unapproved software on to their work computers?	CC-1.3	11.4		DS5	Defer to COBIT
15.S	Is this agency audited for compliance on a regular basis?	SS-2.2	15.2		ME4	2.7.2
15. cov	Are standard security configurations reviewed and revised at least annually?	SS-2.2	12.4		DS9	4.2.2
15. cov	Are security requirements incorporated into each phase of the SDLC? If no, skip to the "Asset Management" part.	CC-1.1	12.5	SP 800-64	PO8	4.5.2
15. cov	Are security risks reviewed in the beginning of the initiation phase (Risk assessment)?	CC-1.1	12.5	SP 800-64	PO8	4.5.2
15. cov	Are security configuration control settings reviewed and approved in the implementation phase?	CC-1.1	12.5	SP 800-64	PO8	4.5.2
15. cov	Is security for the configuration management and change control functions reviewed and approved in the operations/maintenance phase?	CC-2.1	12.5	SP 800-64	PO8	Defer to COBIT

REF #	Checklist Question	FISCAM	ISO 17799	NIST	COBIT	SEC 501
15. cov	Does the agency have a policy regarding inventory management?	CC-3.1	7.1		DS4	10.2.2
15. cov	Does the agency have a policy regarding software license management?		7.1 15.1.2		DS9	10.3.2
	Does the Agency monitor their systems, applications, and databases? If no, then end the questionnaire.	SS-2.1	10.10		DS5	9.4.2
16.A	Has the monitoring of systems, applications or databases ever triggered security changes or business process changes? If no, skip to question 16.C.	SS-2.2	10.10		DS5	Not in standard.
16.B	Do the changes in 16.a go through the change management system?	SS-2.2	10.10		DS5	Not in standard.
16.C	Does the agency classify and document any different types of monitoring?	SS-2.2	10.10		DS5	Not in standard.
16.D	Have any incidents resulted in the change of the standard monitoring practice? If no, skip to question 16.F.	SS-2.2	10.10		DS5	Not in standard.
16.E	Have risk assessments been performed on any changes resulting from 16.D?	SS-2.2	10.10		DS5	Not in standard.
16.F	Are security violations and activities, such as failed logon attempts and other failed access attempts and access attempts to sensitive information, reviewed and documented on a set schedule?	SS-2.2	10.10		DS5	9.3.2
16.G	Are any security violations in 16.F reported to management and investigated?	SS-2.2	10.10		DS5	9.3.2

APPENDIX C – Checklist

APA
Auditor of
Public Accounts
COMMONWEALTH OF VIRGINIA

Auditor Core Information Systems Security CHECKLIST

Purpose:
This checklist, and its supporting documentation, will be used by the Auditor of Public Accounts (APA) to assess the level of information security implemented at an Agency through its policies, procedures, and standards. The assessment will be included in a report to the General Assembly as mandated by *Senate Joint Resolution 51* of the 2006 General Assembly.

Directions:

1. Please do not print this form. Rather, fill the form out electronically.
2. Please fill out the information in the “AGENCY” box on this page.
3. Complete this checklist by marking the box in the “Agency Response” column for each question. A mark means YES, leaving the checkbox blank means NO. Supporting documentation, such as policies and procedures, shall be submitted together with this checklist as separate files. Please reference these files in the W/P Reference column.

Restrictions:
Do not, under any circumstances, e-mail this document or any of its supporting documentation. This document and supporting documentation shall be treated as FOI Exempt due to its sensitivity. This document and supporting documentation shall be hand delivered to the Auditor on a portable media type, such as CD-ROM, ZIP disk, 3.5” disk, etc.

AGENCY	APA
Agency Name: Agency Contact Name: Agency Contact e-mail: Agency Contact Phone: Date Received: Date Returned:	Auditor Name: Date Sent: Date Received: Reviewed for Completeness:

Security Management Structure

Security Management Structure

Determine that the agency established an information security management organizational structure.

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
1.A	Does the agency have an organizational chart that lays out the reporting structure of employees involved with Information Security?	□	□	
1.A	Does the agency have a committee that oversees the security plan?	□	□	
1.B	Does the organizational structure include the assignment of an Information Security Officer (ISO)? If no, skip the "Information Security (ISO) Role" section.	□	□	

Information Security Responsibilities and Separation of Duties

Determine that information security responsibilities have been clearly defined for the following areas

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
2.B	Have separation of duties been established for system owners?	□	□	
2.C	Have separation of duties been established for data owners?	□	□	
2.cov	Have separation of duties been established for system administrators?	□	□	
2.cov	Have separation of duties been established for security administrators?	□	□	

Information Security Officer (ISO) Role

Determine the ISO's role within the Organization. Key areas: development, implementation, maintenance, and oversight of an Agency's Information Systems Security Program.

