Training, Experience, or Time: Which is Most Important to Managing Classified Systems?

by

Jeremy B. Blevins

A Graduate Capstone Project
Submitted to the Extended Campus
In Partial Fulfillment of the Requirements of the Degree of Master of Science in Management

Embry-Riddle Aeronautical University
Extended Campus
Huntsville, AL Center
September 2012

Training, Experience, or Time: Which is Most Important to Managing Classified Systems?

by

Jeremy B. Blevins

This Graduate Capstone Project
was prepared under the direction of the candidate's Project Review Committee Member,
Dr. Robert Wietzel, Adjunct Associate Professor, Extended Campus,
and the candidate's Project Review Committee Chair,
Dr. Charles Roberts, Adjunct Professor, Extended Campus, and has been approved by the Project Review Committee. It was submitted to the Extended Campus in partial fulfillment of
the requirements for the degree of
Master of Science in Management

PROJECT REVIEW COMMITTEE:

Dr. Robert Wietzel
Committee Member

Charles Roberts
Committee Chair

Abstract

Researcher: Jeremy B. Blevins

Title: Training, Experience, or Time: Which is Most Important to Managing Classified Systems?

Institution: Embry-Riddle Aeronautical University

Degree: Master of Science in Management

Year: 2012

Cleared Defense Contractors (CDCs) play a critical role in the research and development of classified information, weapons, and information systems in many of the developed nations around the world. As such, they must employ Information Systems Security Managers (ISSMs) to manage their classified information systems. Many ISSMs fulfill their Information Systems Security duties in a less-than-fulltime capacity, and there are no published requirements to be an ISSM. It is up to the Contractor and/or the ISSM himself to determine what the best mix of training, experience, and time allocated to perform Information Systems Security duties commiserate to the level of the complexity of the particular classified environment. The researcher has surveyed a diverse group of ISSMs to determine that on average, training is perceived to be most important to managing classified systems.

Keywords: Cleared Defense Contractors, Information Systems Security Managers, training, classified systems lifecycle management

Table of Contents

List of Tables

List of Figures

Chapter I

I Introduction

Background of the Problem

Cleared defense contractors (CDCs) play a critical role in the research and development of classified information, weapons, and information systems in many of the developed industrial nations around the world. In order to protect its secrets, a nation puts a regulation or policy in place by which the contractor companies must protect the technology that they are developing. In the United States, this regulation is the National Industrial Security Program, with its guiding document, the National Industrial Security Program Operating Manual (NIPOM) (Defense Security Service, 2006).

Many CDCs develop technologies on classified information systems located on their premises, as opposed to doing all of the work on a military installation. These contractor-managed systems must comply with requirements outlined in NISPOM Chapter 8, Information Systems Security. The requirement is on both contractor-owned equipment and Government Furnished Equipment (GFE). All contractors engaged in classified computing must appoint an Information Systems Security Manager (ISSM), and each computer system that will be used to process classified must have a System Security Plan (SSP). The ISSM may also appoint Information Systems Security Officers (ISSOs) to assist with the management of the classified information system. The computer system that has received approval to process classified data is referred commonly as an accredited information system (AIS). Before the contactor can begin processing classified, the ISSM must configure the Information System (IS), certify that it meets the NISPOM Chapter 8 requirements, and submit the SSP package to the

Designated Approving Authority (DAA). The DAA then reviews the submission, and barring discovery of major discrepancies, issues an Interim Approval to Operate (IATO). This IATO lasts 180 days, during which time the government agency responsible for ensuring compliance with the NISP visits the contractor with the computer system. This visit is to ensure NISPOM Chapter 8 compliance, and ensure that the ISSM is capable of performing all of the responsibilities outlined for an ISSM in Chapter 8. Upon IATO receipt, the contractor can then begin processing classified information on the accredited information system. After the agency has been satisfied that the system meets all of the requirements, the DAA issues a final Approval to Operate (ATO) that is valid for three years.

The steps required to receive accreditation are well documented, but the problem a contractor faces is that the management of the classified information systems lifecycle is not. NISPOM Chapter 8 is short. It does not define the qualifications of an ISSM. It only defines what the ISSM is responsible for.

Researcher's Work Setting and Role

The researcher is a Graduate student pursuing a Master of Science in Management. He has a Bachelor of Business Administration and a Graduate Certificate in Project Management. He has six years military experience; over ten years in Information Technology; six years in Industrial Security. In his current role as Information Systems Security Manager, the researcher has oversight of his entire employer's accredited information system implemented in its offices around the United States.

Statement of the Problem

The purpose of this capstone project was to determine which element, training, experience, or time allocated to perform the job, is more important to managing classified information systems.

Significance of the Problem

Contracts requiring accredited information systems can be severely impacted by the time it takes to receive an IATO, which is the first milestone in the lifecycle management of classified information systems. If receipt of an IATO is delayed and the contractor cannot immediately place, in temporary slots, the staff intended to work on the AIS, idle staff or layoffs could result. On time sensitive projects, it could mean missing critical deadlines and possibly losing funding. On mission-critical projects, it could be the difference between life and death for the soldier engaged in combat.

Given the role of the ISSM in managing classified information systems, a heavy burden lies on her shoulders. Any deficiencies she has in training, experience, or the time allotted to perform IA/IS job functions could be detrimental to the overall effort to manage AIS lifecycles. To compound this problem, the ISSM does not have many resources to investigate as to how to perform the job. Most of the publications that address sensitive information systems assume they are government owned and operated, and that they will be attached to the Global Information Grid (GIG). These documents are predominantly inapplicable to systems under the jurisdiction of the NISPOM. The documentation that does exist for NISPOM-compliant systems is purposefully terse to allow contractors a great degree of flexibility in meeting their contractual requirements. This leaves cleared defense contractors, and often the ISSMs themselves, to determine

their own criteria for managing their classified information systems. The dilemma is compounded when contractors, or even the ISSMs assigned, do not have an understanding of the complexity of the systems they are attempting to have accredited, or a realistic view of the timelines involved. Consequentially, complications might occur in the accreditation process, and contractors run the risks mentioned above.

This capstone project can serve as a resource to the contractor community in that it captured, via a survey of security practitioners, the concerns that existed within the CDC community, and then developed the concept of an "average ISSM", against which contractors could baseline the role of ISSM in their organizations. They could then adjust their security programs to strengthen their ISSMs in areas that need improvement, and use strong ISSMs to mentor other ISSMs that might be weak. CDCs could also use this project as a source of introspection. Have they been supportive of the security measures that needed implementation? Have they provided their ISSMs with adequate training opportunities?

This project provided a metric by which CDCs could evaluate their own efforts to manage their classified information and answered the question: Which is most important to managing classified information systems, training, experience, or time? Answering this question has not just been an academic exercise. ISSMs can look at the results provided and compare their experiences with those of others in their field. This project can serve to open a dialog within the contractor community on how to improve the management of classified information systems across the spectrum and better protect the technologies that the United States uses in maintaining its battlefield advantage. A contractor with a proven record of efficient classified information systems management can establish a

reputation amongst its government customers of effectively protecting the classified information it has been entrusted with. The consequences to the contractor who has not managed its classified information systems well could result in lost contracts, or even worse for a defense contractor, the loss of its security clearance and the ability to bid on future classified contracts.

The greatest beneficiary of this research, however, has been the researcher himself. Through the course of this project, the researcher has been able to analyze his own strengths and weaknesses and improve his abilities as an ISSM managing classified information systems.

Assumptions

The researcher assumes that only the period of time from the decision establish a classified information system to the submission of the SSP can be positively impacted by the ISSM. For the most part, the period from the submission to the issuance of the IATO lie outside of the ISSM's control. There are some exceptions that will be explained. After the SSP is submitted, the ISSM may be required to revise the SSP prior to the issuance of an IATO. Delay in making these revisions and resubmitting the SSP could negatively impact the time it takes to obtain the IATO. The level of experience of the ISSM could be a delaying factor as well. If the government agency determines that the ISSM lacks experience for the level of complexity of the accredited information system under review, it may determine not to issue an IATO. It could instead perform an inspection of the AIS without having approved it to process classified. In this case, if the inspector is satisfied

with the results of the inspection, a final Approval to Operate (ATO) would be issued without the AIS ever having been issued an IATO.

Limitations

The scope of this project is limited to computer systems that fall under the NISP. Given the proprietary nature of international defense industries, the findings of this study may not be applicable outside the United States. This study did not delve into discussions of accredited information systems in a way that could jeopardize United States national security interests.

The researcher used data available from his employer to analyze the problem. This was a small subset of information, as it would not be feasible to obtain an expanded array of data due to the nature of business. Many organizations would be uncomfortable giving up data that might expose undisclosed weaknesses in their security program.

Surveys were used to determine the average experience and education of ISSMs within the CDC community. Given the specialization of the role, this was a very small sampling of individuals, but it gathered the relevant data with regard to information systems accredited under the NISP.

List of Definitions

Accreditation - The official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. (NISPOM, 2006)

Certification - The comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the

accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. (NISPOM, 2006)

Interim Approval to Operate - Temporary authority to operate an IS. (NISPOM, 2006)

List of Acronyms

AIS - Accredited Information System

ATO – Approval to Operate

CDC – Cleared Defense Contractor

CSA – Cognizant Security Agency

DAA – Designated Approving Authority

DSS – Defense Security Service

ERAU – Embry-Riddle Aeronautical University

GCP – Graduate Capstone Project

GFE – Government Furnished Equipment

GIG – Global Information Grid

IATO – Interim Approval to Operate

IS – Information System

ISSM – Information Systems Security Manager

ISSO – Information Systems Security Officer

MSM – Master of Science in Management

NISPOM – National Industrial Security Program Operating Manual

SSP – Systems Security Plan

Chapter II

II Review of the Relevant Literature

NISPOM

At the present time, the researcher has not been able to source much information on the specific problem of reducing the time it takes to receive an Interim Approval to Operate for Accredited Information Systems. In lieu of research on this specific issue, more general sources on the implementation of implementing information systems were evaluated and then relevant data that is applicable to the problem herein discussed was extrapolated.

Before reviewing general information system sources, a baseline understanding of the requirements of processing classified information needs to be laid out. The primary source of information for any contractor engaging in industrial security, automated or otherwise, is the National Industrial Security Program Operating Manual (Defense Security Service, 2006) .

Chapter 8 of the NISPOM outlines the requirements for Information System Security. Section 1 of that chapter outlines the responsibilities and duties of the contracting company. The contractor is required to appoint an Information Systems Security Manager in each facility engaged in classified computing who is responsible to the federal government for the Accredited Information Systems operated in that facility. The ISSM is required to properly manage the security aspects of the classified system(s), provide training to all cleared employees working on the classified system(s), maintain documents and monitor the classified system(s), and periodically inspect the system(s).

Unfortunately, this broad list of responsibilities is not followed by a list of qualifications that the contractor company should look for in a candidate for ISSM.

The next section of the NISPOM outlines the certification and accreditation process. Certification as defined by the NISPOM is “the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.”. Accreditation, per the NISPOM, is “the official management decision to permit operation of an IS in a specific environment at an acceptable level of risk, based on the implementation of a CSA (Cognizant Security Office) approved set of technical, managerial, and procedural safeguards.”. This section then goes on to define other relevant terms and concepts to the certification and accreditation process. It is the responsibility of the ISSM to prepare the system for certification and accreditation and make the submission to the government for approval.

Section 3 lays out the common requirements for Accredited Information Systems. A few key concepts to classified computing are defined here. Clearing is “the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. Sanitization is “the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before sanitizing. The distinction between these two concepts, while similar, is critical in protecting the potential spillage of classified information. The section then discusses more administrative areas of information systems security,

including identification and authentication management, maintenance, classification markings, personnel and physical security, protection of media, review of output and media (for classified content), and configuration management. These important topics are covered in a few paragraphs each, and only in generalities.

Section 4 of Chapter 8 outlines protection measures. This section covers topics such as protection profiles, levels of concern, and protection levels.

Section 5 covers special categories of classified computing. These types of systems deviate from the general type of system that is normally used in classified environments. The first type is a single-user, stand-alone system. This type does not use user accounts to differentiate between users of the system and has special requirements for operating. The next type is a periods processing information system. There are several criteria that can cause a system to engage in periods processing. The third type outlined is called a pure server, or a device that does not have general users or engage in general purpose computing. Another type described is a tactical embedded, data-acquisition, or special-purpose system. This type of system is generally stripped down and possibly hardened, and might be configured with no alterable storage capability. The last type of special system is one with group authenticators. These systems have a logon or logons that are shared amongst a group of individuals.

Section 6 outlines protection requirements for classified computing. It covers requirements for topics such as power, audit, backup and restoration, data integrity, data transmission, access, identification and authentication, resource control, session control, security documentation, separation of function, system recovery, system assurance, security testing, and disaster recovery requirements.

Section 7 discusses interconnected systems. This section refers to the interconnection of local area networks (LAN), and not the interconnectivity of an individual LAN itself. It provides guidance for the documentation requirements and other administrative tasks associated with the interconnected network. It also defines the functions of a controlled interface and requirements for maintaining one.

