Global Information Assurance Certification Paper

Assessing Information Assurance Posture: Key Steps to IA Assessment Methodology

Stephen W. Matthews
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 1
Submitted May 3, 2004

Table of Contents

Abstract

This paper seeks to provide a key set of principles and steps in a methodology for assessing an organization's Information Assurance (IA) posture. This is by no means the only method of assessment, nor the most detailed, but it provides a real methodology, along with a checklist from which to determine notable vulnerabilities. The content of the paper is an overview of what goes into an assessment of IA posture, while the supplied checklist delves into specific issues that the assessment team must evaluate.

More important than the immediate snapshot that security assessment tools provide is an organization's IA policies, and whether they are legitimately being put to practice. A lack of documented policy indicates that a snapshot of an organization's vulnerabilities as determined by security assessment tools is irrelevant; the snapshot could be completely inaccurate, as there is no policy to ensure that procedures were and are consistently followed. Where policies exist, a lack of adherence to policy means that policies are not being enforced, which again, leads to inaccuracy in snapshot assessments through security assessment software tools. Verifying effective policy and consistent enforcement of that policy ensures that a snapshot assessment provides accurate understanding of IA posture and any vulnerabilities that need attention.

The first section of this paper describes several key concepts that are not only associated with IA but also define what an organization's IA posture should look like. The second section describes those actions and issues an IA assessment team needs to understand in order to define the scope of an assessment. The third and fourth sections describe administrative issues and roles and responsibilities associated with an IA assessment. Finally, the heart of the paper, though not nearly the largest portion, describes the actual conduct of an IA assessment.

This last section is complemented by Appendix A, which provides an actual checklist from which to conduct and document an assessment. It needs to be understood that this checklist is only one concrete method of conducting an assessment; many other checklists exist. The checklist is not specific to security assessment tools, as software tools change or are replaced by other tools. The author is one of a number of persons who has worked to contribute to this document. For the purpose of delineation of work, the author of this paper laid out part of the format of the individual checklist steps, provided each step with a title, defined the data collection methods for all steps, and organized the steps through linked checklists and a table of contents. It is fair and accurate to say that the author started from a base checklist and more than doubled the contents. The description of each checklist step and the breakdown of the organization come from the Marine Corps publication, "Information Assurance (IA) Implementation." A further delineation of credit for work completed on this checklist is presented on the first page of Appendix A.

Key Concepts

Information Assurance

In an era where more information is being passed electronically than in any other form, and where a growing percentage of the population get the majority of their information from IT sources, such as the Internet, rather than from books and other printed publications, it is imperative that organizations and businesses understand what is happening to the information they are creating, retrieving, storing, or passing. In past eras, physical capabilities were the key to an organizations success and loss of superiority in that capability could lead to an organization's demise; in the information age, information is the key that needs to be secured against the exploits of outside organizations.

Security of information, though, is not nearly as easy an issue as security of physical production practices, or of physical organization capabilities in general. Securing an organization's abilities was once a matter of ensuring physical security of facilities and security against employee fraud. Machines could be locked or shut down, and paper could be locked in drawers or safes. Information today is shared among colleagues in the same organization not in the form of memos and letters, but in emails, document attachments, and share drive files. Because these organizations connect their networks, which hold this valuable information, to the Internet or to other networks outside of their own, those organizations must realize what they need to be able to do with their wealth of information, and what risks they are willing to take in order to maintain those capabilities.

Information Assurance (IA) is the culmination of a) understanding acceptable loss based on needed capabilities and acceptable risks and b) securing an organization's information assets against unacceptable loss of availability, integrity, or confidentiality. IA also assumes a security of authenticity, as it applies to confidentiality and integrity, and non-repudiation, as it applies to integrity. The Information Assurance Technical Framework (IATF), as put out by the National Security Agency (NSA), defines IA as

> Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [IATF, 1999]

IA imposes on an organization a review of its mission and threats and the securing of its needed capabilities against the risks those threats pose. Conducting an IA vulnerability assessment involves looking at the vulnerabilities an organization has and understanding the mitigation of those vulnerabilities that could create unacceptable losses.

Availability

Availability of information is measure of how often information is capable of being accessed as needed. It involves information being where a user needs it when they need it. If access to system or network resources provides users necessary information, then availability of information can be measured as time that system or network resources are available divided by the amount of time measured. Availability is a key component to IA.

Integrity

Integrity of information is the probability that the information will be correct when accessed. Information can be maliciously or inadvertently modified so that it is incorrect when transmitted or accessed. Information integrity speaks to data control, such that data that is tightly controlled from end to end in transmission should maintain its integrity for the receiving user.

Confidentiality

Confidentiality is a measure of how well protected information is from being read, transmitted, viewed, or interpreted by unauthorized persons or organizations. Confidentiality is protected through security of transmission lines and through encryption of data when transmitted by insecure means.

Vulnerability

A vulnerability is a means for an intruder to enter the information system or to affect a system such that its availability, integrity, or confidentiality is compromised. A vulnerability:

- allows an attacker to execute commands as another user
- allows an attacker to access data that is contrary to the specified access restrictions for that data
- allows an attacker to pose as another entity
- allows an attacker to conduct a denial of service [TERMINOLOGY, 2004]

There are two distinctions of vulnerabilities—those that are universal to all systems, and those that are system specific. "A 'universal' vulnerability is one that is considered a vulnerability under any commonly used security policy […]"[TERMINOLOGY, 2004]. Universal vulnerabilities can be assessed on all information systems. A system specific vulnerability is a vulnerability that an assessment team would look for only on a particular platform or operating system.

Information Attack

An information attack is an assault on an information system carried out for the purpose of disrupting the system and compromising its availability, integrity, and/or confidentiality. It stands to reason that an attacker will likely enter the system by the easiest means possible, which is likely through an

unmitigated vulnerability. Information attacks can come in five basic forms, according to the Information Assurance Technical Framework:

- Passive: include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capture of authentication information
- Active: include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information
- Close-In: consists of a regular type individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information
- Insider: can be malicious (eavesdrop, steal or damage information, etc) or nonmalicious (carelessness, lack of knowledge, etc)
- Distribution: focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product, such as a back door [TERMINOLOGY, 2004]

These forms of attack serve to disrupt an information system and diminish its capabilities.

Acceptable Risk

Before an assessment can be conducted on an organization, the organization must first know what risks it is willing to assume. It is not enough to ask what vulnerabilities an organization has. The organization needs to know which risks it can handle and which it cannot. For example, if an organization's web server absolutely must be available, then the risk of the loss of availability of that server going down is unacceptable. However, if the same organization is not concerned about what information is seen on that server, then the risk of loss of confidentiality of the information on that server is acceptable. Knowing the risks is based on the needed set of capabilities.

Capability Requirements

As with risk, an organization also needs to know what capabilities are required before it can decide which vulnerabilities to be concerned with. Understanding an organization's capability needs should be easier than understanding what risks are acceptable; required IT capabilities should be a subset of the organization's mission as a business. An organization that conducts web business, such as EBay, needs to have its web services running at all times that it conducts business. An organization that transports information between or stores information for customers needs to ensure the integrity of the information it is moving or storing. These capabilities relate conversely to risks, as a need for a capability equates to the need to mitigate the risk associated with the loss of that capability.