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
3.A 3.D	Does the Information Security Officer (ISO) have input in writing the agency's security plan and the power to deny requests that do not fall in line with the security plan?	□	□	
3.C	Does each location have a Security Administrator (SA) assigned?	□	□	

Security Awareness Training

Verify that an ongoing security awareness-training program has been implemented. It should include first time training for all new employees, contractors, and users, as well as periodic refresher training thereafter.

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Does the agency have a training program? If no, skip to the "Resource and Data Classification" section.	□	□	
4.cov	Does the training program define an employee responsible for its implementation and maintenance?	□	□	
4.cov	Does the training program define specific training requirements for employees?	□	□	
4.cov	Does the training program state that attendance is monitored and tracked on annual basis?	□	□	
4.cov	Does the training program define employees' understanding of 7) agency policy for protecting information assets, 8) separation of duties, 9) systems access restrictions, 10) password management, 11) monitoring, and 12) handling of information types?	□	□	
4.cov	Does the training program state that system owners shall not approve access for users that do not meet training requirements?	□	□	
4.cov	Does the training program require employees' signatures on acknowledgement letters?	□	□	
4.B	Does a security administrator or information security officer provide the training?	□	□	
4.C	Does the information security training cover the following topics: Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), Enterprise Security Policies, Procedures and Standards, Applications and Systems?	□	□	
4.C	Do information security training requirements exist for vendors?	□	□	
4.D	Are training programs designed for all organizational levels of employee training?	□	□	
4.E	Are all employees required to attend security awareness training?	□	□	
4.E	If an employee is exempt from attending security training, is this documented, including reason for exemption, and approved by management and the Information Security Officer?	□	□	
4.F	Does the technical staff have training requirements and a predetermined number of professional hours required to meet the agency's training program?	□	□	
4.G	Is technical staff notified of security related events and technology changes?	□	□	

Resource and Data Classifications
Verify that the agency has established resource and data classifications

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
5.A	Does the agency have established classifications and associated criteria? If no, skip to “Information Asset Inventory” section.	□	□	
5.B	Has data classifications been documented by the Agency and approved by its senior management?	□	□	
5.C	Does the agency review the data classifications periodically?	□	□	
5.D	Are the classifications communicated to the resource data owners and end users?	□	□	
5.cov	Has each data owner categorized their data based on confidentiality, integrity, and availability? *For example: Mission critical, mission essential, non-essential*	□	□	
5.cov	Have sensitivity requirements been examined? *For example: HIPAA, FOIA, etc*	□	□	
5.cov	Has each data owner documented potential damages to the agency if security requirements are not met?	□	□	

Information Assets Inventory
Verify that the agency has a documented inventory of assets.

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
6.A	Does the agency have a documented and maintained list of its hardware and software? If no, skip to the “Risk Assessment (RA)” section.	□	□	
6.B	Does the agency have a documented policy to periodically review and update the list of its software and hardware?	□	□	
6.C	Does the agency have an updated network diagram?	□	□	
6.D	Does the agency have a designated network administrator responsible for maintaining the network diagram?	□	□	

Risk Assessment (RA)
Verify that the agency has a documented risk assessment

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Has the agency completed and documented a RA relating to its IT infrastructure? If no, skip to the “Business Impact Analysis (BIA)” section.	□	□	
7.cov	Is the RA reviewed at least annually to check compliance with the Commonwealth of Virginia security standard?	□	□	
7.cov	Is the RA updated at least every three (3) years?	□	□	

7.G	Does the agency require all components of its IT infrastructure to be rated in the RA?	□	□	

Business Impact Analysis (BIA)
Verify that the agency has a documented Business Impact Analysis.