While Chapter 8 of the NISPOM tells an ISSM what must be done to meet accreditation requirements for an information system, it does not go into technical detail or cover any type of computer system. It is agnostic to any particular hardware or software platforms, and through its vagueness has the potential to survive major technology changes while remaining relevant to the task of regulating classified computing. It provides no guidance to the ISSM on the type of background or experience needed to accomplish the requirements outlines within it.

Industrial Security Field Operations Process Manual

Supplementary to the NISPOM, and just as binding on accredited information systems is the Industrial Security Field Operations Process Manual for Certification and Accreditation of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM), or ISFO PM (Defense Security Service, 2011). This document has been revised more recently than the NISPOM itself, and goes into greater detail on the requirements outlined in NISPOM Chapter 8.

Section 1.3 details the three primary information system types that exist in the contractor realm. The first is a multi-user, stand-alone system (MUSA). Per the ISFO PM, around half of the systems submitted for accreditation fall into this category. This type of system generally has multiple general users. All of the mainstream Operating

Systems for general purpose computing in the last decade have the ability to support multiple users, even if they are only used for a single user. A system configured as MUSA does not have connectivity to any other systems. The second type of system is a Local Area Network (LAN). LANs consist of two or more computers connected via a cross-over cable or dedicated network hardware, but are a short distance from each other, such as an isolated network in a lab. LANs can be configured for peer-to-peer authentication with user accounts local to each computer, or user accounts can be centrally managed via some type of authentication server. The third type of system is a Wide Area Network, or WAN, which consists of LAN segments that are interconnected via routers across public communication lines. In a classified computing environment, LAN segments on a WAN must be protected with approved encryption hardware and must meet stringent requirements. Whereas a MUSA or LAN requires a System Security Plan (SSP) that outlines how the accredited information system will meet NISPOM Chapter 8 compliance, a WAN additionally requires a Network Security Plan (NSP).

Section 2 of the ISFO PM expands on the NISPOM's certification and accreditation requirements. The life cycle of an accredited information system begins with the submission of an SSP or Master SSP (MSSP) by the ISSM, then the issuance of an Approval to Operate (ATO) by DSS, and completes with the disestablishment of the accredited information system when it is determined that there is no longer a need to process classified information. Preliminary to the submission of the SSP, however, exists the greatest unknown in the process, the actual preparation and configuration of the hardware and software to be integrated as the AIS. It is not until this has been completed that the life cycle can begin. Only after this has been done can the ISSM submit the SSP

for approval. After it has been submitted, the agency responsible will assign it to a agent who will review the SSP, and if the paperwork is in order, process it for an Interim Approval to Operate. The IATO is the green flag for the contractor to begin processing classified information. The agent, may however, required corrections and revisions to the SSP prior to granting the IATO. After the IATO has been issued, the agent will normally schedule an onsite visit to review the system. If the visit is satisfactory, an Approval to Operate (ATO) is issued, otherwise, necessary corrections must be made prior to issuance. The ATO is valid for three years, at which time it can be renewed for an additional three years. The life cycle ends when the accreditation for the system is removed.

Section 2.3 outlines the three types of security plans, which have already been mentioned. The SSP is used for a system that will not have additional similar systems added by the contractor in the future. A MSSP is the same in structure as a SSP, but allows the ISSM the opportunity to "Self-Certify" additional "Like-Systems" at a future date. A like-system is one whose security relevant features are identical to the original system that the MSSP was submitted for. The benefit of placing systems under a MSSP instead of a SSP is that the future systems do not have to undergo the full accreditation process and can begin processing classified information without waiting for an official review or additional ATO. The other major type of security plan is the NSP, which is additional to the (M)SSP and covers the interconnectivity aspects of a WAN.

The ISFO PM goes on in subsequent sections to provide a paragraph or two on technologies that might be implemented and controlled, such as antivirus software, USB devices, and thin clients. Other than provide an overview, nothing is discussed in enough

depth as to provide the ISSM with guidance as to how to implement those technologies in his or her environment. The ISFO PM does, however, include several appendices with more detail on how to accomplish the administration of an accredited information system from a paperwork perspective. It outlines the proper formats for submissions and the correct verbiage to use.

Standardization of Baseline Technical Security Configurations

Given these two documents, an ISSM can know what she is expected to manage and maintain, but no guidance is provided in them on how to go about accomplishing the requirements outlines. This is understandable given the variety of operating environments that might be implemented. The agency that publishes the NISPOM and the ISFO PM has, however, provided one document for the configuration of one popular operating environment. The Standardization of Baseline Technical Security Configurations (Defense Security Service, 2009) provides a step-by-step guide for configuring a Windows® based computer to meet the NISPOM Chapter 8 requirements. This document assumes that the ISSM is familiar with the Local Policy Editor and changing permissions on directories, or that the ISSM at least has someone available to him to assist in those areas. For the ISSM who is unfamiliar with systems administration, the information provided can be daunting.

DoD Directive 8570.01-M

Another valuable document in understanding Department of Defense (DoD) computer security is the DoD Directive 8570.01-M, Information Assurance Workforce Improvement Program (Department of Defense, 2012). This document, while not required for accredited information systems under the oversight of the Defense Security

Service, focuses on the training of Information Assurance workers, which the ISSM can be classified as. This directive outlines the certifications that personnel interacting with DoD computer systems are expected to obtain, based on their role and interaction level. Certification requirements are detailed for Information Assurance Technicians, Information Assurance Managers, Computer Network Defense Professionals, and Information Assurance Systems Architects and Engineers.

There are three levels of Information Assurance Technician (IAT) certifications. Level I is the entry level for IATs and one of three certifications can meet the requirement: A+, Network +, or Systems Security Certified Practioner (SSCP). Level II requirements can be satisfied with the GIAC Security Essentials Certification (GSEC), Security +, Security Certified Network Professional (SCNP), or SSCP. Level III requires Certified Information Systems Auditor (CISA), GIAC Security Expert (GSE), Security Certified Network Architect (SCNA), Certified Information Systems Security Professional (CISSP) or Associate (CISSA), or GIAC Certified Incident Handler (GCIH).

The Information Assurance Manager tract requires a certification from IAT Level III and has three levels of its own. IAM Level I requires either: Certification and Accreditation Professional (CAP), GIAC Information Security Fundamentals (GISF), GIAC Security Leadership Certification (GSLC), or Security +. Level II can met by having: CAP, GSLC, Certified Information Systems Manager (CISM) or CISSP/ CISSA. The certification options for level III are: GSLC, CISM, or CISSP/ CISSA.

Computer Network Defense Professionals are subdivided by role. CND Analysts must have either GIAC Certified Intrusion Analyst (GCIA) or Certified Ethical Hacker (CEH). CND Infrastructure Support personnel must have either SSCP or CEH. CND

Incident Responders must have one of the following: GIAC Certified Incident Handler (GCIH), CERT®-Certified Security Incident Handler (CSIH), or CEH. CND Auditors must have one of the following: CISA, GIAC Systems and Network Auditor (GSNA), or CEH. CND-SP Managers must either CISSP-ISSMP (Information Systems Security Management Professional) or CISM.

Information Assurance Systems Architects and Engineers have three levels of certification. Both Levels I and II require CISSP/ CISSA. Level III requires either CISSP-ISSAP (IS Security Architecture Professional) or CISSP-ISSEP (IS Security Engineering Professional.

The rest of the document goes on in greater detail outlining the different roles mentioned above. It bears notice, however that this directive does not currently apply to systems accredited by the Defense Security Service. DSS leaves the qualification requirements for an ISSM solely to the contractor company.

The Problem

Given that DoDD 8570.01-M does not apply to contractors performing classified work on their own systems in the own locations, a dilemma can arise as to how the contractor either hires or trains an individual to fulfill the duties of an ISSM outlined in the NISPOM to a level that allows the ISSM to effectively manage the classified system lifecycle. Without government requirements for training and qualifications, the contractor is left to its standard Information Technology practices to determine how to best meet the need. To develop a broader understanding, a look outside defense contracting is in order. Application must be made from other sources within the greater IT community.

Leading Geeks

Given that there is no innate requirement for the ISSM to be an overtly technical person, she must have at her disposal an individual who is. This individual should serve as the ISSO under the non-technical ISSM. The ISSM must understand how to manage not only the administrative aspects of the accredited information system, but also provide guidance to the ISSO. The ISSM must understand that leadership is not a general practice that can be applied turn-key from one business discipline to another (Glen, 2003). The book *Leading Geeks* goes provides insight into non-technical managers successfully managing technical personnel. The word "geek" is used unceasingly through this text as a term of endearment. The text takes an anthropological look at the geek and "geekwork" to provide a framework of understanding for the non-technical manager. Geekwork can be seen as a variety of activities revolving around technology and the often creative solutions that must be undertaken to accomplish the given task. Whereas in other work environments there is a leader and worker relationship, highly technical fields must add a third member to the relationship, the technology itself.

Geek stereotypes abound, but as technology has advanced, the geek has moved from the sci-fi convention to the mainstream of society. The difference lies in the emotion for the technology that many geeks express. Many technology workers have a strong passion for their occupation and the opportunity to work on the cutting edge. Generally, a professional has the standard mindset of the occupation he is engaged in. For the geek, it is a mindset of problem and solution. When a situation arises, the problem is determined, and the solution sought out.

One concept from the text that applies in setting up accredited information systems under the NISPOM is that ambiguity rules. While many systems may follow a standard path using a common Operating System, others have special needs and are inherently more difficult to implement and poorly documented. This ambiguity is where much time can be spent in the system development phase and can often pose more of a challenge in figuring out how it can be done than it does in actually implementing it. A major issue that can arise from this is time estimates in completing the current task. A technical person may have a strong opinion of the time it takes to accomplish a particular item and completely miss the mark.

The rest of the text goes in more detail on geek leadership and how geek leaders can direct the technology professionals in a manner that is conducive to accomplish the tasks before them with success.

Managing Information Technology Projects

Being an ISSM, to an extent, involves managing a technology project inside the greater government contract project. The accredited information system lifecycle may or may not be accounted for by the actual project manager, but the work must still be accomplished and NISPOM compliant. It is thus important for the ISSM to understand how to apply project management concepts to meet this objective. Research shows that 80-90% of software projects fail, and 30-45% of all systems fail (Taylor, 2004). In defense contracting, this rate of failure is not an option. Relevant to the accredited information system lifecycle, two of the most significant problems in the project management process are training and mentoring and implementation plans.

Another important topic covered in this text is project and systems development lifecycles. The general phases of an IT project are initiation, planning, monitoring and controlling, closeout, and customer service and system maintenance. The lifecycle of an accredited information system deviates from this slightly because after closeout, the contractor is no longer authorized to operate the system.

Other important topics of project management and systems engineering are covered in this text. While the ISSM need not be an expert in this area to complete her job, a basic understanding would be beneficial.

Getting Things Done When You Are Not in Charge, Second Edition

One of the biggest hurdles that an ISSM may face in managing the lifecycle of an accredited information system is that ultimately, he is not in charge of the system. He is only there to ensure compliance with the NISPOM. This can be a challenge, and this is where the ISSM must know how to meet his obligation to the government to ensure the integrity of the system. A good source for information on accomplishing this is *Getting Things Done When You Are Not in Charge* (Bellman, 2001). One of the key concepts to extract from this text are the five steps to discovering reality. The first step is to identify the issue. The second is to gather information. The third is to know and understand the information gathered. The fourth is to respect and accept what others have done. The final step is to decide and act based on the knowledge acquired. Another important point in the text is to accept other's lack of knowledge. In a team, each person may have some unique knowledge and it should not be taken for granted that the others on the team have any knowledge in that area, or have any interest in learning it. Many people only are concerned with something to the point that it relates to their job.

Software Verification and Validation: A Practitioner's Guide

Although *Software Verification and Validation: A Practitioner's Guide* (Rakitin, 1997) focuses on developing code, the lessons it presents can be applied to the accredited information system lifecycle. This is especially applicable prior to receipt of an IATO. Figure 1. Plan-Do-Check-Act, illustrates the cycle of Plan-Do-Check-Act that all systems go through prior to accreditation.