Acceptable Loss

Ultimately, for purpose of assessing an organization's information assurance posture, what needs to first be understood is how much loss of availability, integrity, and confidentiality the organization can withstand and still continue to conduct business. Some businesses use IT for administrative purposes in place of a replaced paper system or a simple enough system that loss of information capabilities can be tolerated. Other businesses, however, rely very heavily on their IT systems and do not have an acceptable non-IT fallback solution; those businesses are incapable of loss of their IT system availability for any length of time. Some businesses understand that the traffic they pass over their IT systems is unsecure, but the information they pass is relevant for such a short duration or it is simply understood that information is seen by the general public that a loss of confidentiality is an acceptable loss not worth mitigating. The amount and type of acceptable loss are dependent on the organization's mission and needs.

Scope of Assessment

In order to conduct an appropriate IA vulnerability assessment, the assessing team must first understand the scope of the assessment. The assessment team needs a clear picture of what is to be assessed and what is being looked for. A lack of understanding of the scope of an assessment can lead to wasted time and effort looking at vulnerabilities that were never intended for examination. This waste of time and effort is not only at the expense of the assessment team, but is also a waste of network resources and usable bandwidth that the assessed organization could otherwise use productively. While this waste of resources is a serious issue to prevent, it is not nearly so serious as the assessment team that does not have a clear picture of what IP ranges, ports, and systems it is allowed to scan; scanning outside of ranges authorized by the assessed unit could lead to reprimand, loss of job, or even legal repercussions, and could cause serious damage to systems that were not intended to be probed by software tools.

Know What You Are Looking For

No organization wants an assessment team to poke around all of their information just because it might find something. Nor should an assessment team conduct an assessment without first knowing what it is looking for. Not only is it unprofessional that an assessment team not be able to verbalize what steps it is going to take and what vulnerabilities it intends to look for prior to the beginning of an assessment, but many organizations simply cannot or will not tolerate being assessed for IA posture vulnerabilities without seeing a detailed assessment plan in advance, in order to ensure that the assessment is not a waste of time and money. Further, a healthy amount of work up front can save an assessment team time and embarrassment during the reporting phase of the

assessment. Not knowing what to look for can lead to a lack of appropriate assessment data or too much data to sift through. This can lead to deficient, unprofessional, and incomplete reports, which do not provide the assessed organization with any positive information.

An IA assessment team should look for trends and vulnerabilities in an organization's posture. These include unmitigated and unnecessary risks in information availability, integrity, and confidentiality. Looking at the capabilities of the assessed organization, a solid breakdown of categories in which to define specific criteria to examine could include (according to the Marine Corps instructional publication entitled "Information Assurance (IA) Implementation): [DODI8500.2, 2003]

- Security Design and Configuration
- Identification and Authentication
- Enclave and Computing Environment
- Enclave Boundary Defense
- Physical and Environmental
- Personnel
- Continuity
- Vulnerability and Incident Management

From these categories, specific questions and criteria can be derived in order to more concretely define the scope of what the assessment team is looking for. For a concrete example of this type of breakdown, see Appendix A: IA Assessment Checklist.

Know What You Are Looking At

One clear goal every efficient assessment team should have is to complete its assessment with as little interruption and loss of resources to the assessed organization as possible. In order to facilitate this, as well as to prepare—in advance of the assessment—a solid, formal plan of how to conduct the assessment, the assessment team should determine the network architecture and host and software configurations prior to arrival. Knowing the architecture to be assessed allows a very specific plan to be devised, which minimizes wasted time and effort while allowing the assessment team time to tackle the on-the-spot and unplanned issues.

Special Limitations

One important aspect of the environment that an assessment team is going to review is the boundaries and limitations. Rarely is it the case that an organization wants an assessment team to run rampant, even within its own borders. In order to prevent loss of key assets, some organizations will move resources to hosts that they do not want probed or assessed. Organizations may have information that they do not want the possibility of leaking or losing. Certainly, the preferred solution would be to remove assets from the network, at

least during the assessment, but it may be the case that an organization cannot afford to do so. For these reasons, and others, organizations will set "off-limits" IP ranges, assets, or even physical spaces that an assessment team needs to know and respect. Violating these limits may be more than a nuisance; it could bring legal actions if an assessment team has signed an agreement with the assessed organization and violates agreed upon boundaries.

Understand the Assessed Organization's Expectations

Knowing what the assessed organization expects of the team is important in defining the limits and the goals of the assessment. Does the organization asking for an assessment expect a cursory look for the purpose of finding gaping holes, or would they prefer an in-depth analysis of their entire architecture? Are they expecting physical security to be evaluated, or are they only looking for host vulnerabilities as found by scanning software? Do they expect penetration testing? What one organization will expect of an assessment team may vary drastically from another organization, and neither is more right in their expectations. This comes down to the concept of customer service. An assessment team, whether internal to an organization or hired from outside needs to understand what the organization wants and needs to provide according to those expectations, in a customer service role.

One important aspect to understand is the organization's expectation of what it will receive in the form of reports. If an assessment team's function is to provide an organization with a picture of its IA posture, its method of doing so is through reporting procedures. The organization may be expecting more detail, or maybe it expects a higher, broader level than the assessment team is used to giving, but if that is what the organization wants in order to effect positive change in its IA posture, then that is what it should receive.

Ensure Your Expectations Are Understood

An organization understanding an assessment team's expectations is just as important to an assessment. A team that is visiting an organization or is scheduling many assessments does not have the time to waste waiting until it arrives before receiving all necessary planning documentation. In order for the assessment team to formulate a plan, organizational policy, network diagrams, and other documents are needed in a timely fashion. Additionally, in order for the assessment team to conduct its task, it will need the assessed organization to provide certain assets, such as the names of system administrators and the time slots within which they can be freely interviewed.

Administration

Conduct of an effective IA assessment does not happen without some advance administrative work in order to ensure an assessment team has everything it needs to complete its assignment. An unprepared assessment

team may find itself incapable of completing its task due to lack or resources or permissions.

Request Needed Resources

In order to conduct an IA assessment, an assessment team will need to coordinate some resources. Some of these resources involve the access needed to conduct an assessment. To begin with, an assessing team that brings its own IT assets from with to conduct an assessment will need to be able to plug into the network, so they will need appropriate IP addresses from which to assess network resources. In order to conduct in-depth baseline analyses of all network host machines, the assessment team will most likely also need access to be in the domain that the assessed hosts are on.

Some other resources needed are more related to time and physical resources. First, access to appropriate spaces is addressed, generally through the issuance of visitor clearances and/or badges. Additionally, meetings may need to be set up, preferably well in advance, so that key persons can and will attend. Finally, resources for assessment conduct need to be requested such as workspace from which to conduct an assessment and time slots for interviews.

Forms and Reports

As already stated, the assessed organization is expecting results from the assessment in the form of reports. Most likely, an assessed organization would like to know some information immediately, but more importantly, a final report of a formal nature, defining what process was conducted and what information was found, will be expected. An assessment team needs to narrow the collection of data into a concise, usable report that the assessed unit will be capable of implementing changes from. This report should highlight serious issues and trends found during data collection. Providing the assessed unit with a cover letter and raw data is not a strategy to elicit appropriate measures, as, if the organization had the time to pore over raw data to begin with, it most likely would not need a team to conduct an assessment for it.