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Does the agency have a documented BIA? If no, skip to the “Business Continuity Plan (BCP)” section.	□	□	
8.A	Is the BIA updated at least every three (3) years or when a new system is introduced, whichever is earlier?	□	□	
8.B	Does the agency involve the Data and Systems owners in the BIA process?	□	□	
8.C	Does the BIA include and define all agency mission critical business functions and secondary business functions?	□	□	
8.D	Are maximum allowable downtimes stated for those systems classified as critical?	□	□	
8.E	Does the upper management make the final decision of allowable downtime?	□	□	
8.cov	Has the agency designated one employee to be responsible for the BIA and is this employee coordinating his/her efforts with Virginia Department of Emergency Management (VDEM)	□	□	

Business Continuity Plan (BCP)
Verify that the Agency has a Business Continuity Plan, sometimes called Continuity of Operations Plan (COOP)

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Does the agency have a documented BCP? If no, skip to the “Disaster Recovery Plan (DRP)” section.	□	□	
9.A	Is the BCP reviewed and updated at least annually?	□	□	
9.A	Has the Agency designated one employee responsible for the BCP?	□	□	

Disaster Recovery Plan (DRP)
Verify that the Agency has established a Disaster Recovery Plan.

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Does the agency have a documented DRP? If no, skip to the “Incident Response Procedure (IRP)” section.	□	□	
10.B	Does the plan include manual processing procedures for critical functions that users can follow until operations are restored?	□	□	
10.cov	Does the DRP reference the BCP?	□	□	
10.cov	Does the DRP state the order of restoration?	□	□	
10.cov	Does the DRP specify support teams and their members?	□	□	
10.cov	Does the DRP specify responsibilities?	□	□	

10.cov	Does the DRP specify an alternate site?	□	□	
10.cov	Does the DRP include technical procedures for restoration?	□	□	
10.cov	Does the DRP state procedures for returning to normal operations?	□	□	
10.cov	Does the DRP include controls to ensure regular backups?	□	□	
10.cov	Are backup media stored at a secure location off-site?	□	□	

Incident Response Procedure (IRP)

Verify that the Agency has an incident response procedure.

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Does the agency have a documented IRP? If no, skip to the “Confidentiality, Integrity, and Availability (CIA)” section.	□	□	
11.A	Does the IRP include the use of virus identification software, means for prompt centralized reporting and a response team that has the necessary knowledge, skills, and abilities?	□	□	
11.C	Does the IRP define controls that manage problems and incidents?	□	□	
11.E	Does the IRP include a problem or incident management contact list and is this list included in the BCP?	□	□	
11.cov	Are the requirements for scanning, monitoring, removal, alerts, logs, and prevention stated in the IRP?	□	□	

Data Protection, Integrity, Availability and Confidentiality

Confidentiality, Integrity and Availability (CIA)

Determine controls are in place to protect confidentiality, integrity, and availability of the agency's data

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Authorization			
14.A	Does the agency have policies and procedures for approving logical access? If no, skip to the "Authentication" part.	□	□	
14.B	Do data owners and security officers issue the final approval or denial of access request?	□	□	
14.C	Does the Agency have policies and procedures that approve and remove authorization for vendors and/or third-parties?	□	□	
14.D	Does the agency have policies and procedures for removing logical access, including terminated and transfer employees?	□	□	
14.E	Has the agency documented that it practices the philosophy of "least privileges" for granting access?	□	□	
14.F	Do data owners and/or Information Security Officers periodically review access authorization listings to determine whether they remain appropriate?	□	□	
14.G	Are there documented employee job descriptions that accurately reflect assigned duties, responsibilities and segregate duties?	□	□	
14.H	Have controls been implemented to mitigate possible segregation of duties risk?	□	□	
14.I	Does the agency actively review employee activity to identify other possible segregation risks?	□	□	
14.J	Is the request and approval of emergency or temporary access documented on a standard form and maintained on file, approved by appropriate managers, securely communicated to the security function, and automatically terminated after a predetermined period?	□	□	
14.K	Are inactive user IDs deactivated after a specific period of time?	□	□	
	Authentication			
14.L	Are users required to be authenticated for access to all systems, are exceptions approved by management, and have risks of those exceptions been evaluated and accepted?	□	□	