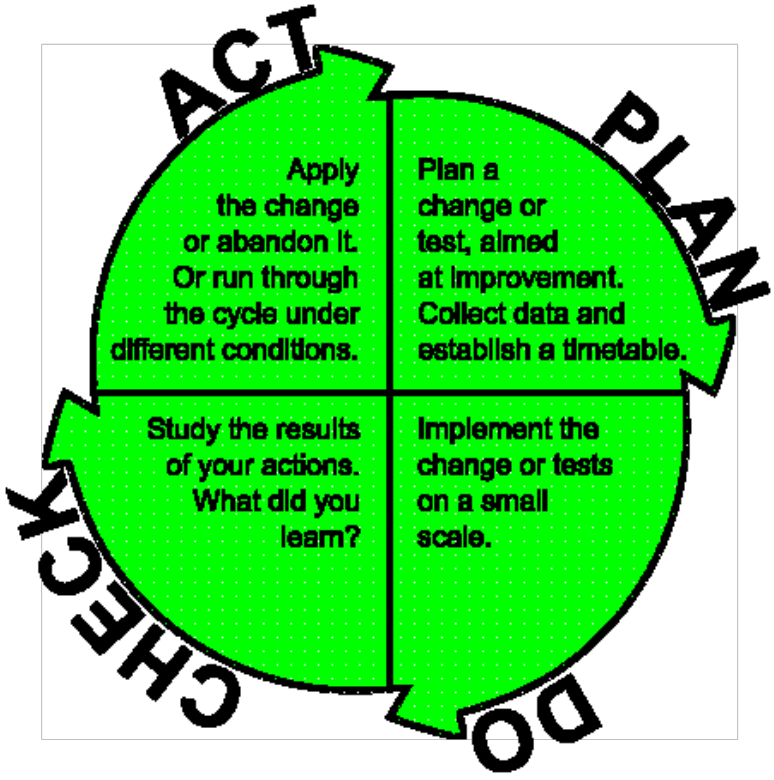

Figure 1. Plan-Do-Check-Act (Rakitin, 1997)

Another topic covered in this text is configuration management. Configuration management is critical because it documents and establishes a process by which the configuration of a system is changed. Software configuration management can be broken into three categories: identification, baseline management, and auditing and reporting. There are standard definitions (IEE Standards Association) applied to several relevant configuration management terms:

- Baseline: A baseline is a milestone in the software development process marked by the delivery of one or more software configuration items. A baseline consists of software configuration item(s) that have been formally reviewed and agreed on and that thereafter serves as the basis for further development. A baseline can be changed only through formal change control procedures.
- Software configuration item. A software configuration item is a collection of software elements treated as a unit for the purposes of configuration management.
- Configuration. A configuration is defined as consisting of a parts list and an exploded parts diagram that define all the elements of a baseline and how they fit together.
- Configuration control board (CCB). The CCB is responsible for reviewing and approving changes to baselines. The CCB usually consists of representatives of the project team.
- Software. Software, in the context of configuration management, is defined as information structured with logical and functional properties. It is created and maintained in many forms and representations over the course of its development.
- Version. A version is a specific instance of a baseline or a software configuration item.

Another critical aspect to verification and validation is auditing. There are three types of audits defined: functional, physical, and quality systems. Functional audits verify that the item being audited meets its functional and performance expectations. Physical audits ensure that the version of the software and documentation are consistent with what is

expected and ready for deployment. Quality Systems audits ensure that the quality assurance process has been followed and are normally conducted by outside parties.

Summary

The literature references above consisted is a culmination of the required government regulations and books on information technology as they pertain to software project management.

On one hand, there is the NISPOM and the ISFO process manual with their non-technical generalizations and ordinances of what must be done to be compliant. Also on the government side is the DoDD 8570.01-M that outlines training requirements for individuals working on DoD computer systems. Since the systems regulated under the NISPOM are not owned by the DoD, personnel working on them are not required to meet the training requirements that exist for the DoD owned systems. But, given the vagueness of the NISPOM and ISFO PM, it might be worth the effort of the ISSM to become familiar with and pursue the certifications outlined in DoDD 8570.01-M.

On the other hand, however, are the other books reviewed which focus on IT projects wherever they may exist. These texts did not get into the regulatory aspects that were outlined in the government regulations, but provided industry standard practices that can be applied to the classified computing environment. The ISSM can take away a plethora of information from these sources to improve the lifecycle management of a classified computer system.

The ultimate goal of this research is to determine if training, experience, or time allotted to perform IA/IS job functions has the greater impact on improving the process for receiving an IATO so that the actual classified work can begin.

Statement of the Research Question

The dilemma that any ISSM faces in bringing up a new classified computer system is the time between receiving the instruction to build the new system to actually being able to process classified information on it. This can be a frustrating time period because the no one can work on the system until it has been approved. This can lead to the actual users of the system sitting idle with unbillable time because they cannot execute work on the contract that they need to be working on. This can be frustrating for the project manager over the project because she does not have authority over the ISSM who she sees as holding up her staff. It can be frustrating for the ISSM because he may or may not have the expertise to configure the new system depending on its complexity. The ISSM may be at the mercy of an ISSO who does not work for him and might work for the project manager or some other department such as IT. All of this is factored into the greater equation of managing the classified system lifecycle. The ultimate question that this research aims to answer is simple: Which has the greater impact on improving the classified system lifecycle: training, experience, or time allotted to perform IA/IS job functions?

Chapter III

III Research Methodology

Research Model

This Graduate Capstone Project was conducted as a descriptive study whose research variable was the activity that best improves the process managing the lifecycle of a classified system.

Survey Population

They survey population consisted of individuals serving in Information Systems Security/ Information Assurance positions within the United States cleared CDC community under the National Industrial Security Program who are members of the National Classification Management Society (NCMS).

Sources of Data

The sources of data for this capstone project were responses to an Internet-based survey, enumerated in Appendix C Data Collection Device.

Data Collection Device

The data collection device for this capstone project was a survey. The survey consisted of a series of single-answer questions relevant to the issue of managing the lifecycle of a classified system. This survey was available to the survey population via the Internet and requests were sent out based on membership in NCMS. The survey was constructed based on the duties of serving as an ISSM for a cleared defense contractor under the NISP and requirements for operating an accredited information system, as outlined in the Industrial Security Field Operations (ISFO) Process Manual. The

independent variable in this survey was that all respondents were involved in information systems security. Dependent variables included:

- Nominal: Primary role, education level, certifications
- Ordinal: Experience, hours a week spent on information systems security, time needed to complete tasks
- Interval: Rating of statements

Each of these variables is interrelated with the efficiency of managing a classified system lifecycle. This information, when correlated, helps to build the profile of the average ISSM/ISSO.

Pilot Study

A pilot study was conducted using the researcher's experience as an Information Systems Security Manager.

Instrument Pretest

Other Information Systems Security Managers/ Officers were solicited to review the survey questions and provide feedback prior to launching the survey online. The questions were distributed to peer ISSMs via an electronic document to allow for feedback on the questions.

Distribution Method

The data collection device was hosted on www.surveymonkey.com. The researcher contacted the NCMS board member who was the Chair of its Information Systems Security Committee. The researcher explained the purpose of the survey and requested he email the survey link to all of the Information Systems Security

professionals associated with the committee. The Chair obliged and sent the link out to the committee membership.

Instrument Reliability

The reliability of the instrument was difficult to determine, since it was based on the honesty of the individual respondents. Given the target population, however, the researcher feels a measure of confidence that those who participate in the survey responded accurately and honestly.

Instrument Validity

Steps were taken to ensure the validity of the data gleaned from the survey. Only individuals involved in Information Systems Security were polled. Given the relatively small number of individuals meeting the criteria of Information Systems Security Managers/ Officers, the number of responses to the survey received provided a reasonable representative sample. The content of the survey questions was validated by vetting them through the pilot survey prior to deploying the final survey online.

Procedures

After the survey was advertised via email and the respondents had opportunity to complete the instrument, the results were collected and analyzed to develop descriptive statistics of the respondents' preference to training, experience, or time allotted to IS activities. This allowed the determination of whether the responses proved or disproved the researcher's theory that training is the most important aspect of managing the lifecycle of a classified system.

Assumptions

The researcher assumed that the data gathered from this instrument is a modest sampling of practitioners in the field of classified information systems security, given the extreme specialization of the field. The researcher also believed the data collection device deployed was the best means of gathering the information needed for this effort. Also assumed was that individuals responded honestly and accurately as the questions related to their personal experiences with managing classified information systems.

Limitations

The data collected data collection device was limited to the input of a group of information security professionals who were members of a specific national organization. A greater sampling could possibly have been taken had the instrument been advertised to a greater audience, but given time constraints and lack of visibility to the greater IS professional community, the researcher limited participation to the group mentioned previously.

Ethical Assurances

Individual respondents were not asked to provide any personally identifiable information. The ability of the data collection device to store the respondent's IP address in the survey results was disabled, thus removing the ability of one to trace back an IP address to an individual respondent or owner of the block of IP addresses that the connection originated from.

Treatment of Data

Quantitative analysis was conducted on the data. Since the primary goal of this project was to determine which the greater importance between training, experience, and

time to perform tasks with regards to managing classified systems lifecycles (Question 7, h-j), histograms were used to evaluate the data. Once the three preference groups had been determined, the remaining data sets were sorted in histograms based on training, experience, or time preference. The interval data (Question 7, a-g) were treated as discrete and followed a normal distribution.

Chapter IV

IV Results

The Survey

Seven questions were posed to the survey respondents. The first several questions gathered information on the respondent's background with regard to managing accredited information systems. Questions one and two focused on the individuals role in information security and the amount of time per week were spend performing IS security duties. Question three was related to years of experience. Question four asked the respondents what their education level was. Question five involved computer certifications. Although certifications are not required for IS positions related to DSS-accredited information systems, The list of acceptable certifications identified in DoD Directive 8570.1, Information Assurance Workforce Improvement Program, was used to populate this question.

Question six consisted of three parts related to how long it takes the respondent to complete a (M)SSP submission for a typical system. The first part asked how long it took to complete the system configuration, alone or with other IS staff. Configuration begins with a computer or computers without Operating Systems installed on their hard drives. It concludes with a functional computer with its operating system and all necessary software installed. The second part of the question dealt with implementing and certifying the security requirements of the system. This involves the individual configuring security settings and then certifying that the systems meet the required security baseline. The last part of the question dealt with completing and submitting the

SSP package to the DAA. This involves preparing all of the necessary documentation and submitting it to the DAA with a request for accreditation.

Question seven asked the respondents to rate a series of sub-questions on a scale ranging from "Strongly Disagree" to "Strongly Agree". The last three sub-questions of question seven asked which was most important: Training, Experience, or adequate Time for IA/IS duties. The data were then analyzed based on the "agree" and "strongly agree" responses with regard to Training, Experience, and Time.

Is training most important to a computer security program?

As shown in Figure 51**,** 88% of those surveyed viewed training as most important to managing a successful computer security program. Of this group of respondents, a few conclusions can be reached when their other responses are analyzed. A Majority of them were IA/IS managers, whether that was as an Information Assurance Manager or an Information Systems Security Manager. The data were inconclusive concerning hours a week spent on information systems security. A majority had more than ten years of experience in information technology, with a large plurality likewise having more than ten years of experience in information systems security. A majority of individuals held a Bachelor's or Master's degree. Most respondents did not have a computer certification, but of those who did, most of them were Certified Information Security Professionals (CISSP).

Table 1 shows the response breakdown concerning the time the respondents took to go from beginning system configuration to complete and submit a SSP package to their DAA.

Table 1

Pro-training SSP submission times

Configuration to Submission	Complete system configuration	Implement and certify security requirements	Complete and submit SSP package to DAA
<1 Day	30.4%	21.7%	13%
2 days – 1 week	43.5%	56.5%	43.5%
1 - 2 weeks	17.4%	8.7%	26.1%
3 - 4 weeks	4.3%	4.3%	13%
4 – 8 weeks	-	4.3%	-
>2 months	4.3%	4.3%	4.3%

Note: Percentages represent the subset of individuals who responded in favor of training as most important to a successful computer security program.

Three other questions address the issue of training. When asked if they felt that additional training would shorten the time it takes to complete a submission, a consensus was not reached. There were nearly as many individuals on the negative end of the spectrum as there was on the positive, with a small plurality that neither agreed nor disagreed. The same group had a slightly different view concerning their employer providing adequate training for their job function. A majority of respondents believed that their employers did provide adequate training. A mixed opinion existed with regard to the adequacy of training provided by the DAA.

Table 2

Pro-training responses to other training questions.

Question	Strongly Disagree	Disagree	Neither Agree/ Disagree	Agree	Strongly Agree
Additional training would shorten the time it takes me to complete a submission.	8.7%	21.7%	39.1%	17.4%	13%
My employer provides adequate training for my job function.	8.7%	13%	17.4%	47.8%	13%
My DAA provides adequate training for my job function.	4.3%	26.1%	39.1%	30.4%	-

Note: Percentages represent the subset of individuals who responded in favor of training as most important to a successful computer security program.

The group was also asked if other job duties impeded their ability to perform their IA/IS duties. No definitive conclusion could be drawn from their responses. Almost as many respondents disagreed as agreed.

The results were more definitive; however, when the respondents were asked about the impact of others on helping do their jobs better. 43.5% each either agreed or strongly agreed that interacting with other IA/IS professionals helped them do their jobs better. Only 13% held a neutral opinion. 43.5% agreed that being a member of a professional organization focused on IA/IS helped them do their jobs better, with an additional 32.8% strongly agreed. The remaining 21.7% held a neutral opinion.

When asked directly if their experience allowed them to perform security-relevant tasks without additional training, a 52.1% concurred, with 21.7% disagreeing, and the remaining 26.1% having no opinion.

Is Experience More Important to a Computer Security Program?

Figure 52 shows that 80.8% of respondents viewed experience as most important to maintaining a successful computer security program. The responses of this group can also be analyzed to draw conclusions. A slightly higher percentage of respondents, 76.2%, were ISSMs or IAMs. They were statistically similar with regards to time spent performing IA/IS functions and years in information systems in general, but had more years of experience in information systems security (Figure 33). This group had similar educational accomplishments and certifications to the group that showed preference to training.

Table 3 shows the response breakdown concerning the time the respondents took to go from beginning system configuration to complete and submit a SSP package to their DAA.