The use of template forms and reports reduces the time taken to conduct surveys and interviews and to compile outbriefs and final reports. If survey questions will always be of the same format, even if the questions asked will change, starting from a template reduces the time to create surveys through reuse of similar questions and ease of creation for new ones. In fact, the preferable method of survey creation would be to start from a template that includes all possible questions to ask and simply pare questions down to those needed. In creating final reports, having templates handy at an assessment can provide an assessment team with the ability to give a “quick look” immediately following the assessment.

Roles and Responsibilities

Ensure Your Role is Understood

An assessment team needs to ensure that the assessed organization understands its purpose and function; otherwise it is wasting its own time and that of the organization. In order to ensure that an assessed organization really understands what it is getting out of an assessment, an assessment team needs to provide several sets of definitions. Terminology can be a barrier to an organization understanding what the team's function is and what it will produce. In order to alleviate this confusion, terminology should be defined and described in context as best as possible. Additionally, passing and failing criteria should be clearly laid out so that the organization has no confusion about what a passing or failing score really means. Finally, the assessment team needs to ensure that all of the assessed organization's personnel understand what its authority is; in some instances, an assessment team may simply be providing recommendations that an assessed organization can review and do with as it pleases, while in other instances, the assessment team has been brought in to make hard-line determinations as to how to fix an organization's IA posture.

Know Where to Report Results

An assessment team needs to understand whom they are providing information to, and they need to ensure that they do not divulge assessment results to any parties other than those agreed to. This is a trust issue; an assessed organization will most likely not want an assessment team to view their network if the team intends to air the organization's "dirty laundry" in public. Organizations expect to know up front who is going to see the results of the assessment, with valid concern. If the assessed organization knows in advance that the results will be provided to the next higher organizational level, they can plan to brief senior personnel on what they expect and what was found so that there are no surprises. Conversely, an assessment team needs to ensure that the results go to all specified recipients. Again, an organization may not like that they are being assessed and that a higher organization expects the results, but this type of assessment reporting ensures accountability on the part of the subordinate organization; if the assessed organization knows they will be periodically assessed for their IA posture and that results will be forwarded to a higher organization, they just may give it more attention in the interim.

Execution

Preparation and Setup

Showing up to an assessment unprepared not only appears unprofessional but also can be a detriment to the conduct of the assessment. Preparation for an assessment should be thorough and should ensure that on-site preparation is minimized to those functions that cannot be prepared for in

advance. Many factors must be considered during the preparation and setup phase of the assessment.

Review Organizational Policy

One of the most important—yet probably the most neglected—steps to preparing for an assessment is reviewing organizational policies and documents related to policy. It is of utmost importance that the assessment team understands the IA posture of the organization as defined in its policy for two reasons. First, organizational IA policy provides a baseline expectation; an organization's policy should define what information capabilities the organization needs, what risks the organization is willing to accept in the course of business, and how it intends to institute IA policy. From this policy, the assessment team has a baseline from which to determine whether the organization is following and enforcing the IA measures it expects, and where it is deficient in instituting documented IA controls. The second reason the assessment team needs to understand organizational policy is to determine in advance of the assessment what measures it believes the organization is deficient in instituting. The assessment team that understands IA and understands the assessment of an organization's IA security measures against its required capabilities and acceptable risks can make recommendations concerning policy changes that reflect an IA policy that better suits the assessed organization.

Configuration Management of Team Assets

Configuration management of assessment team hardware and software resources will ensure a fairly smooth assessment. Setting up assessment computers, preferably laptops for portability, is an absolute necessity prior to arrival on-site for an assessment. To begin with, all necessary software needs to be installed on assessment computers so that team members do not have to waste time loading software during an assessment. More importantly, assessment machines need to be secured such that they do not present any additional vulnerabilities onto an assessed organization's network and are not vulnerable themselves to any potential malicious activity from the organization's network. Nothing is more professionally embarrassing than to infect an assessed organization's network with a virus due to negligence in ensuring that the assessment team takes the time to find and secure its own vulnerabilities. Just short of that embarrassment is that of an assessment team's computers being compromised by the assessed network due to their own lack of security. Not as professionally embarrassing, but just as devastating to the outcome, is the lack of assessment tools due to poor configuration management prior to arrival to the assessment.

Administrative Details

In addition to management of computers, administrative issues need to be tended to prior to the assessment as well. To begin with, assessment team members may need to have visitor badges or clearances to enter organization facilities. Oversight of this detail could prematurely end an assessment.

Assessment teams also need to ensure they have received authority to connect to the assessed unit's network; again, lack of the appropriate paperwork. In preparation of the assessment, the assessment team will want to ask for any organizational IA policy, network diagrams, and other paperwork that will assist the team in understanding the situation prior to arrival. Additionally, the assessment team will want to provide the organization with any relevant paperwork to ensure that the assessment is an "open book" test.

Updated Vulnerability Definition Files

Finally, an assessment team will want to ensure its definition files are current and that the team understands current vulnerabilities. Security assessment tools use definition files that include definition of how to verify current vulnerabilities, and generally, these definition files are updated frequently. The assessment team will want to visit the web sites of all assessment tools and ensure that they are working with the current software version and current definition file. The assessment team can also familiarize itself with current—or all—vulnerabilities, by platform or other breakdown, from various noted IA and security web sites, such as http://isc.sans.org/, http://www.us-cert.gov/, http://www.cert.org/, http://www.securityfocus.com/, and http://www.infosyssec.com/. These sites maintain databases explaining current and historical vulnerabilities, and also provide forums for dissemination of current computer security news and information, such as "Common Security Vulnerabilities in E-Commerce Systems." [MOOKHEY, 2004]

Conduct of the Assessment

Minimize Assessment Duration

Any assessment can be stressful to both the assessed organization as well as to the assessment team. Assessments take time and resources away from the assessed organization that could otherwise be used for the conduct of business. In addition to time and resources expended on an assessment, the assessed organization is generally deficient in both paperwork and practice, and in general, ends up devoting a portion of its time and resources for a time prior to assessment preparing. Conversely, an assessment team also spends time and resources preparing to assess an organization, in order to provide a thorough and professional evaluation. For these reasons, an assessment team should strive to conduct an assessment in as little time as practical, to ensure minimization of loss of time and resources. Particularly, in the case of an IA assessment, where information availability is potentially reduced during the conduct of the assessment, this attempt to conduct the assessment thoroughly in the minimal amount of time is of particular concern.

Use Checklists

In order to conduct a thorough and professional assessment of an organization's IA posture in a minimal time frame, an assessment team should conduct its assessment from a set of checklists. Checklists provide a sequential

set of instructions that lead an assessment team in an organized and professional order from inception to conclusion of an assessment and ensure that all necessary tasks are accomplished and all relevant information is evaluated. Checklists are valuable tools for every step and piece of the assessment, and for subsections as well. Whereas an overall assessment checklists can provide the assessment team leader an understanding of what tasks have and have not been accomplished and how far along the assessment is, each major assessment task can also have its own checklist; this breakdown can be continued down to the level in which individual actions are accomplished; for example, one task on the overall assessment may involve the conduct of the software assessment tools, which can be broken down into a daily checklist of software tools to be used, which can be broken down to the steps for using each software tool. In this manner, a detailed assessment plan can be laid out so that an assessment team can inform the assessed organization how the team intends to conduct its assessment. While the actual conduct of the assessment may or may not be conducted flawlessly according to plan, the assessment team will at least have a cookbook checklist as a point from which to start and can adjust and document the plan accordingly. For an example of an overall checklist from which to conduct an IA assessment, the reader is directed to Appendix A; this checklist is one approach to an IA assessment, and could, in fact, be subordinated into lower checklists for further detail of actions. The checklist in Appendix A is also broken into eight major sections that can be tasked out to individual teams.