Password Controls				
14.M	Are there policies and procedures regarding password controls? *These procedures should include procedures to reset passwords, password file encryption, minimum length and complexity, grace period, password history, screen saver passwords, passwords not displayed when entered, session locks, failed access attempts are logged, etc.*	□	□	
14.N	Are vendor supplied (default) passwords changed immediately after installation?	□	□	
Physical Access				
14.O	Has the agency identified all critical and service resources (mainly tangible items), including servers, computers, data centers, and sensitive materials for lockup?	□	□	
14.P	Have critical physical security points been identified?	□	□	
14.Q	Has the agency reviewed physical risks associated with equipment and resources?	□	□	
14.R	Does all the critical and sensitive assets have the appropriate physical safe guards in place to protect against unauthorized access and is it documented who approves these controls?	□	□	
14.S	Does the agency have critical and/or sensitive resources, which are not under the control of the information systems department and are appropriate physical security controls in place?	□	□	
14.T	Does the agency have policies and procedures in place for approving and removing physical access?	□	□	
14.U	Is physical access limited for specific personnel and are there controls in place?	□	□	
14.V	Does the agency have controls in place for visitors, vendors, 3^{rd} parties with respect to physical access?	□	□	
14.W	Are entry codes used and changed regularly to control access to computer rooms and equipment?	□	□	
14.X	Does the agency have emergency exit and re-entry procedures to ensure that resources are properly protected?	□	□	
14.Y	Does management regularly review the list of persons allowed physical access to sensitive resources?	□	□	
14.Z	Must all deposits and withdrawals of storage media located off-site be authorized and logged?	□	□	
14.cov	Has physical security safeguards been established for structures?	□	□	
14.cov	Has physical security safeguards been established for door/windows?	□	□	
14.cov	Has physical security safeguards been established for the perimeter?	□	□	

14.cov	Has physical security safeguards been established for environmental conditions?	□	□	
14.cov	Has physical security safeguards been established for electrical needs?	□	□	
14.cov	Has physical security safeguards been established for fire safety?	□	□	
14.cov	Has physical security safeguards been established for water damage?	□	□	
14.cov	Has physical security safeguards been established for anti-terrorism?	□	□	
14.cov	Has physical security safeguards been established for emergency evacuation?	□	□	
14.cov	Are background investigations performed before granting access to systems?	□	□	
14.cov	Does the user have to sign non-disclosure and security agreements?	□	□	
14.cov	Do controls exist to ensure that physical objects (badges, keys, etc) are returned after termination or transfer?	□	□	
14.cov	Does separation of duties exist when physical access is determined and approved?	□	□	
Interfaces / Interoperability				
14.α	Are there security agreements for sharing system information with other systems and/or data owners?	□	□	
14.β	Do any security agreements include any mandated requirements (i.e. HIPAA) and is it documented that both partied (agencies) have to abide by these requirements?	□	□	
14.cov	Do password controls include secure delivery of initial password?	□	□	
14.cov	Do password controls include a requirement to investigate any unusual activities?	□	□	
14.cov	Do password controls include existence of auditable records?	□	□	
14.cov	Do password controls include using groups for Access Control Lists (ACL)?	□	□	
14.cov	Do password controls include the masking of passwords?	□	□	
14.cov	Do password controls include not using guest/shared accounts?	□	□	

Configuration and Change Management

Change and Configuration Authorization

Determine what controls are in place for accepting and authorizing changes and configurations

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Change Management			
15.A	Are there written policies and procedures for change management? If no, skip to the “Software Change Management” part.	□	□	
15.B	Does the agency have a change management committee to rank the priority of changes?	□	□	
15.C	Does the agency have separate development, test, and productions areas?	□	□	
15.D	Is programmer testing required to be documented and fully tested?	□	□	
15.E	Are the results of the tests reviewed by the programmer’s manager?	□	□	
15.F	Is there a test plan developed before end-user testing begins?	□	□	
15.G	Does management approve such a test plan?	□	□	
15.H	Is end-user acceptance required for all changes?	□	□	
15.I	Are all changes documented so that they can be traced from authorization to the final approved code?	□	□	
15.J	Is code secured from programmer alteration after testing so that changes during user testing and after user acceptance testing can be prevented?	□	□	
15.K	Does someone other than the programmer move code changes into production?	□	□	
15.L	Are emergency changes recorded, reviewed, and approved after the problem is resolved?	□	□	
15.M	Are all risky impacts considered by a configuration management committee before a change is implemented?	□	□	
15.N	Is a proper approval process implemented?	□	□	
	Software Change Management			
15.O	Does the agency have a policy for version control? If no, skip to the “Standard Configurations” part.	□	□	
15.P	Does the version control policy include a cost-benefit analysis?	□	□	
15.Q	Do any software packages fall outside the scope of the version	□	□	

	control policy, and does it follow the agency's exception policy?			
15.R	Are there policies in place to prevent users from installing unapproved software on to their work computers?	□	□	
15.S	Is this agency audited for compliance on a regular basis?	□	□	
Standard Configurations				
15.cov	Are standard security configurations reviewed and revised at least annually?	□	□	
SDLC Security				
15.cov	Are security requirements incorporated into each phase of the SDLC? If no, skip to the "Asset Management" part.	□	□	
15.cov	Are security risks reviewed in the beginning of the initiation phase (Risk assessment)?	□	□	
15.cov	Are security configuration control settings reviewed and approved in the implementation phase?	□	□	
15.cov	Is security for the configuration management and change control functions reviewed and approved in the operations/maintenance phase?	□	□	
Asset Management				
15.cov	Does the agency have a policy regarding inventory management?	□	□	
15.cov	Does the agency have a policy regarding software license management?	□	□	

Monitoring and Logging

Monitoring and Logging

Determine that controls are in place that require monitoring and logging of Information Systems resources and uses.