Table 3

Pro-experience SSP submission times

Configuration to Submission	Complete system configuration	Implement and certify security requirements	Complete and submit SSP package to DAA
<1 Day	23.8%	14.3%	4.8%
2 days – 1 week	47.6%	61.9%	47.6%
1 - 2 weeks	19%	9.5%	28.6%
3 - 4 weeks	4.8%	4.8%	14.3%
4 – 8 weeks	-	4.8%	-
>2 months	4.8%	4.8%	4.8%

Note: Percentages represent the subset of individuals who responded in favor of experience as most important to a successful computer security program.

Three other questions address the issue of training. When asked if they felt that additional training would shorten the time it takes to complete a submission, a consensus was not reached. There were nearly as many individuals on the negative end of the spectrum as there was on the positive, with a small plurality that neither agreed nor disagreed. The same group had a slightly different view concerning their employer providing adequate training for their job function. A majority of respondents believed that their employers did provide adequate training. A mixed opinion existed with regard to the adequacy of training provided by the DAA.

Table 4

Pro-experience responses to other training questions.

Question	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Additional training would shorten the time it takes me to complete a submission.	9.5%	23.8%	33.3%	19%	14.3%
My employer provides adequate training for my job function.	9.5%	9.5%	19%	52.4%	9.5%
My DAA provides adequate training for my job function.	4.8%	23.8%	42.9%	28.6%	-

Note: Percentages represent the subset of individuals who responded in favor of experience as most important to a successful computer security program.

The respondents who believed experience to be most important had similar responses (Table 3) to the pro-training group concerning other job requirements impeding with their ability to perform IA/IS functions. A slightly higher percentage agreed that interacting with other IA/Is professionals helped them do their jobs better Figure 48). They saw slightly less value in belonging to a professional organization focused on IA/IS (Figure 49).

This group was a little more confident that their experience allowing them to perform security-relevant tasks without additional training (Figure 50).

Is Adequate Time to perform IA/IS Duties Most Important to a Computer Security Program?

Those surveyed were given a third option with regard to most important to maintaining a successful security program: adequate time for IA/IS duties. 80.8% of respondents believed that time was most important. 76.2% of these respondents were IA/Is managers. They spend roughly the same amount of time as the other two groups each week on information systems security (Figure 30). This group, however, had more experience in general information systems and information systems security (Figure 33, Figure 34). Their education levels (Figure 36) and certifications held (Figure 38) were also similar to the other two groups.Table 5 shows the response breakdown in regard to the time the respondents took to go from beginning system configuration to complete and submit a SSP package to their DAA.

Table 5

Pro-time SSP submission times

Configuration to Submission	Complete system configuration	Implement and certify security requirements	Complete and submit SSP package to DAA
<1 Day	23.8%	23.8%	23.8%
2 days – 1 week	47.6%	52.4%	52.4%
1 - 2 weeks	19%	9.5%	9.5%
3 - 4 weeks	-	-	-
4 – 8 weeks	-	4.8%	4.8%
>2 months	9.5%	9.5%	9.5%

Note: Percentages represent the subset of individuals who responded in favor of time as most important to a successful computer security program.

Three other questions address the issue of training. Inconclusive results were reached when asked if they felt that additional training would shorten the time it takes to complete a submission, similar to the results of the other two groups with regards to this question. Results were likewise inconclusive with regards to employer-provided training.

The DAA was credited with providing adequate training more highly than it had been by the other two groups (Figure 46).

Table 6

Pro-time responses to other training questions.

Question	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Additional training would shorten the time it takes me to complete a submission.	9.5%	23.8%	33.3%	19%	14.3%
My employer provides adequate training for my job function.	9.5%	9.5%	19%	52.4%	9.5%
My DAA provides adequate training for my job function.	4.8%	23.8%	42.9%	28.6%	-

Note: Percentages represent the subset of individuals who responded in favor of time as most important to a successful computer security program.

The respondents who believed that adequate time for duties to be most important held a stronger opinion that other job duties impeded with their IA/IS duties than the other two groups did (Table 1,Table 3). 95% agreed that interacting with other IA/Is professionals helped them do their jobs better (Figure 48). 71.4% agreed that belonging to a professional organization focused on IA/IS helped them do their job better (Figure 49).

This group was slightly more neutral to the statement that their experience allowing them to perform security-relevant tasks without additional training than the pro-experience group was Figure 50).

Training is more important

Based on raw statistical figures, more respondents stated that they viewed training to be more important to maintaining a successful computer security program.

Chapter V

V Discussion

What does the typical ISSM look like?

The questions in the survey began by gathering factual information about the respondent and then finished out by asking a battery of opinion questions. Based on the answers provided, the researcher built a composite sketch of a typical Information Systems Security Manager.

This composite ISSM spends an average of 40+ hours a week performing his job. He has greater than ten years' experience in information systems in general, and information systems security in specific. He has a Bachelor's Degree, but has not placed much emphasis on computer certifications. If certifications are obtained they are either CompTIA certifications such as A+, Network+, or Security+, or (ISC)2's Certified Information Systems Security Professional (CISSP) certification.

Concerning preparation of a system to be submitted for accreditation, she usually can completely configure a system in two days to a week, with or without assistance from other staff. Locking the system down and certifying the security requirements takes an additional two days to a week. Completing all required paperwork and sending the submission in is done in another two days to a week. In total, it can take her between six days and three weeks to go from a completely configured system to an ISSM certified system that is waiting accreditation.

With regard to his opinion on improving the time it takes to complete a submission and wait for accreditation, the ISSM had this to say: for the most part that additional training probably would not have an effect one way or the other on shortening

the time that it takes to complete a submission. His employer provides adequate training to perform his job. He is inconclusive as to whether his Designated Approving Authority could do a better job providing training for the task. Other job requirements, however, can impede his ability to perform the security tasks he has been assigned.

When questioned on interacting with peers in Information Systems Security, the ISSM believed that interacting with others was a positive, for the most part, being involved in a professional organization focused on IA/IS helped her do her job better.

With regard to his confidence in his abilities, the ISSM leaned toward the thought that his experience allowed him to perform security-relevant tasks without additional training.

The last three questions with regard to which was most important to maintaining a successful security program posed a problem for the ISSM. In general, she viewed training, experience, and adequate time for IA/IS duties all as the most important; however, there she leaned slightly more toward training as being the greatest of the three.

Role

The majority of respondents were IA/Is Managers. There are no requirements levied for CDCs as to the type of candidate to fill this role (Defense Security Service, 2006). Many times this individual a manager of a system but not of the staff that works with the system. He must understand how to ensure compliance while giving direction to someone else's direct reports (Bellman, 2001).

Time Involved

Given that the responses to the time a week that is spent on information systems security was less than forty hours a week for a majority of respondents, it would appear

that most of them have other duties that occupy their time. These might or might not be computer or security related. Though not necessarily a project manager, an information systems security manager must engage in project-related activities in order to properly manage an established accreted information system, or to bring up a new system for accreditation (Taylor, 2004). He must understand the Plan-Do-Check-Act cycle in order to accomplish this as well (Rakitin, 1997).

Experience

The majority of respondents had over ten years of information systems experience and six years or more of information systems security experience. In that timeframe, much has changed in the computer industry, although the nature of operating in disconnected environments isolates the ISSM from some of those changes. This can be viewed one of two ways: either the ISSM has opportunity to perfect his skill set due to the stability of not adapting to Internet-based threats, or he stagnates because he is not exposed to Internet-based threats. An individual with at least six years of information systems security experience also most likely has dealt with two revisions of Chapter 8 the NISPOM. He also has seen the advent of the ISFO Process Manual, published DSS Baseline Standards, and a couple of revisions of the SSP templates. This legacy allows the ISSM to have an appreciation for the changes that have occurred in the streamlining and standardization that have occurred in the accreditation process.

Education/ Certification

Over half of the respondents held at least a Bachelor's Degree, with almost a quarter of all respondents having a Master's Degree. Only 11.5% of respondents did not have any college experience. Almost half of the respondents however did not hold any

computer certifications. It is worth noting that 47.8% of individuals who either agreed or strongly agreed that training was most important to maintaining a successful security program did not hold any computer certifications while almost 5% less respondents who said experience was most important were not certified.

There might be many variables leading to this that cannot be deduced from the data available, such as whether or not the individual is not certified because his employer does not pay for certifications, or the lack of certification requirements under the NISPOM. When asked if their employer provided adequate training, however, 61.6% of respondents agreed or strongly agreed. The type of training, however, cannot be determined since they survey did not directly ask. The result is a vagueness that is left open to interpretation.

The response to the question of the DAA providing adequate training is likewise inconclusive. The respondents were almost evenly split between agreeing, disagreeing, and not having an opinion on the topic.

Other job requirements

When asked if other job requirements impeded their ability to perform their IA/IS duties, the spectrum of answers leaned more toward agreement.

Interaction with others

None of those surveyed disagreed that interacting with other IA/IS professionals helped them do their jobs better. 46.2% of respondents agreed, and another 42.3% strongly agreed that such interaction helped them do their jobs better. It has been the experience of the researcher, that despite the small number of individuals across the country employed as ISSMs, they are well connected to each other. However,

membership in a professional organization focused on IA/IS was not esteemed quite as highly by the recipients. Slightly more than one quarter of those polled had no opinion, while 42.3% agreed, and only 30.8% strongly agreed.

Chapter VI

VII Conclusions

In the course of analyzing the survey results, it became glaringly apparent that the survey itself was flawed, but not in such a way that no results could be gleaned from it. The flaw in the instrument was this: respondents were not forced to select only one of the three options for “most important to maintaining a successful computer security program”. Respondents could agree or strongly agree that all three were most important, and many did. The limitations with the data collection device prohibited embedding logic in the survey to prevent this from occurring. Had the “most important” question been separated from the other opinion questions, it could have allowed the participants to only select one option as most important. It is the recommendation of the researcher that a more pointed survey would remediate the deficiencies discovered and allow for a more thorough study on the subject of the importance of training, experience, and time allotted to perform duties as they pertaining to their importance to managing classified information systems.

Chapter VII

VII Recommendations

Based on the research conducted, it would be the recommendation of the researcher that minimum training and education standards such as those outlined in DoD D 8570.01-M be levied on CDCs for DSS-accredited systems. This would remove some of the vagaries of operating contractor-owned hardware to process classified information. This would need to be gradually phased in to allow the ISSMs to obtain the required certifications that the Directive requires for administrators of government owned and operated information systems. Contractors would have to be prepared to absorb the costs of obtaining and maintaining certifications. Despite the drastic change this would force upon the contractor community, it would provide a documented baseline from which performance metrics could be generated.

Also, a corrected survey should be conducted to correct some of the deficiencies discovered in the instrument that this project deployed. It should be used to validate the revised hypotheses proposed. Additionally, the new survey should be executed annually to document changes in the survey population and to detect trends that may be relevant in improving contractor-owned classified information systems management.

Additionally, the Department of Defense should make efforts to centralize of one set of rules for all classified information systems, whether they are government or contractor owned. Divergent policies lead to variations in interpretation of the various regulations.

References

Bellman, G. M. (2001). *Getting Things Done When You Are Not in Charge, Second Edition.* Retrieved July 27, 2010, from Books24x7: http://common.books24x7.com/book/id_2942/book.asp

Caplan, D. (2005, December 20). *CHAPTER 5: FLEXIBLE BUDGETING*. Retrieved March 04, 2009, from Oregon State Unversity College of Business: http://classes.bus.oregonstate.edu/spring-06/ba422/Management%20Accounting%20Chapter%205.htm

Defense Security Service. (2006, February). *NISPOM (February 2006).* Retrieved 02 07, 2012, from U.S. Department of Defense, Defense Security Service: http://www.dss.mil/documents/odaa/nispom2006-5220.pdf

Defense Security Service. (2009, March). Standardization of Baseline Technical Security Configurations Version 2.2. Quantico, VA, US.

Defense Security Service. (2010 йил 07-March). *History*. Retrieved 2010 йил 10-June from Defense Security Service (DSS) Internet Home Page: http://www.dss.mil/about_dss/history/about_dss_history.html

Defense Security Service. (2011, June). Industrial Security Field Operations (ISFO) Process Manual Revision 3. Quantico, VA, US.

Department of Defense. (2012, January 24). *Information Assurance Workforce Improvement Program, Change 3.* Retrieved February 07, 2012, from Defense Technical Information Center: www.dtc.mil/whs/directives/corres/pdf/857001m.pdf

Garrison, R. N. (2008). *Managerial Accounting* (12th Edition ed.). Bostin, MA, United States of America: McGraw-Hill Irwin.