Break the Assessment Into Manageable Pieces

Creating a detailed assessment plan through a series of checklists accomplishes several important actions. As already stated, a detailed assessment plan based on a series of checklists provides the assessment team with a starting plan from which to begin conducting an assessment. In addition to this, a detailed assessment plan also helps an assessment team to break an assessment into manageable pieces that can be tasked to individuals or teams. This, again, allows an assessment team to minimize the time required to conduct the assessment while also ensuring that all of the individual pieces are given thorough attention by individuals or teams who see their pieces through from start to finish; in this fashion, tasks can be parceled to individuals or teams to be thoroughly conducted and then rolled up into the final assessment report. Some specific pieces that can be parceled out include: review of organizational IA policy, interview of system administrators and other privileged users as well as all other authorized users, enumeration of network and computer resources, and conduct of software tool assessments.

Conduct Under Lack of Resources

Creation and use of a detailed assessment plan and conduct of all tasks assumes that the assessment team has the resources to conduct the full assessment. If it does not, then compromise has to be made as to whether to conduct a shallower assessment or to remove certain tasks from the assessment

plan. Both choices leave potential vulnerabilities unmitigated and, indeed, unknown. For this reason, the better choice between the two compromises, given limited resources for the assessment, is to conduct a limited number of overall tasks but to conduct those tasks thoroughly; in this manner, an assessment team can report on those vulnerabilities it finds and can clearly delineate which portions of an organization's IA posture were not reviewed.

Reporting

Template Reports

Once the conduct of the assessment is completed, the assessment team needs to conduct reporting procedures. Actually, reporting procedures begin during the preparation phase, when the assessment team ensures it has templates for all reports it intends to complete. While the creation of template reports may be tedious in the preparation phase, it pays dividends during and after the conduct of the evaluation, as reports can be available to be added to continually and finalized quickly. In this manner, preliminary reports can be assembled and finished prior to the assessment team's departure or conclusion of the assessment.

Quick-Look Report

This leads to an important precept in assessment reporting—the assessment team should provide immediate feedback to assessed organization. This can be accomplished through a slide brief, a short synopsis, or "quick-look" report, of the conduct of the assessment and a schedule for the follow-on of a final report. Certainly the assessment team needs time to review all data and come to final conclusions based on fact, but clear vulnerabilities that need immediate attention and trends that do not require a great deal of analysis can be brought to light immediately. This gives the assessed unit a general picture of how the results will turn out, as a lack of immediately noted trends and vulnerabilities tends to reveal a positive outcome, while a preponderance of trends and vulnerabilities tells the assessed unit that the final report will be multiplicative of the early findings.

Final Report

The final result should display for the organization what vulnerabilities were found and should explain how, if known, to mitigate those vulnerabilities. Of importance is whether vulnerabilities are in violation of organizational policy, noting a lack of policy enforcement, or a are vulnerabilities the assessment team noted as not being covered or mitigated in policy, validating a need for policy update or review. The preliminary report gives the assessed organization a general feeling for how the reduction of data will conclude in a final report, and a cover letter to the final report can provide a high-level summary of the conduct of the assessment and an overall impression of the assessment team's results, but the body of the final report needs to be comprised of the details necessary for the

assessed organization's system administrators to correct vulnerabilities and effectively mitigate risks as needed.

Conclusion

It should be clear to the reader that the organization attempting to mitigate risks associated with IA should welcome an IA assessment. Likewise, the team levied to assess an organization's IA posture should be capable, professional, and thorough in its evaluation of the organization; anything less can lead to falsely positive assumptions within the assessed organization concerning its IA posture and to unmitigated holes in the organization's IA posture that can lead to unacceptable losses of availability, integrity, or confidentiality.

A competent IA assessment team needs to understand Information Assurance and all of its related facets and terminology, in order to determine what to look for and what to expect. An IA assessment team should prepare for a formal assessment by laying out the scope of the assessment, taking care of all administrative aspects, and defining roles and responsibilities of the assessment team and the assessed organization. In doing so, the conduct of the assessment should be thorough and professional, while minimizing the detraction of time and resources from the assessed unit. Finally, reporting should be conducted efficiently and as quickly as practical, providing immediate feedback of initial observations followed by a detailed and organized assessment of collected data.

In the end, the real measure of how well an IA assessment was conducted is whether an assessed organization, after evaluating the assessment team's reports and mitigating any unnecessary vulnerabilities, can perform all of its intended and required capabilities within a framework of minimal risk.

Appendix A: IA Assessment Checklist

This checklist is intended to be a tool for the IA assessment team, with the goal of evaluating overall IA posture. It is separated into a series of blocks, each with supporting steps. Each step has been given a referential title, a description, standards to resolve whether the step passes or fails, and specific data collection methods to provide data for resolution of standards.

Note that this checklist includes some specific requirements, such as Configuration Control Board review in Step 1. This checklist is a modification of a checklist developed by a number of sources—including the author of this paper—that is designed to address Department of Defense Information Assurance (IA) issues, and will contain some specific items and steps that users will want to modify to their situation. The user is strongly urged to review the checklist in its entirety and modify it to fit the specific criteria that the assessment team will be looking for in policy and in software vulnerability assessment.

For grading purposes, it is important to note that all checklist step descriptions are taken from the Department of Defense Instruction on Information Assurance, "Information Assurance (IA) Implementation," [DODI8500.2, 2003] Enclosure 4. The IA control measures in this enclosure form a basis for a solid checklist, which is why they are used here. Additionally, the architect of the original checklist that this checklist derives from is Charles Minnis, who originally took all of the control measures from the DoD instruction and laid them out in checklist style. Edmund Spinella and Peter Christensen have also made comments and additions. All other work is the product of the author of this paper, who laid out the Title, Description, Pass/Fail Standards, Data Collection Methods format, modified the original checklist to create the Pass/Fail Standards, derived appropriate Data Collection Methods from personal experience and research, and provided a title to each checklist step. The author further added the Checklist Verification List for purpose of being able to check off completed steps as accomplished and the Checklist Table of Contents, hyperlinked, to make the checklist an easily navigable and usable document. The author's thanks go to all persons who helped to make this checklist possible, which includes, in addition to those persons listed above, all persons in the business of conducting IA research for Department of Defense interests.