Ref #	Question	Agency Response	APA Use	Manual Reference or Comment
	Does the Agency monitor their systems, applications, and databases? If no, then end the questionnaire.	□	□	
16.A	Has the monitoring of systems, applications or databases ever triggered security changes or business process changes? If no, skip to question 16.C.	□	□	
16.B	Do the changes in 16.a go through the change management system?	□	□	
16.C	Does the agency classify and document any different types of monitoring?	□	□	
16.D	Have any incidents resulted in the change of the standard monitoring practice? If no, skip to question 16.F.	□	□	
16.E	Have risk assessments been performed on any changes resulting from 16.D?	□	□	
16.F	Are security violations and activities, such as failed logon attempts and other failed access attempts and access attempts to sensitive information, reviewed and documented on a set schedule?	□	□	
16.G	Are any security violations in 16.F reported to management and investigated?	□	□	

GLOSSARY OF TERMS

Authentication The process of verifying the identity of a user. Is the user whom they claim to be?

Authorization The process of establishing and enforcing a user's rights and privileges to access specified resources.

Business continuity plan (BCP or COOP) Details the processes to follow in order to continue business operations in the event that a critical information system is unavailable. This could be due to a disaster, malfunction, malicious attack, etc.

Business impact analysis (BIA) Details the extent to which risks to systems defined in the risk assessment can affect business practices.

Critical (or Mission Critical) Information resources whose unavailability or improper use has the potential to adversely affect the ability of an Agency to accomplish its mission.

Data owner The entity, group, or individual that has ultimate responsibility for the creation and modification of information stored in a database or other system. The data owner is responsible for ensuring that the System Owner has implemented sufficient security in the system platform to safeguard the applications and data stored on that server.

Disaster recovery plan (DRP) Details the process for restoring systems in the event that a natural or other event causes a system to be unusable.

End-user An individual or group who has access to an information system or its data.

Information security officer (ISO) Responsible for developing, maintaining, and enforcing an agency's security policies and procedures.

Risk assessment (RA) Details occurrences, natural or manmade, that may affect the operability of a system or the integrity of the data contained on that system.

Security administrator Manages security controls over networks and systems to prevent improper or unauthorized use of data.

System administrator Manages the day-to-day operation of the computer system(s) within an organization.

Systems development life cycle (SDLC) A methodology used to develop, maintain, and replace information systems. Typical phases in the *SDLC* are: Analysis and Requirements, Design, Development, Integration and Testing, Implementation, Maintenance.

System owner A group (i.e., Agency or Agency unit) which controls a set of information resources and determines its level of criticality and sensitivity.

COMMONWEALTH *of* VIRGINIA

Lemuel C. Stewart, Jr.
CIO of the Commonwealth
Email: lem.stewart@vita.virginia.gov

Virginia Information Technologies Agency
110 South 7th Street
Richmond, Virginia 23219
(804) 371-5000

TDD VOICE -TEL. NO.
711

December 4, 2006

Mr. Walter J. Kucharski
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218

Dear Mr. Kucharski:

Thank you for the opportunity to review and respond to the Auditor of Public Accounts' Review of Information Security in the Commonwealth of Virginia for the fiscal year ended June 30, 2006. The review highlights many of the challenges the Commonwealth must address to enhance information security.

We are in agreement with the four recommendations and will prepare a recommended corrective action plan for the two specifically within VITA's authority (numbers 1 and 3) for consideration and adoption by the Finance and Audit Committee and the Information Technology Investment Board at their January meetings.

As we discussed at our Exit Conference, motivating compliance is a current obstacle that we must strive to overcome. Linking appropriate consequences to noncompliance would hasten the enhancement of information security within the Commonwealth. As always, we appreciate the professionalism of your staff.

Sincerely,

Lemuel C. Stewart, Jr.

c: The Honorable Aneesh P. Chopra, Secretary of Technology
Judy Napier, Deputy Secretary of Technology
Members, Information Technology Investment Board