Glen, P. (2003). *Leading Geeks: How to Manage the People Who Deliver Technology.* Retrieved July 27, 2010, from Books24x7: http://common.books24x7.com/book/id_5387/book.asp

IEE Standards Association. (n.d.). *ANSI/IEEE 1042-1987 IEEE Guide to Software Configuration Management.* Retrieved July 27, 2010, from IEE Standards Association: http://standards.ieee.org/reading/ieee/std_public/description/se/1042-1987_desc.html

Rakitin, S. R. (1997). *Software Verification and Validation: A Practitioner's Guide.* Retrieved July 27, 2010, from Books24x7: http://common.books24x7.com/book/id_360/book.asp

Taylor, J. (2004). *Managing Information Technology Projects: Applying Project Management Strategies to Software, Hardware, and Integration Initiatives.* Retrieved July 27, 2010, from Books24x7: http://common.books24x7.com/book/id_6740/book.asp

Appendices

A Bibliography

B Permission to Conduct Research

C Data Collection Device

A Bibliography

Bellman, G. M. (2001). Getting Things Done When You Are Not in Charge, Second Edition. Retrieved July 27, 2010, from Books24x7: http://common.books24x7.com/book/id_2942/book.asp

Provides insight into working across departmental lines and through organizational politics to accomplish a goal even when one might not be in a position of authority over the individuals needed to accomplish one's goals. An ISSM might find himself in such a predicament. By employing the concepts covered in this text, he can work garner management support of the greater security objectives within the organization.

Defense Security Service. (2006, February). NISPOM (February 2006). Retrieved 02 07, 2012, from U.S. Department of Defense, Defense Security Service: http://www.dss.mil/documents/odaa/nispom2006-5220.pdf

The Department of Defense Directive that regulates CDCs with regards to protecting classified information. Chapter 8 outlines the requirements of managing a classified computing environment.

Defense Security Service. (2009, March). Standardization of Baseline Technical Security Configurations Version 2.2. Quantico, VA, US.

Provides Windows XP configuration for NISPOM Chapter 8 compliance. Following this guide allows ISSMs of varying levels of technical proficiency to prepare Windows XP systems for accreditation.

Defense Security Service. (2010, March). History. Retrieved 2010 10-June from Defense Security Service (DSS) Internet Home Page: http://www.dss.mil/about_dss/history/about_dss_history.html

Provides an overview of the history of the Defense Security Service.

Defense Security Service. (2011, June). Industrial Security Field Operations (ISFO) Process Manual Revision 3. Quantico, VA, US.

Provides additional guidance on meeting NISPOM Chapter 8 compliance.

Department of Defense. (2012, January 24). Information Assurance Workforce Improvement Program, Change 3. Retrieved February 07, 2012, from Defense Technical Information Center: www.dtc.mil/whs/directives/corres/pdf/857001m.pdf

Provides training and certification requirements for federally-employed information workers. Though not directly binding on CDC staff who work on NISPOM-accredited systems, it provides guidance on the types of certification that one can pursue to increase proficiency in technical areas.

Glen, P. (2003). Leading Geeks: How to Manage the People Who Deliver Technology. Retrieved July 27, 2010, from Books24x7: http://common.books24x7.com/book/id_5387/book.asp

Explores the dynamic of managing technologists that many non-technical individuals face. Given that DSS does not provide guidance on the type of candidate required to fill the role of ISSM, a CDC might place a non-technical person in this role. An understanding of how to manage the “geeks” one depends on to maintain a NISPOM-accredited system in that scenario would be

beneficial, both to the ISSM who understand the security requirements, and the technical staff who have to implement them.

Rakitin, S. R. (1997). Software Verification and Validation: A Practitioner's Guide. Retrieved July 27, 2010, from Books24x7: http://common.books24x7.com/book/id_360/book.asp

Discusses software development lifecycle models and how to implement them. The topics discussed in the text enhance the security professional's understanding of the C&A process of managing AIS lifecycles.

Taylor, J. (2004). Managing Information Technology Projects: Applying Project Management Strategies to Software, Hardware, and Integration Initiatives. Retrieved July 27, 2010, from Books24x7: http://common.books24x7.com/book/id_6740/book.asp

Provides guidance on implementing project management principles relevant to IT projects, whether they are software, hardware, or integration projects. Project management is often a core component in a CDC's program effort, but AIS lifecycles may not be included as a component of the project. By utilizing the material covered in this text, an ISSM can "projectize" AIS lifecycle management within the greater scope of the overall program effort.

B Permission to Conduct Research

CAO / IRB Review Form 1

For a research proposal involving human subjects, the Capstone Committee Chair must complete this form prior to Proposal Approval and forward it electronically to the ERAU- W CAO in accordance with instructions below. Note: As a minimum, Chapter Three of the Research Proposal (to include survey instrument if used) must accompany this submission.

Committee Chair Submission

Capstone Proposal Title: Training, Experience, or Time Allotted: Which is the Most Important Factor in Improving the Process for Receiving an IATO for an AIS?

Full Name of Researcher: Jeremy B. Blevins

Capstone Committee Chair: Dr. Rick Roberts

Proposal Research Methodology: (See attachment.)

Signature of the Committee Chair: [signature] Date: 22 Sept 12

ERAU CAO Review

This section is to be completed by the ERAU-W CAO and returned to the Capstone Committee Chair.

IRB Review Required: X Yes X No

Note: If the CAO determines an IRB is required, the Committee Chair will electronically forward this signed form to the researcher who will then complete the ERAU IRB Human Subjects Protocol Packet and forward it to the ERAU Office of Sponsored Research.

Signature of the ERAU-W CAO: [signature] Date: Oct 4, 2012

03

C Data Collection Device

Displaying **1** of **26** respondents

« Prev | Next » | **Jump To:** 1 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

31-40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?				X	
How many years do you have in information systems security?				X	

4. What is your education level?

Associate's Degree

5. Do you have any of the following computer certifications?

A+
CISSP
Network+
Security+

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?			X			

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.		X			
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.			X		
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.					X
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 2. Survey response 1.

Displaying **2** of **26** respondents

« Prev | Next » | **Jump To:** 2 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Edit Response | Delete
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

11-20

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?				X	
How many years do you have in information systems security?				X	

4. What is your education level?

Master's Degree

5. Do you have any of the following computer certifications?

Security+

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?	X					
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.					X
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.			X		
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.			X		
Training is most important to maintaining a successful computer security program.			X		
Experience is most important to maintaining a successful computer security program.			X		
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.			X		

Figure 3. Survey response 2.

Displaying **3** of **26** respondents

« Prev | Next » | **Jump To:** 3 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am a non-management IS/IA person (ISSO, systems administrator)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

CISSP

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?			X			
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?			X			

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.		X			
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.					X
My experience allows me to perform security-relevant tasks without additional training.					X
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.					X
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.					X

Figure 4. Survey response 3.

Displaying **4** of **26** respondents

« Prev | Next » | **Jump To:** 4 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?				X	
How many years do you have in information systems security?			X		

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

CISM

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?			X			
Implement and certify security requirements?			X			
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.	X				
My employer provides adequate training for my job function.		X			
My DAA provides adequate training for my job function.		X			
Other job requirements impede my ability to perform my IA/IS duties.		X			
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.					X
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 5. Survey response 4.

Displaying **5** of **26** respondents

« Prev | Next » | **Jump To:** 5 | Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?				X	

4. What is your education level?

Some college

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.				X	
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.		X			
Other job requirements impede my ability to perform my IA/IS duties.			X		
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.					X
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.					X

Figure 6. Survey response 5.

Displaying **6** of **26** respondents

« Prev | Next » | **Jump To:** 6 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

CISA

CISSP

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.	X				
My employer provides adequate training for my job function.	X				
My DAA provides adequate training for my job function.		X			
Other job requirements impede my ability to perform my IA/IS duties.		X			
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.					X
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.					X
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 7. Survey response 6.

Displaying **7** of **26** respondents

« Prev | Next » **Jump To:** 7 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am a non-management IS/IA person (ISSO, systems administrator)

2. How many hours a week would you estimate you spend on information systems security?

1-10

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?			X		
How many years do you have in information systems security?			X		

4. What is your education level?

HS Diploma/GED

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?			X			
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?			X			

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.				X	
My employer provides adequate training for my job function.			X		
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.			X		
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.			X		
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 8. Survey response 7.

Displaying **8** of **26** respondents

« Prev | Next » | **Jump To:** 8 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am a non-management IS/IA person (ISSO, systems administrator)

2. How many hours a week would you estimate you spend on information systems security?

<1

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?			X		
How many years do you have in information systems security?	X				

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?				X		
Implement and certify security requirements?				X		
Complete and submit SSP package to DAA?				X		

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.				X	
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.		X			
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.		X			
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.			X		

Figure 9. Survey response 8.

Displaying **9** of **26** respondents

« Prev | Next » **Jump To:** 9 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

CISSP

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.		X			
Other job requirements impede my ability to perform my IA/IS duties.					X
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.					X
My experience allows me to perform security-relevant tasks without additional training.		X			
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 10. Survey response 9.

Displaying **10** of **26** respondents

« Prev | Next » | **Jump To:** 10 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Edit Response | Delete
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

21-30

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?			X		
How many years do you have in information systems security?			X		

4. What is your education level?

Some college

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.				X	
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.					X
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 11. Survey response 10.

Displaying **11** of **26** respondents

« Prev | Next » | **Jump To:** 11 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

11-20

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Master's Degree

5. Do you have any of the following computer certifications?

A+

CISSP

Network+

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.					X
My DAA provides adequate training for my job function.		X			
Other job requirements impede my ability to perform my IA/IS duties.			X		
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.					X
My experience allows me to perform security-relevant tasks without additional training.					X
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 12. Survey response 11.

Displaying **12** of **26** respondents

« Prev | Next » | **Jump To:** 12 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

No, my primary role is not information systems security

2. How many hours a week would you estimate you spend on information systems security?

11-20

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

Security+

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?						X
Implement and certify security requirements?						X
Complete and submit SSP package to DAA?					X	

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.				X	
My employer provides adequate training for my job function.		X			
My DAA provides adequate training for my job function.		X			
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.			X		
My experience allows me to perform security-relevant tasks without additional training.			X		
Training is most important to maintaining a successful computer security program.			X		
Experience is most important to maintaining a successful computer security program.			X		
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 13. Survey response 12.

Displaying **13** of **26** respondents

« Prev | Next » | **Jump To:** 13 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

1-10

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Some college

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?	X					
Complete and submit SSP package to DAA?	X					

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.				X	
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.		X			
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.			X		
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.			X		
Experience is most important to maintaining a successful computer security program.			X		
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 14. Survey response 13.

Displaying **14** of **26** respondents

« Prev | Next » | **Jump To:** 14 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

11-20

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Master's Degree

5. Do you have any of the following computer certifications?

CISSP

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?						X
Implement and certify security requirements?						X
Complete and submit SSP package to DAA?						X

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.					X
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.					X
My experience allows me to perform security-relevant tasks without additional training.			X		
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 15. Survey response 14.

Displaying **15** of **26** respondents

« Prev | Next » **Jump To:** 15 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

1-10

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?			X		
How many years do you have in information systems security?				X	

4. What is your education level?

Some college

5. Do you have any of the following computer certifications?

Security+

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?	X					
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.					X
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.		X			
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.			X		
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.			X		

Figure 16. Survey response 15.

Displaying **16** of **26** respondents

« Prev | Next » **Jump To:** 16 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?				X	

4. What is your education level?

Master's Degree

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.		X			
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.		X			
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.			X		
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.			X		

Figure 17. Survey response 16.

Displaying **17** of **26** respondents

« Prev | Next » | **Jump To:** 17 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

1-10

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?			X		

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?			X			
Implement and certify security requirements?			X			
Complete and submit SSP package to DAA?				X		

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.					X
My employer provides adequate training for my job function.			X		
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.			X		
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 18. Survey response 17.

Displaying **18** of **26** respondents

« Prev | Next » | **Jump To:** 18 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

No, my primary role is not information systems security

2. How many hours a week would you estimate you spend on information systems security?

1-10

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?	X				
How many years do you have in information systems security?	X				

4. What is your education level?

HS Diploma/GED

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?			X			

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.			X		
Interacting with other IA/IS security professionals helps me do my job better.			X		
Being a member of a professional organization focused on IA/IS helps me do my job better.			X		
My experience allows me to perform security-relevant tasks without additional training.		X			
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 19. Survey response 18.

Displaying **19** of **26** respondents

« Prev | Next » **Jump To:** 19 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Master's Degree

5. Do you have any of the following computer certifications?

CISSP

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?	X					
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.		X			
My employer provides adequate training for my job function.		X			
My DAA provides adequate training for my job function.		X			
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.					X
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.					X
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 20. Survey response 19.

Displaying **20** of **26** respondents

« Prev | Next » | **Jump To:** 20 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

1-10

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?	X				
How many years do you have in information systems security?				X	

4. What is your education level?

Some college

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?	X					
Implement and certify security requirements?	X					
Complete and submit SSP package to DAA?		X				

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.			X		
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.			X		
Being a member of a professional organization focused on IA/IS helps me do my job better.			X		
My experience allows me to perform security-relevant tasks without additional training.		X			
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.					X
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 21. Survey response 20.

Displaying **21** of **26** respondents

« Prev | Next » **Jump To:** 21 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

CISSP

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?		X				
Complete and submit SSP package to DAA?				X		

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.		X			
My employer provides adequate training for my job function.			X		
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.			X		
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.				X	

Figure 22. Survey response 21.

Displaying **22** of **26** respondents

« Prev | Next » | **Jump To:** 22 | Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

No, my primary role is not information systems security

2. How many hours a week would you estimate you spend on information systems security?

<1

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?	X				
How many years do you have in information systems security?	X				

4. What is your education level?

HS Diploma/GED

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?	X					
Implement and certify security requirements?	X					
Complete and submit SSP package to DAA?	X					

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.		X			
My DAA provides adequate training for my job function.		X			
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.			X		
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.		X			
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.			X		
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.			X		

Figure 23. Survey response 22.