IA Checklist Table of Contents

Checklist Verification List

- ❑ STEP 1.: CCB Control
- ❑ STEP 2.: Functional Architecture
- ❑ STEP 3.: HW Baseline Inventory
- ❑ STEP 4.: Potential Hosting Enclaves and Software
- ❑ STEP 5.: IA Role Appointments and Responsibility Designations
- ❑ STEP 6.: SW Comprehensive Baseline Inventory
- ❑ STEP 7.: Authentication via Individual Identifier
- ❑ STEP 8.: Comprehensive Account Management Process
- ❑ STEP 9.: Audit Trail Records Reviewed
- ❑ STEP 10.: Host-Based Intrusion Detection System
- ❑ STEP 11.: Transaction Roll Back and Journaling
- ❑ STEP 12.: Audit of Security Label Changes
- ❑ STEP 13.: Successive Logon Attempt Control
- ❑ STEP 14.: Security of Privileged User Accounts Through Separation of Duties
- ❑ STEP 15.: Classification Level Marking and Labeling
- ❑ STEP 16.: Conformance Testing
- ❑ STEP 17.: Network Device Control Program Implemented
- ❑ STEP 18.: Privileged User Account Administration
- ❑ STEP 19.: Audit Record Reviewing Tools
- ❑ STEP 20.: Audit Record Retention
- ❑ STEP 21.: Security Configuration Measures Applied
- ❑ STEP 22.: Audit Record Backup
- ❑ STEP 23.: Protection of Audit Trail Contents
- ❑ STEP 24.: Virus Protection Implementation
- ❑ STEP 25.: Appropriate Warning Banner
- ❑ STEP 26.: Defense Mechanisms (Firewall, IDS, etc.) Deployed at Enclave Boundary
- ❑ STEP 27.: Remote Access for Privileged Functions
- ❑ STEP 28.: Managed Access Control Point for Remote Access
- ❑ STEP 29.: VPN Traffic Visibility
- ❑ STEP 30.: Physical Access
- ❑ STEP 31.: Maintenance Performed by Authorized Personnel
- ❑ STEP 32.: Access to Protected Information
- ❑ STEP 33.: Rules for IA Operations and Responsibilities
- ❑ STEP 34.: Training for IA Responsibilities
- ❑ STEP 35.: Alternate Site for Functional Restoration
- ❑ STEP 36.: Data Backup
- ❑ STEP 37.: Disaster Plan
- ❑ STEP 38.: Enclave Boundary Defense at Alternate Site
- ❑ STEP 39.: Exercise of Continuity of Operations Plan (COOP) and Contingency Plan
- ❑ STEP 40.: Maintenance Support for Key IT Assets
- ❑ STEP 41.: Uninterrupted Power to Key IT Assets

- ❑ STEP 42.: Maintenance Spares
- ❑ STEP 43.: Trusted Recovery Procedures
- ❑ STEP 44.: Incident Response Plan
- ❑ STEP 45.: Comprehensive Vulnerability Management Process

***Block 1*: Design and Configuration supports business functions.**	
STEP 1.: CCB Control Description: Verification that all information systems are under the control of a chartered Configuration Control Board(CCB) that meets regularly. The Information Assurance Manager (IAM) is a member of the CCB. Pass/Fail Standard: 1.) Is the system under control of a CCB that meets regularly? 2.) Is the IAM a member of the CCB? Data Collection Method: 1.) View CCB charter/appointment letter. 2.) View IAM appointment letter to CCB. 3.) View training schedule or CCB-specific schedule showing meeting dates. 4.) View meeting minutes from most recent meeting.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 2.: Functional Architecture

☐ Pass
☐ Fail
☐ Not Evaluated

Description:

Verification that for AIS applications, a functional architecture that identifies the following has been developed and is maintained:
- all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface
- user roles required for access control and the access privileges assigned to each role
- unique security requirements (e.g., encryption of key data elements at rest)
- categories of sensitive information processed or stored by the AIS application, and their specific protection plans
- restoration priority of subsystems, processes, or information.

Pass/Fail Standard:

1.) Is there a functional architecture that identifies external interfaces, the information being exchanged, and the protection mechanisms associated with each interface?
2.) Is there a functional architecture that identifies user roles required for access control and the access privileges assigned to each role?
3.) Is there a functional architecture that identifies unique security requirements (e.g., encryption of key data elements at rest)?
4.) Is there a functional architecture that identifies categories of sensitive information processed or stored by the AIS application, and their specific protection plans?
5.) Is there a functional architecture that identifies restoration priority of subsystems, processes, or information?

Data Collection Methods:

1.) View policy on external interfaces, information being exchanged, and protection mechanisms associated with each interface.
2.) View user role requirements and privileges.
3.) View policy on any unique security requirements.
4.) View specification of categories of sensitive information processed or stored by the AIS application, and specific protection plans for that information. Ask for clarification at interview.
5.) View policy on restoration priority of subsystems, processes,

or information. 6.) Interview Question: What is the order of restoration of systems and links when restoring system?	
Comments:	
STEP 3.: HW Baseline Inventory Description: Verification that a current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB). A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. Pass/Fail Standard: 1.) Is a current and comprehensive baseline inventory of all hardware (HW) required to support enclave operations maintained by the Configuration Control Board (CCB)? 2.) Is a backup copy of the inventory stored in a fire-rated container or otherwise not collocated with the original? Data Collection Method: 1.) View baseline HW inventory. 2.) Verify against actual system hardware. Note discrepancies. 3.) Note location of backup copy of HW inventory.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 4.: Potential Hosting Enclaves and Software Description: Verification that for AIS applications, a list of all (potential) hosting enclaves is developed and maintained along with connection rules and requirements. For enclaves, a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms is developed and maintained along with connection rules and requirements. Pass/Fail Standard: 1.) Has a list of all (potential) hosting enclaves been developed and maintained along with connection rules and requirements? 2.) Is a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms developed and maintained along with connection rules and requirements? Data Collection Method: 1.) View the list of all potential hosting enclaves. 2.) View connection rules and requirements for potential hosting enclaves. 3.) View the list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms. 4.) View connection rules and requirements for hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 5.: IA Role Appointments and Responsibility Designations Description: Verification that all appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the Information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup or emergency response). Pass/Fail Standard: 1.) Are all appointments to required IA roles (e.g., Information Assurance Manager, System Administrator {Privileged User}) established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation? 2.) Is a System Security Plan established that describes the technical, administrative, and procedural IA program and policies that govern the information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response)? Data Collection Method: 1.) View appointment letters; ensure they establish roles and assigned duties and appointment criteria such as training, security clearance, and IT-designation. 2.) View System Security Plan for the technical, administrative, and procedural IA program and policies that govern the information system, and identify all IA personnel and specific IA requirements and objectives.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 6.: SW Comprehensive Baseline Inventory Description: Verification that a current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support Information system operations is maintained by the CCB. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. Pass/Fail Standard: 1.) Is a current and comprehensive baseline inventory of all software (SW) required to support the system maintained by the Configuration Control Board (CCB)? 2.) Is a backup copy of the inventory stored in a fire-rated container or otherwise not collocated with the original? Data Collection Method: 1.) View baseline inventory of software required to support system. Ensure it is maintained by the CCB. 2.) Audit systems to note discrepancies as to software on the system vs software on the inventory. 3.) View backup copy and storage container.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

***Block 2*: Identification and Authentication should restrict unauthorized access in the business environment.**	
STEP 7.: Authentication via Individual Identifier Description: Information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each. At least four characters must be changed when a new password is created. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission. Pass/Fail Standard: 1.) Are individual identifiers used to logon to the system? 2.) For systems using logon ID does the password meet minimum requirements stated above? 3.) Does the policy for issuing passwords meet minimum requirements stated above? 4.) Are mechanisms implemented to protect passwords to meet minimum requirements stated above? 5.) Are all factory set, default or standard-user IDs and passwords removed or changed? Data Collection Method: 1.) Evaluate password policy 2.) Observe logon procedures 3.) Use automated tools to evaluate password policy compliance/complexity and factory default settings are changed/removed/modified	☐ Pass ☐ Fail ☐ Not Evaluated

Comments:	
STEP 8.: Comprehensive Account Management Process Description: Verification that a comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated. Pass/Fail Standard: 1.) Is a comprehensive account management process implemented to ensure that only authorized users can gain access to workstations, applications, and networks? 2.) Are individual accounts, which are designated as inactive, suspended, or terminated, promptly deactivated? Data Collection Method: 1.) Evaluate user policy documentation on access. 2.) Get a roster of personnel that have left the organization recently (3 months). 3.) Verify that personnel who have recently left do not have active accounts.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

***Block 3*: The Enclave and Computing Environment should support business functions.**	
STEP 9.: Audit Trail Records Reviewed Description: Verification that audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with Information system IA procedures. Pass/Fail Standard: 1.) Are audit trail records from all available sources regularly reviewed for indications of inappropriate or unusual activity? 2.) Are suspected violations of IA policies analyzed and reported in accordance with IA policy reporting procedures? Data Collection Method: 1.) Verify that audit trail records are being recorded for all available sources. 2.) Evaluate results of recent reviews, if available. 3.) Evaluate audit records for possible inappropriate or unusual activity to validate local reporting process. 4.) Evaluate audit policy and reporting procedures.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 10.: Host-Based Intrusion Detection System Description: Verification that host-based intrusion detection systems are deployed for major applications and for network management assets, such as routers, switches, and domain name servers (DNS). Pass/Fail Standard: 1.) Is a host-based intrusion detection systems deployed for major applications and for network management assets, such as routers, switches, and domain name servers? Data Collection Method: 1.) Evaluate host-based intrusion detection policy and software/setup.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 11.: Transaction Roll Back and Journaling Description: Verification that transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents. Pass/Fail Standard: 1.) Do transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents? Data Collection Method: 1.) Evaluate transaction roll-back and transaction journaling, or technical equivalents.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 12.: Audit of Security Label Changes Description: Verification that system automatically records the creation, deletion, or modification of confidentiality or integrity labels, if required by the information owner. Pass/Fail Standard: 1.) Does IA policy require an audit of security label changes? 2.) Does the system automatically records creation, deletion, or modification of confidentiality or integrity labels? Data Collection Method: 1.) Determine if IA policy requires an audit of security label changes? 2.) If so, confirm the system automatically records creation, deletion, or modification of confidentiality or integrity labels	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 13.: Successive Logon Attempt Control

☐ Pass
☐ Fail
☐ Not Evaluated

Description:

Verification that successive logon attempts are controlled using one or more of the following:
- access is denied after multiple unsuccessful logon attempts.
- the number of access attempts in a given period is limited.
- a time-delay control system is employed.

If the system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions. Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon.

Pass/Fail Standard:

1.) Are successive logon attempts controlled using one of the above methods?
2.) If multiple logon sessions are allowed, is the number of logon sessions controlled?
3.) Is the user notified of the date and time of the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon?

Data Collection Method:

1.) View successive logon policy.
2.) Verify policy through successive logon attempts.
3.) Verify system control of multiple concurrent logon sessions.
4.) Verify user notification of last logon and number of previous unsuccessful logon attempts.

Comments:

STEP 14.: Security of Privileged User Accounts Through Separation of Duties Description: Verification that access procedure enforces the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization. *(Note: This control is in addition to an appropriate security clearance and need-to-know authorization.)* Pass/Fail Standard: **1.)** Is access to privileged accounts limited to privileged users? **2.)** Is the use of privileged accounts limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions? Data Collection Method: 1.) View privileged user access policy. 2.) Interview privileged users to verify account usage and access protection. 3.) Verify recent use of non-privileged accounts by privileged users.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 15.: Classification Level Marking and Labeling Description: Verification that information and Information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions. Pass/Fail Standard: 1.) Do the markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions? Data Collection Method: 1.) Evaluate marking and labeling policy. 2.) Evaluate markings and labels on operational information systems.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 16.: Conformance Testing Description: Verification that conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as IAVA or other IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities. Pass/Fail Standard: 1.) Is conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the IAVA or other IA practices is planned, scheduled, conducted, and independently validated? Data Collection Method: 1.) Evaluate the conformance testing policy. 2.) Evaluate results from most recent penetration test.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 17.: Network Device Control Program Implemented Description: Verification that an effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA). Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested. Pass/Fail Standard: 1.) Is an effective network device (e.g., routers, switches, firewalls) control program implemented? Data Collection Method: 1.) Evaluate policy on use and configuration of network devices control programs. 2.) Evaluate COOP and Contingency Plan. 3.) Evaluate system and system diagram to ensure system matches policy.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 18.: Privileged User Account Administration Description: Verification that all privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). The IAM tracks privileged role assignments. Pass/Fail Standard: 1.) Are all privileged user accounts established and administered in accordance with a role-based access scheme? 2.) Does the IAM track privileged role assignments? Data Collection Method: 1.) Evaluate assignment procedures for privileged role assignments or list of privileged role assignments, as maintained by IAM. 2.) Evaluate policy on privileged role assignments.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 19.: Audit Record Reviewing Tools Description: Verification that tools are available for the review of audit records and for report generation from audit records. Pass/Fail Standard: 1.) Are tools available for the review of audit records and for report generation from audit records? Data Collection Method: 1.) Evaluate tools used to audit records. 2.) Evaluate audit using above tools.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	
STEP 20.: Audit Record Retention Description: Verification that audit records are retained for a duration as specified in IA policy. Pass/Fail Standard: 1.) Are audit records retained for duration as specified in IA policy? Data Collection Method: 1.) Verify audit retention requirements in policy. 2.) Evaluate audit records and associated dates.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 21.: Security Configuration Measures Applied Description: Verification that for enclaves and AIS applications, all appropriate security configuration measures have been applied. Pass/Fail Standard: 1.) Have all appropriate security configuration measures been applied? Data Collection Method: 1.) Examine requirements for the use of security configuration measures in policy. 2.) Spot check that enclave hosts' local policy meets or exceeds security configuration measures required.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 22.: Audit Record Backup Description: Verification that the audit records are backed up not less than weekly onto a different system or media than the system being audited. Pass/Fail Standard: 1.) Are audit records backed up not less than weekly onto a different system or media than the system being audited? Data Collection Method: 1.) Evaluate backup policy. 2.) Evaluate most recent backup, ensuring it is no more than 1 week old. 3.) Interview privileged users to verify that backups are occurring.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 23.: Protection of Audit Trail Contents Description: Verification that the contents of audit trails are protected against unauthorized access, modification or deletion. Pass/Fail Standard: 1.) Are the contents of audit trails protected against unauthorized access, modification or deletion? Data Collection Method: 1.) Evaluate policy on audit trail information protection. 2.) Verify audit trail information is properly protected as per policy.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 24.: Virus Protection Implementation Description: Verification that all servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates. Pass/Fail Standard: 1.) Do servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates? Data Collection Method: 1.) Verify virus protection requirement in policy and SW baseline 2.) Verify virus protection software on servers, workstations and mobile computing devices. 3.) Verify automatic update capability on the above systems.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 25.: Appropriate Warning Banner Description: Verification that all users are provided with appropriate privacy and security notices upon login to include statements informing them that they are subject to monitoring, recording and auditing as necessary. Pass/Fail Standard: 1.) Are individuals who access the system provided security notices and statements regarding monitoring, recording and auditing? Data Collection Method: 1.) Ensure warning banner requirement is in policy. 2.) Spot-check warning banner on system or enclave hosts as required by policy.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

Block 4: Enclave Boundary Defense should protect the enclave from unauthorized access.