Displaying **23** of **26** respondents

« Prev | Next » | **Jump To:** 23 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

>40

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Master's Degree

5. Do you have any of the following computer certifications?

A+
CISSP
Network+

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?		X				
Implement and certify security requirements?	X					
Complete and submit SSP package to DAA?	X					

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.		X			
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.			X		
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.					X
My experience allows me to perform security-relevant tasks without additional training.			X		
Training is most important to maintaining a successful computer security program.				X	
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.					X

Figure 24. Survey response 23.

Displaying **24** of **26** respondents

« Prev | Next » **Jump To:** 24 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

11-20

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?	X					
Implement and certify security requirements?					X	
Complete and submit SSP package to DAA?			X			

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.				X	
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.		X			
Interacting with other IA/IS security professionals helps me do my job better.				X	
Being a member of a professional organization focused on IA/IS helps me do my job better.				X	
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.					X
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.					X

Figure 25. Survey response 24.

Displaying **25** of **26** respondents

« Prev | Next » **Jump To:** 25 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

No, my primary role is not information systems security

2. How many hours a week would you estimate you spend on information systems security?

1-10

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?				X	

4. What is your education level?

Associate's Degree

5. Do you have any of the following computer certifications?

A+

Security+

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?	X					
Implement and certify security requirements?	X					
Complete and submit SSP package to DAA?			X			

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.					X
My employer provides adequate training for my job function.	X				
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.				X	
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.			X		
My experience allows me to perform security-relevant tasks without additional training.				X	
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.				X	
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.					X

Figure 26. Survey response 25.

Displaying **26** of **26** respondents

« Prev | Next » | **Jump To:** 26 Go »

Response Type: Normal Response
Collector: Web Link (Web Link)
Custom Value: *empty*
IP Address:
Response Started:
Response Modified:
Edit Response | Delete

1. Is your primary role IA/IS?

Yes, I am an IS/IA Manager (ISSM/ IAM)

2. How many hours a week would you estimate you spend on information systems security?

21-30

3. Experience

	<1 (1)	1-2 (2)	3-5 (3)	6-10 (4)	>10 (5)
How many years of experience do you have in information systems in general?					X
How many years do you have in information systems security?					X

4. What is your education level?

Bachelor's Degree

5. Do you have any of the following computer certifications?

N/A

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following:

	1 day or less (1)	2 days - 1 week (2)	1-2 weeks (3)	3-4 weeks (4)	4-8 weeks (5)	>2 months (6)
Complete system configuration (either individually or with other IA/IS staff)?	X					
Implement and certify security requirements?	X					
Complete and submit SSP package to DAA?	X					

7. Rate the following statements:

	Strongly Disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly Agree (5)
Additional training would shorten the time it takes me to complete a submission.			X		
My employer provides adequate training for my job function.					X
My DAA provides adequate training for my job function.				X	
Other job requirements impede my ability to perform my IA/IS duties.	X				
Interacting with other IA/IS security professionals helps me do my job better.					X
Being a member of a professional organization focused on IA/IS helps me do my job better.					X
My experience allows me to perform security-relevant tasks without additional training.			X		
Training is most important to maintaining a successful computer security program.					X
Experience is most important to maintaining a successful computer security program.			X		
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.					X

Figure 27. Survey response 26.

1. Is your primary role IA/IS? Create Chart | Download

	Response Percent	Response Count
Yes, I am an IS/IA Manager (ISSM/ IAM)	73.1%	19
Yes, I am a non-management IS/IA person (ISSO, systems administrator)	11.5%	3
No, my primary role is not information systems security	15.4%	4
answered question		26
skipped question		0

Figure 28. Question 1 raw results.

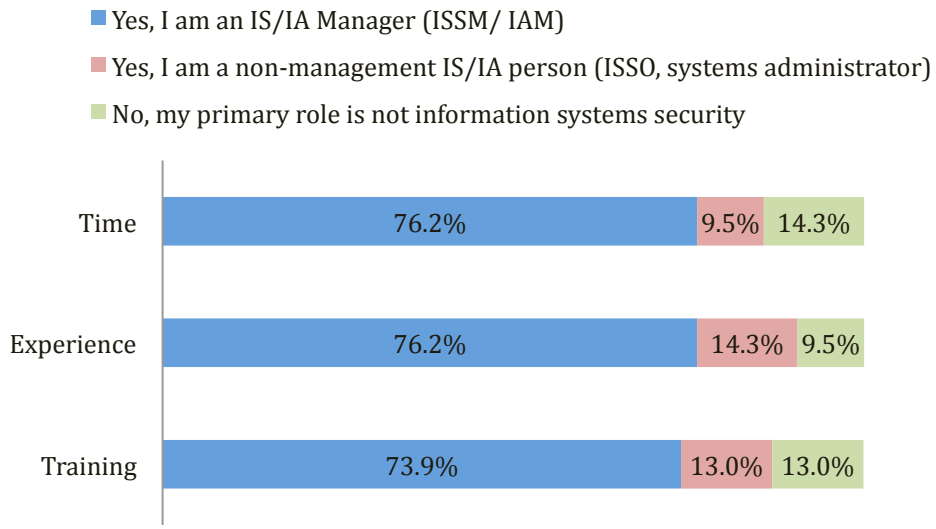

Figure 29. Question 1 aggregated results.

2. How many hours a week would you estimate you spend on information systems security?

Create Chart | Download

	Response Percent	Response Count
<1	7.7%	2
1-10	26.9%	7
11-20	19.2%	5
21-30	7.7%	2
31-40	3.8%	1
>40	34.6%	9
	answered question	26
	skipped question	0

Figure 30. Question 2, raw results.

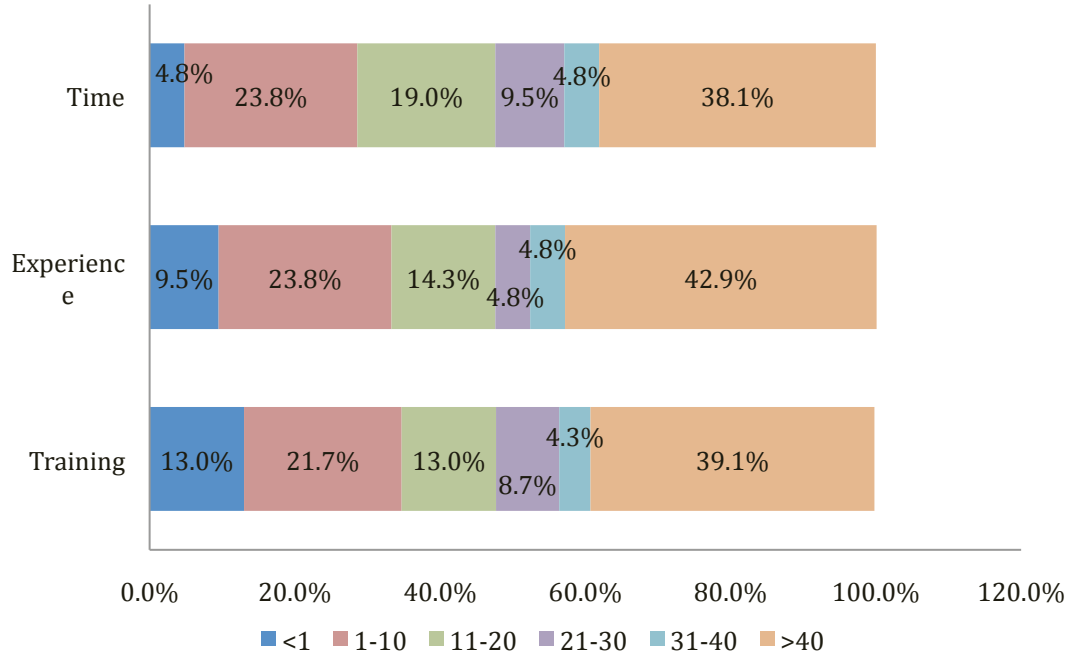

Figure 31. Question 2 aggregated results.

3. Experience						Create Chart	Download
	<1	1-2	3-5	6-10	>10	Rating Average	Response Count
How many years of experience do you have in information systems in general?	11.5% (3)	0.0% (0)	15.4% (4)	11.5% (3)	**61.5% (16)**	4.12	26
How many years do you have in information systems security?	11.5% (3)	0.0% (0)	15.4% (4)	26.9% (7)	**46.2% (12)**	3.96	26
					answered question		26
					skipped question		0

Figure 32. Question 3 raw results.

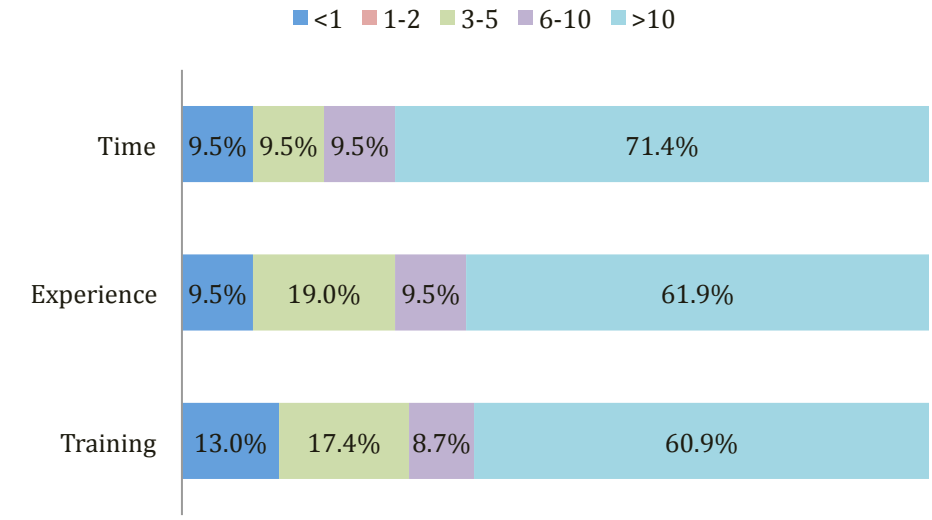

Figure 33. Question 3a aggregated results.

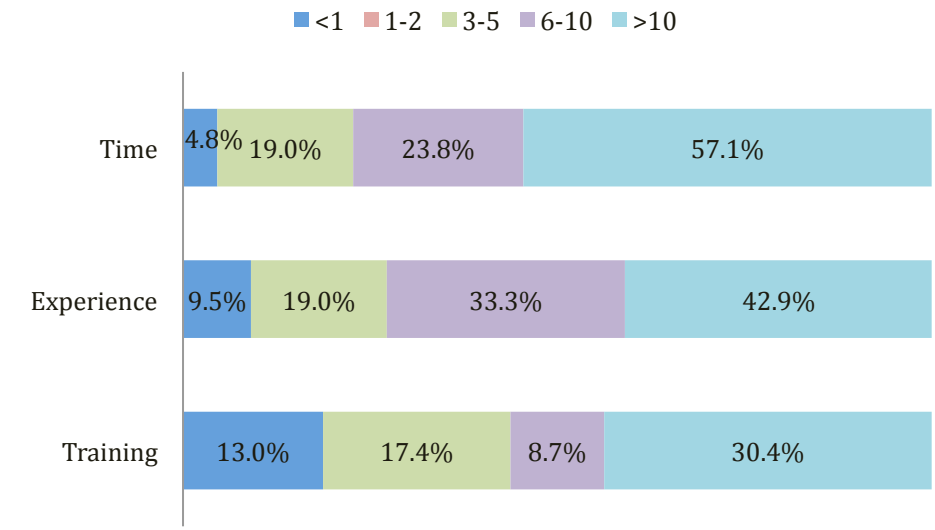

Figure 34. Question 3b aggregated results.

4. What is your education level? Create Chart | Download

	Response Percent	Response Count
No HS Diploma/GED	0.0%	0
HS Diploma/GED	11.5%	3
Some college	19.2%	5
Associate's Degree	7.7%	2
Bachelor's Degree	38.5%	10
Master's Degree	23.1%	6
PhD	0.0%	0
	answered question	26
	skipped question	0

Figure 35. Question 4 raw results.

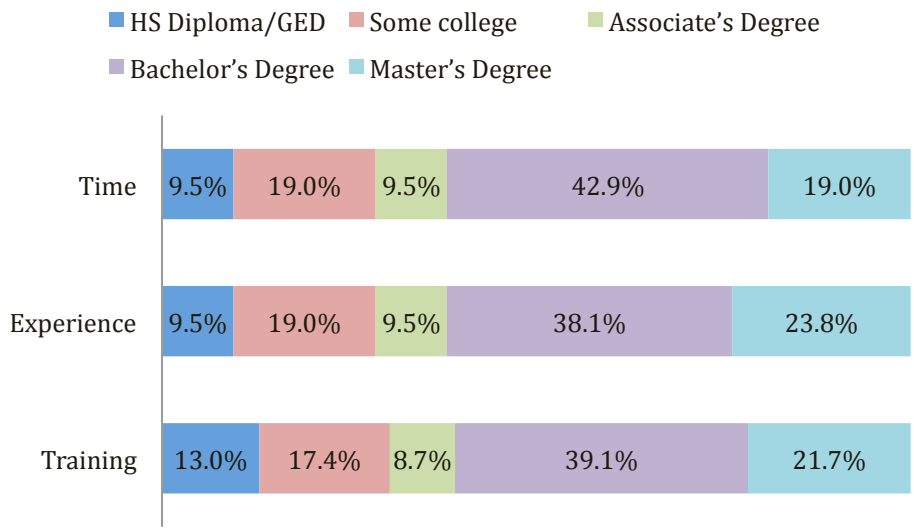

Figure 36. Question 4 aggregated results.