STEP 26.: Defense Mechanisms (Firewall, IDS, etc.) Deployed at Enclave Boundary

☐ Pass
☐ Fail
☐ Not Evaluated

Description:

Verification that boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other Information systems by physical or technical means.

Pass/Fail Standard:

1.) Is Internet access proxied through Internet access points that are under the management and control of the enclave and are isolated from other Information systems by physical or technical means?
2.) Is layered defense in depth implemented at internal enclave boundaries and at key points in the network?

Data Collection Method:

1.) Confirm Network Diagrams indicate that network assets are isolated from the Internet via appropriate physical and technical means such as a Firewall, IDS or similar device.
2.) Confirm physical and/or technical means are appropriately implemented.
3.) Confirm layered defense in depth is implemented at internal enclave boundaries and at key points in the network, as required.

Comments:

STEP 27.: Remote Access for Privileged Functions Description: Verification that remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. Remote sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the Information Assurance Manager(IAM) reviews the log for every remote session. Pass/Fail Standard: 1.) Is a complete audit trail of each remote session recorded, and the IAM reviews the log for every remote session? Data Collection Method: 1.) Evaluate policy on remote access. 2.) Evaluate assessment results of open ports in order to verify possible remote access functions. 3.) Evaluate audit logs as per IAM to note remote access activity. 4.) Interview privileged users on use of remote access.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 28.: Managed Access Control Point for Remote Access Description: Verification that all remote access to Information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected. Pass/Fail Standard: 1.) Is all remote access to Information systems, to include telework access, mediated through a managed access control point, such as a remote access server in a DMZ? 2.) Remote access always uses encryption to protect confidentiality? Data Collection Method: 1.) Evaluate remote access policy. 2.) Interview privileged users who manage the DMZ for remote access (including telephone access) procedures. 3.) Interview privileged users who manage DMZ on remote access encryption. Note: Penetration testing may be appropriate to evaluate this MOE.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 29.: VPN Traffic Visibility Description: Verification that all VPN traffic is visible to network intrusion detection systems (IDS). Pass/Fail Standard: 1.) All VPN traffic is visible to network intrusion detection systems (IDS). Data Collection Method: 1.) Examine IDS traffic records to confirm visibility of VPN traffic.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

***Block 5*: Physical and Environmental Controls should support business functions.**	
STEP 30.: Physical Access Description: Verification that only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information and that only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release. Pass/Fail Standard: 1.) Are only authorized personnel with appropriate clearances granted physical access to computing facilities that process classified information? 2.) Are only authorized personnel with a need-to-know access granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release? Data Collection Method: 1.) Evaluate policy and execution of physical access controls as described IA policy or Standard Operating Procedures(SOPs). 2.) Test physical access, preferably with both authorized and unauthorized personnel.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

***Block 6*: Personnel Controls should ensure the confidentiality of the system and resident information.**	
STEP 31.: Maintenance Performed by Authorized Personnel Description: Verification that maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel are documented. Pass/Fail Standard: 1.) Is maintenance only performed by authorized personnel? 2.) Are the processes for determining authorization and the list of authorized maintenance personnel documented? Data Collection Method: 1.) Verify maintenance personnel are explicitly authorized by name to maintain system. 2.) Verify that policy reflects the above procedures.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 32.: Access to Protected Information Description: Verification that only individuals who have a valid need-to-know and who satisfy all personnel security criteria are granted access to information with special protection measures or restricted distribution as established by the information owner. Pass/Fail Standard: 1.) Are only individuals who have a valid need-to-know, and who satisfy all personnel security criteria granted access to information with special protection measures or restricted distribution as established by the information owner? Data Collection Method: 1.) Confirm that individuals granted access to information meet need-to-know and personnel security criteria.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 33.: Rules for IA Operations and Responsibilities Description: Verification that a set of rules that describe the IA operations of the Information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access. Pass/Fail Standard: 1.) Does the system have Security Rules of Behavior? 2.) Do the rules include consequences of inconsistent behavior or non-compliance? 3.) Is signed acknowledgement of the rules a condition of access? Data Collection Method: 1.) Evaluate policy for security rules of behavior. 2.) Evaluate consequences of inconsistent behavior or non-compliance in policy. 3.) Evaluate past signed acknowledgement of the rules.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 34.: Training for IA Responsibilities Description: Verification that a program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA-related plans such as incident response, configuration management and Continuity of Operations Plan (COOP) or disaster recovery. Pass/Fail Standard: 1.) Do personnel receive initial and periodic IA training? Data Collection Method: 1.) Review unit training logs for IA training.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

Block 7: Continuity Controls should sustain availability in the business environment.	
STEP 35.: Alternate Site for Functional Restoration Description: Verification that alternate site is identified that permits the restoration of all business essential functions. Pass/Fail Standard: 1.) Is an alternate site identified that permits the restoration of all mission or business essential functions? Data Collection Method: 1.) Evaluate alternate site. 2.) Review restoration process in IA policy, such as in COOP. 3.) Review restoration process in interviews. Note: This site will be exercised if COOP is exercised during testing.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 36.: Data Backup Description: Verification that data backup is performed daily, and recovery media are stored off-site at a location that affords appropriate protection of the data. Pass/Fail Standard: 1.) Is a data backup performed daily, and recovery media stored off-site at a location that affords protection of the data? Data Collection Method: 1.) Confirm data backups performed daily 2.) Confirm recovery media is stored off-site at a location that affords protection of the data Note: Demonstration of data restoration may be required.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 37.: Disaster Plan Description: Verification that a disaster plan exists that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.) Pass/Fail Standard: 1.) Does a disaster plan exist that provides for the smooth transfer of all mission or business essential functions to an alternate site? 2.) Is the plan adequate to support the mission for the duration of an event with little or no loss of operational continuity? Data Collection Method: 1.) Evaluate the disaster plan and confirm it provides for smooth transfer of all business essential functions to an alternate site. This plan may include disaster recovery procedures, business recovery plans, system contingency plans and/or, facility disaster recovery plans and plan acceptance. 2.) Verify that the plan is adequate to support business operations for the duration of an event with little or no loss of operational continuity. Note: These plans should be executed to fully evaluate effectiveness in step labeled “Exercise of COOP and Contingency Plan”.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 38.: Enclave Boundary Defense at Alternate Site Description: Verification that enclave boundary defense at the alternate site provides security measures equivalent to the primary site. Pass/Fail Standard: 1.) Does the enclave boundary defense at the alternate site provide security measures equivalent to the primary site? Data Collection Method: 1.) Confirm enclave boundary defense at the alternate site provides security measures equivalent to the primary site.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 39.: Exercise of Continuity of Operations Plan (COOP) and Contingency Plan Description: Verification that the continuity of operations or disaster recovery plans or significant portions are exercised semi-annually. Pass/Fail Standard: 1.) Are significant portions of the continuity of operations or disaster recovery plans exercised semi-annually? Data Collection Method: 1.) Confirm policy explicitly requires semi-annual exercise of continuity of operations or disaster recovery plans. 2.) Exercise and evaluate as much of the disaster recovery plan as feasible. If possible, evaluate scheduled exercise(s) and most recent exercise. 3.) Interview privileged users on exercise of continuity of operations or disaster recovery plans.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 40.: Maintenance Support for Key IT Assets Description: Verification that maintenance support for key IT assets is available to respond 24 X 7 immediately upon failure. Pass/Fail Standard: 1.) Is maintenance support for key IT assets available to respond 24 X 7 immediately upon failure? Data Collection Method: 1.) Verify that maintenance support is in place that will provide immediate maintenance assistance. 2.) Evaluate maintenance support to confirm timely support provided.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 41.: Uninterrupted Power to Key IT Assets Description: Verification that electrical systems are configured to allow continuous or uninterrupted power to key IT assets and all users accessing the key IT assets to perform mission or business-essential functions. This may include an uninterrupted power supply coupled with emergency generators or other alternate power source. Pass/Fail Standard: 1.) Are electrical systems configured to allow continuous or uninterrupted power to key IT assets and all users accessing the key IT assets to perform mission or business-essential functions? Data Collection Method: 1.) Ensure system has provisions for uninterrupted power to key IT assets and all users accessing those assets to perform mission or business-essential functions as described. 2.) Evaluate uninterrupted power supplies to key IT assets and all users that access those assets to perform mission or business-essential functions; verify primary uninterrupted power supply use as for those key IT assets and users. 3.) Evaluate generators used to restore power to key IT assets; verify primary generator use as for those key IT assets and users. 4.) Conduct a loss of power drill.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 42.: Maintenance Spares Description: Verification that maintenance spares and spare parts for key IT assets are available 24 X 7 immediately upon failure. Pass/Fail Standard: 1.) Are maintenance spares and spare parts for key IT assets available 24 X 7 immediately upon failure? Data Collection Method: 1.) Verify that ordering procedures are in place that should lead to immediate delivery of maintenance spares and spare parts. 2.) Exercise supply system to demonstrate availability.	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

STEP 43.: Trusted Recovery Procedures Description: Verification that recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place. Pass/Fail Standard: 1.) Do recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner? Data Collection Method: 1.) Evaluate recovery procedures as stated in policy. 2.) Evaluate circumstances that can inhibit a trusted recovery as documented in policy. 3.) Evaluate procedures as written in policy for mitigating those circumstances that can inhibit a trusted recovery. 4.) Verify data integrity after recovery (MD5 hashsums of files; TripWire comparison, etc)	☐ Pass ☐ Fail ☐ Not Evaluated
Comments:	

***Block 8*: Vulnerability and Incident Management procedures should ensure a defensive IA posture of the system within the business environment.**

STEP 44.: Incident Response Plan

☐ Pass
☐ Fail
☐ Not Evaluated

Description:

Verification that an incident response plan exists that defines reportable incidents, outlines a standard operating procedure for incident response, provides for user training, and establishes an incident response team. The plan is exercised at least every 6 months.

Pass/Fail Standard:

1.) Does an incident response plan exists that, defines reportable incidents, outlines a standard operating procedure for incident response, provides for user training, and establishes an incident response team?
2.) Is the plan exercised at least every 6 months?

Data Collection Method:

1.) Evaluate incident response procedures.
2.) Confirm definition of reportable incidents.
3.) Evaluate SOP for incident response.
4.) Evaluate procedures for user training.
5.) Identify incident response team.
6.) Confirm plan has been exercised in the last 6 months.

Comments:

STEP 45.: Comprehensive Vulnerability Management Process Description: Verification that a comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) [CVE, 2004] naming convention and use the Open Vulnerability Assessment Language (OVAL) [OVAL, 2004] to test for the presence of vulnerabilities. Pass/Fail Standard: 1.) Is a comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities in place? 2.) Whenever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools? 3.) Have vulnerability assessment tools been acquired, personnel been appropriately trained, procedures been developed, and regular internal and external assessments are conducted. 4.) For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities? Data Collection Method: 1.) Evaluate vulnerability management process in policy. 2.) Evaluate vulnerability assessment tools as used to conduct assessment. 3.) Evaluate results of most recent internal assessment. 4.) Conduct a vulnerability assessment with automated tools.	☐ Pass ☐ Fail ☐ Not Evaluated

Comments:

Appendix B: References

1. [CARNEGIE, 2004]: Carnegie Mellon Software Engineering Institute. “Cert Coordination Center.” <http://www.cert.org/>. updated May 3, 2004. May 3, 2004.

2. [CSRC, 2004]: National Institute of Standards and Technologies (NIST). “Computer Security Resource Center (CSRC).” <http://csrc.nist.gov/>. created Jan 28, 2004. May 3, 2004.

3. [CURTS, 2003]: Curts, Raymond J., Ph.D., and Campbell, Douglas E., Ph.D. Building a Global Information Assurance Program. Boca Raton, FL: Auerbach, 2003.

4. [CVE, 2004]: The MITRE Corporation. “Common Vulnerabilities and Exposures.” <http://cve.mitre.org/>. updated Apr 28, 2004. May 3, 2004.

5. [DODI8500.2, 2003]: Department of Defense (DoD). Information Assurance (IA) Implementation. DoDI 8500.2. Department of Defense, 06 February, 2003. <http://niap.nist.gov/cc-scheme/d85002p.pdf>.

6. [Herrmann, 2002]: Herrmann, Debra S. Security Engineering and Information Assurance. Boca Raton, FL: Auerbach, 2002.

7. [IASE, 2004]: Defense Information Systems Agency. “Information Assurance Support Environment.” <http://iase.disa.mil>. May 3, 2004.

8. [IATAC, 2004]: “Information Assurance Technology Analysis Center (IATAC).” <http://iac.dtic.mil/iatac/>. May 3, 2004.

9. [IATF, 1999]: U.S. National Security Agency (NSA). Information Assurance Technical Framework (IATF). Rel 2.0.1. Ft. Meade, MD: National Security Agency, Sep 1999.

10. [IATF, 2002]: U.S. National Security Agency (NSA). Information Assurance Technical Framework (IATF). Rel 3.1. Ft. Meade, MD: National Security Agency, Sep 2002. <http://www.iatf.net/framework_docs/version-3_1/index.cfm>.

11. [ISC, 2004]: The SANS Institute. “Internet Storm Center.” <http://isc.sans.org/>. updated May 3, 2004. May 3, 2004.

12. [MOOKHEY, 2004]: Mookhey, K. K. “Common Security Vulnerabilities in e-commerce systems.” <http://www.securityfocus.com/infocus/1775>. updated April 26, 2004. May 3, 2004.

13. [OVAL, 2004]: “Open Vulnerability Assessment Language.” <http://oval.mitre.org/>. updated Apr 21, 2004. May 3, 2004.

14. [TERMINOLOGY, 2004]: The MITRE Corporation. “Common Vulnerabilities and Exposures: Terminology.” <http://cve.mitre.org/about/terminology.html#Universal>. updated May 23, 2001. May 3, 2004.