5. Do you have any of the following computer certifications?		Create Chart	Download
		Response Percent	Response Count
A+		15.4%	4
CISA		3.8%	1
CISM		3.8%	1
CISSP		34.6%	9
GSE		0.0%	0
GSEC		0.0%	0
GSLC		0.0%	0
Network+		11.5%	3
Security+		19.2%	5
SCNA		0.0%	0
SCNP		0.0%	0
SSCP		0.0%	0
N/A		46.2%	12
		answered question	26
		skipped question	0

Figure 37. Question 5 raw results.

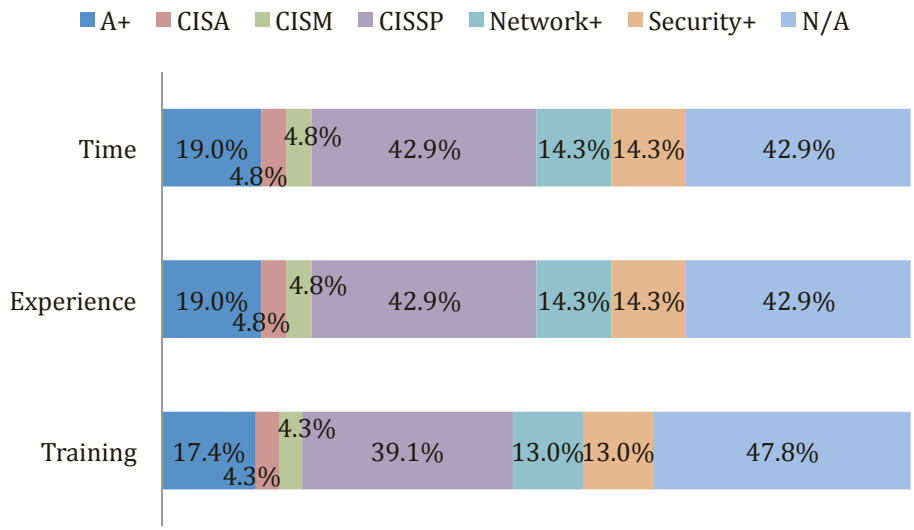

Figure 38. Question 5 aggregated results.

6. For your typical system, what do you estimate to be the average time it takes (from the point of being notified of the need) to complete the following: Create Chart Download

	1 day or less	2 days - 1 week	1-2 weeks	3-4 weeks	4-8 weeks	>2 months	Rating Average	Response Count
Complete system configuration (either individually or with other IA/IS staff)?	30.8% (8)	**42.3% (11)**	15.4% (4)	3.8% (1)	0.0% (0)	7.7% (2)	2.23	26
Implement and certify security requirements?	23.1% (6)	**53.8% (14)**	7.7% (2)	3.8% (1)	3.8% (1)	7.7% (2)	2.35	26
Complete and submit SSP package to DAA?	15.4% (4)	**42.3% (11)**	23.1% (6)	11.5% (3)	3.8% (1)	3.8% (1)	2.58	26
						answered question		**26**
						skipped question		**0**

Figure 39. Question 6 raw results.

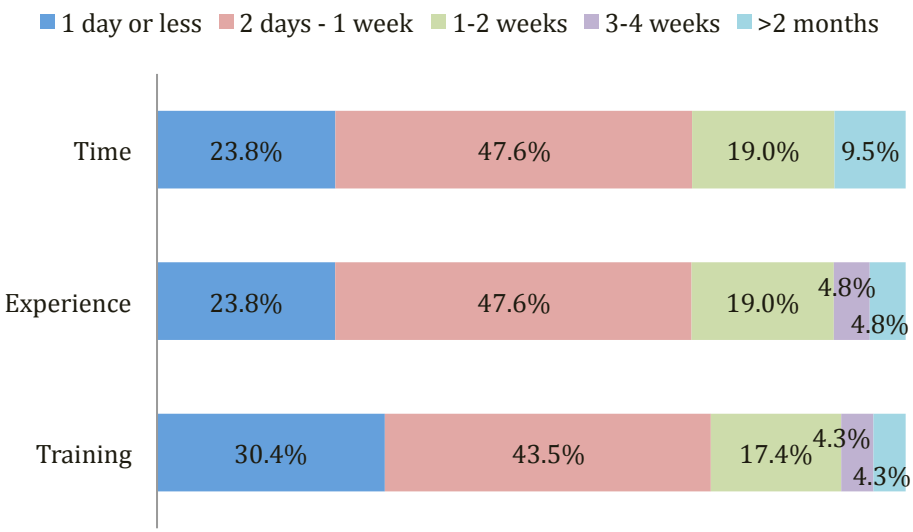

Figure 40. Question 6a aggregated results.

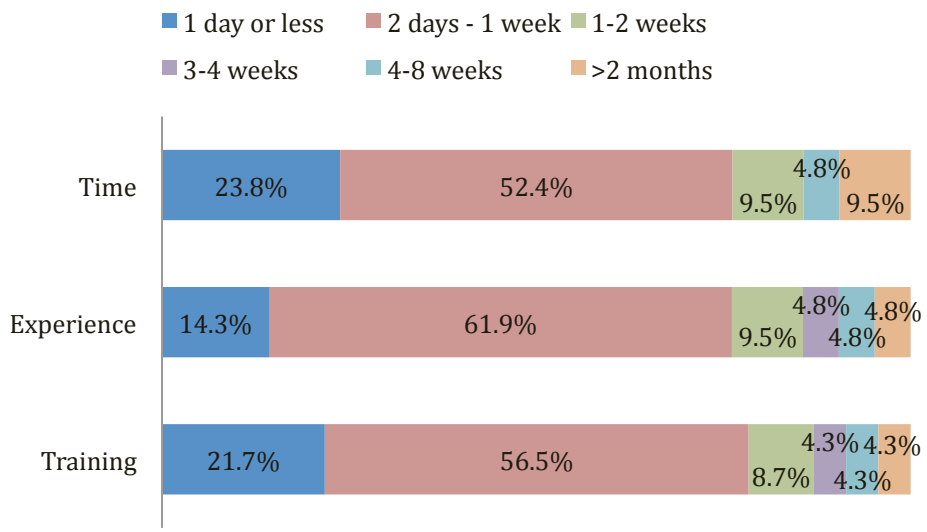

Figure 41. Question 6b aggregated results.

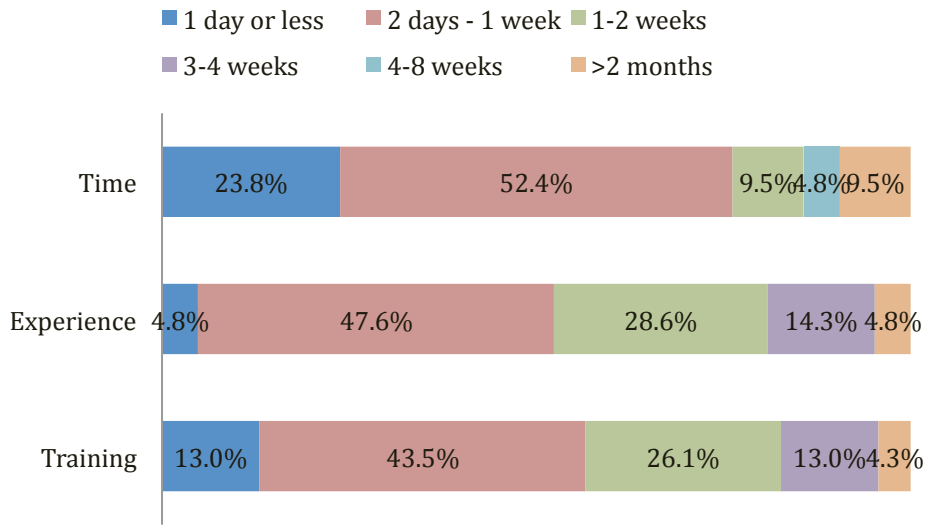

Figure 42. Question 6c aggregated results.

7. Rate the following statements: Create Chart Download

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree	Rating Average	Response Count
Additional training would shorten the time it takes me to complete a submission.	7.7% (2)	19.2% (5)	**38.5% (10)**	23.1% (6)	11.5% (3)	3.12	26
My employer provides adequate training for my job function.	7.7% (2)	15.4% (4)	15.4% (4)	**46.2% (12)**	15.4% (4)	3.46	26
My DAA provides adequate training for my job function.	0.0% (0)	30.8% (8)	**34.6% (9)**	**34.6% (9)**	0.0% (0)	3.04	26
Other job requirements impede my ability to perform my IA/IS duties.	3.8% (1)	30.8% (8)	23.1% (6)	**38.5% (10)**	3.8% (1)	3.08	26
Interacting with other IA/IS security professionals helps me do my job better.	0.0% (0)	0.0% (0)	11.5% (3)	**46.2% (12)**	42.3% (11)	4.31	26
Being a member of a professional organization focused on IA/IS helps me do my job better.	0.0% (0)	0.0% (0)	26.9% (7)	**42.3% (11)**	30.8% (8)	4.04	26
My experience allows me to perform security-relevant tasks without additional training.	0.0% (0)	19.2% (5)	30.8% (8)	**38.5% (10)**	11.5% (3)	3.42	26
Training is most important to maintaining a successful computer security program.	0.0% (0)	0.0% (0)	11.5% (3)	**50.0% (13)**	38.5% (10)	4.27	26
Experience is most important to maintaining a successful computer security program.	0.0% (0)	0.0% (0)	19.2% (5)	**50.0% (13)**	30.8% (8)	4.12	26
Adequate time for IA/IS duties is the most important to maintaining a successful computer security program.	0.0% (0)	0.0% (0)	19.2% (5)	**57.7% (15)**	23.1% (6)	4.04	26
					answered question		**26**
					skipped question		**0**

Figure 43. Question 7 raw results.

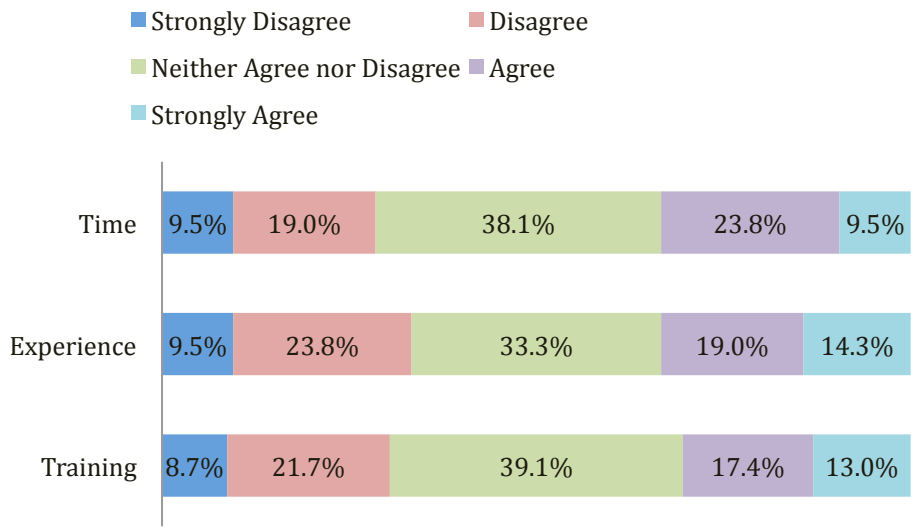

Figure 44. Question 7a aggregated results.

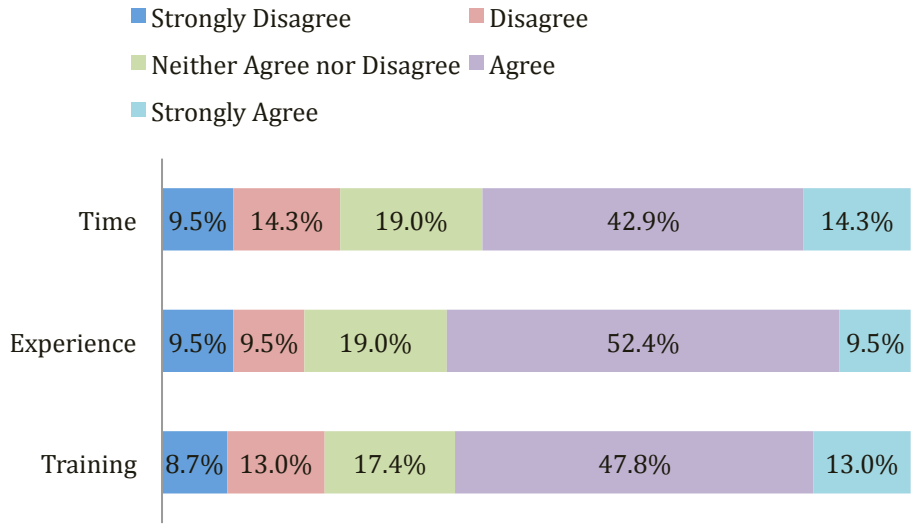

Figure 45. Question 7b aggregated results.

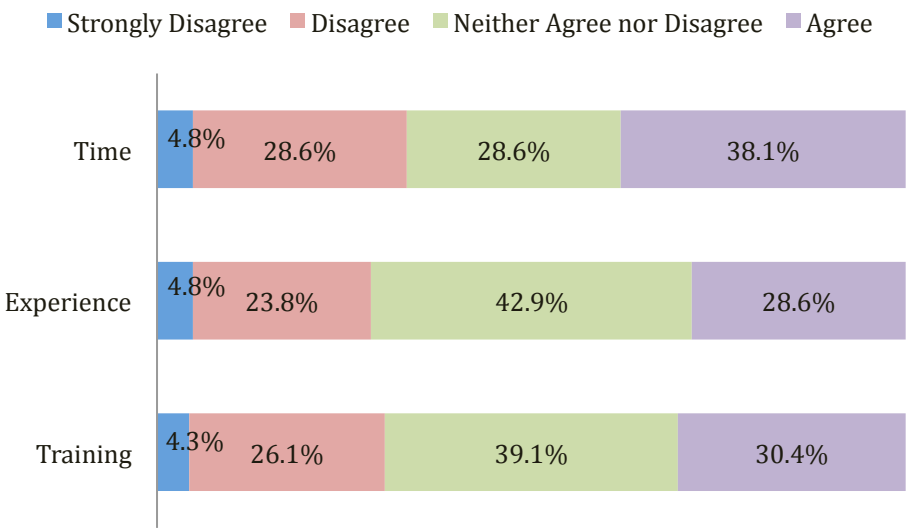

Figure 46. Question 7c aggregated results.

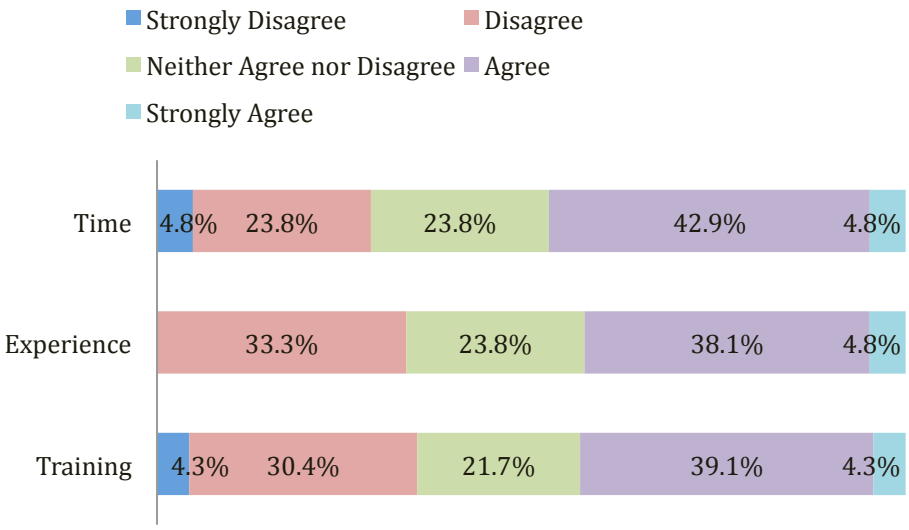

Figure 47. Question 7d aggregated results.

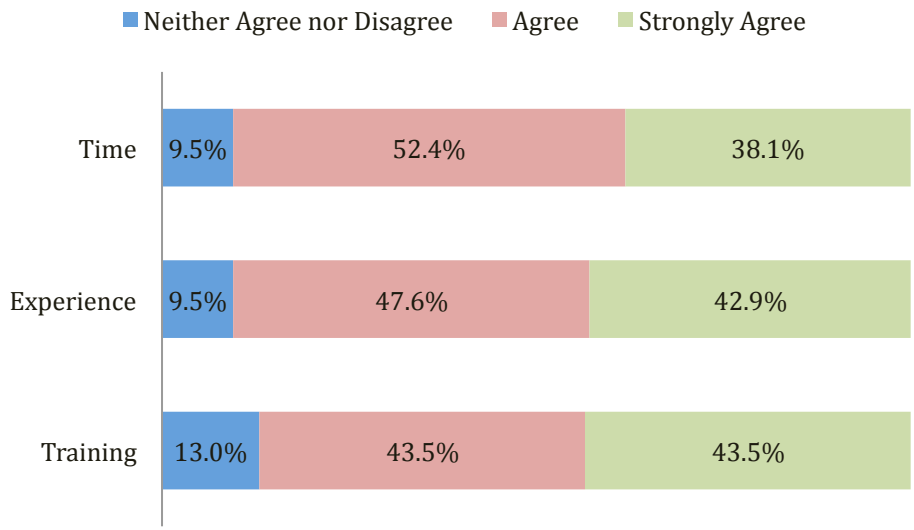

Figure 48. Question 7e aggregated results.

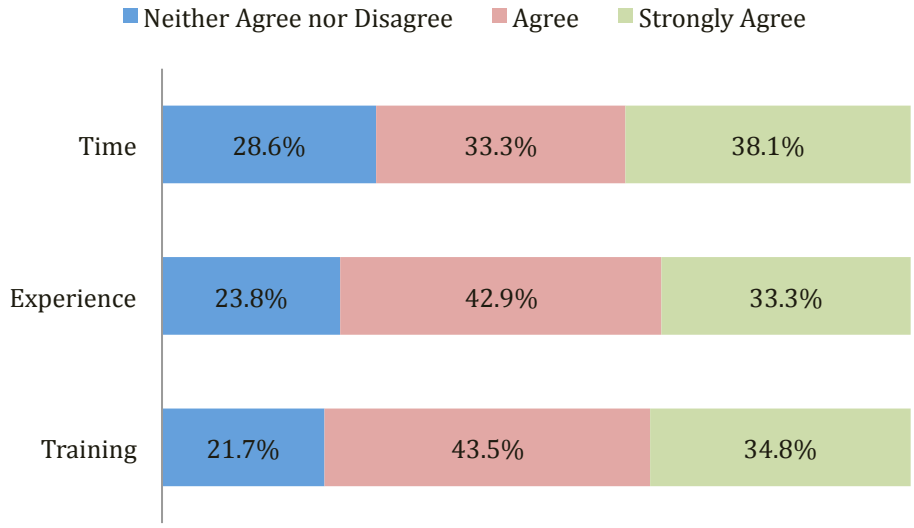

Figure 49. Question 7f aggregated results.

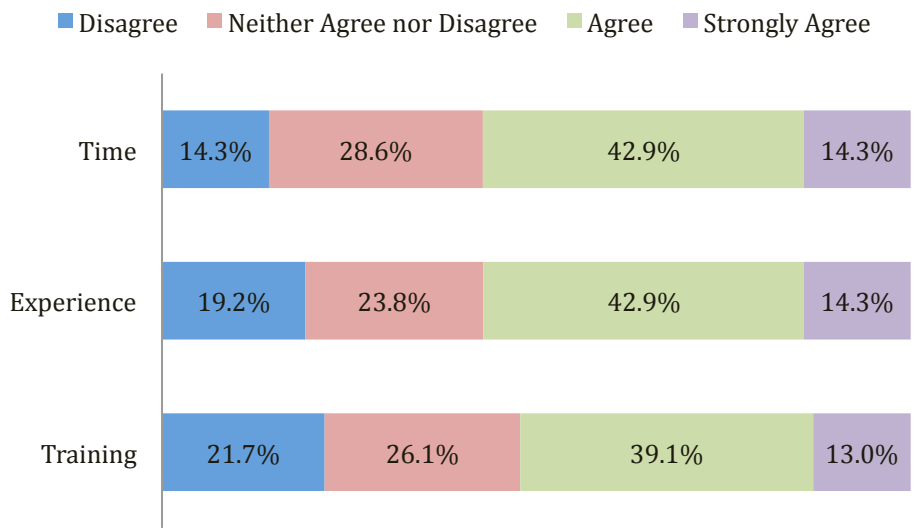

Figure 50. Question 7g aggregated results.

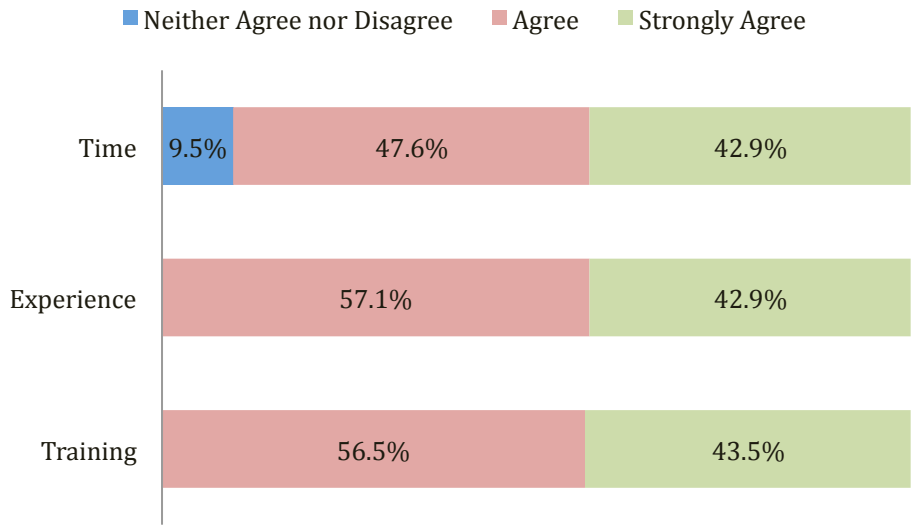

Figure 51. Question 7h aggregated results.

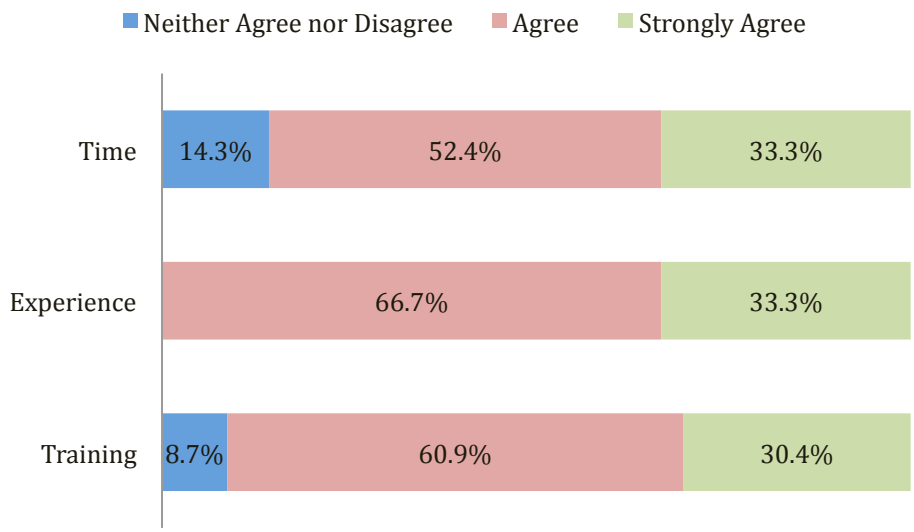

Figure 52. Question 7i aggregated results.

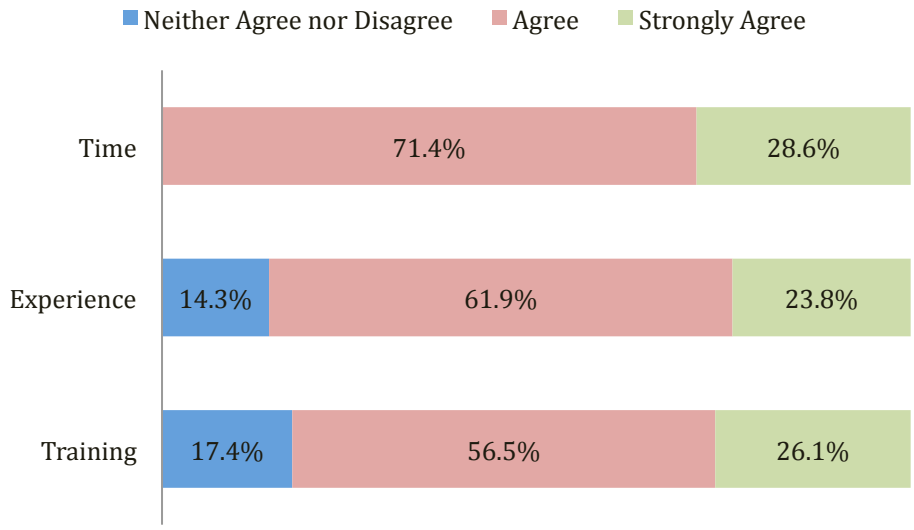

Figure 53. Question 7j aggregated results.