Call For Papers - NCISSE 2001
5th National Colloquium for
Information Systems Security Education

2001: A security Odyssey
Government, Industry, and Academia

At

George Mason University
Fairfax, Virginia
May 22-24, 2001

INFOSEC Assessment Methodology (IAM)
A High Level Qualitative Vulnerability Assessment and Documentation Review That Can be Used by Government, Industry, and Academia

By

Robert K. Smith, CISSP

1-410-691-4052

Computer Sciences Corporation (CSC)
7459 Candlewood Road M/C 301
Hanover, Maryland, 21076

Rsmit204@csc.com

General Track White Paper
A Qualitative, High Level INFOSEC Assessment Methodology (IAM)

Introduction

In May 1998, the INFOSEC community became aware of the White Paper titled "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (PDD-63). Shortly after this date, the National Security Agency (NSA) using its technology transfer charter, took a proactive stance to the PDD-63 by offering an INFOSEC Assessment Methodology (IAM) course to government and private sector security professionals. The intent of the course is to make available a qualitative (not quantitative) approach for carrying out a high-level policy/documentation review that is non-intrusive, uses non-attribution (the process is not an inspection or an audit), yet produces an analysis of an organization's overall security posture. The course originally offered by the National Security Agency (NSA) may come under the National Information Assurance Partnership (NIAP). It is being offered to security professionals who have two years of INFOSEC experience at a minimum, and an overall five years of experience using the other security disciples. INFOSEC organizations can be appraised through use of a nine point Information Assurance Capability Maturity Model (IA-CMM). Once appraised, such an organization can deploy assessment teams who provide IA services through use of the IAM. The methodology should precede a technical approach for scanning the client's networks and hosts. If the client authorizes, the more technical scan of networks and hosts can occur concurrently with the IAM. (http://www.ciao.ncr.gov/CIAO_Document_Library/paper598.htm)

NSA has authorized a number of internal NSA security professionals and six private sector security professionals contractors to facilitate the two-day IAM class. As of the date of this paper, over 800 security professionals from all over the U.S. have taken the two-day training. Individuals who successfully passed the test, and who received a certificate, are soon to be listed on a web page so that any organization can call upon these security professionals to perform the IAM.

The methodology is currently being used throughout the government, the private sector, and in academia. The lead government agencies using the IAM are as follows:

1. National Security Agency (NSA)
2. General Services Administration (GSA), Federal Technology Service (FTS)
3. Defense Information Systems Agency (DISA), Field Security Ops (FSO)

At present, there is no way of knowing how many corporations, large and small, as well as how many individuals are teaming or forming alliances in order to field a team of IAM trained security professionals. The NSA is not following up behind private sector IAM service providers, and is taking the position that NSA is not responsible for the content or results of security assessments carried out by security professionals who passed the IAM exam and received a certificate. We as security professionals, performing an assessment

using the IAM, are solely responsible for the final report that represents the deliverable offered to our clients. (http://www.NSA.gov:8080/ISSO/IAM/index.htm)

Understanding the IAM Process

The IAM consists of three phases:

1. Pre-Assessment (1-2 day visit, then 2-4 weeks reading documentation)
2. On-Site Activities (1-2 weeks for interviews, demonstrations, documents)
3. Post-Assessment (2-8 weeks for analysis and final report writing).
   Note: The timeframes are offered as **guidelines only**. The scope of each assessment, based on the target environment, determines the number and expertise of the team, as well as the number of days or weeks to accomplish tasks.

Pre-Assessment Phase

Because of the variety of ways that an assessment comes to be, the discussion of marketing by the service provider/assessment team, and the required legal issues, statement of work issues, and other start up issues are deemed to be beyond the scope of this paper. The path is different depending on whether you are within the government, a corporation, a small business alliance, academia, or an individual looking to team with other security professionals in order to carry out an IAM. However, having been on a number of IAM teams, and using the lessons learned concept or constant process improvement technique, it is a good idea to include a marketing/budget presence on the initial discussions with the client or their legal representative. Once a client indicates acceptance and authorizes and IAM, then run the proposal past the legal staff or take the writings to a trusted legal representative who knows the pitfalls of poorly worded statements of work and business proposals.

In the Pre-Assessment Phase, the client and the assessment team collaborate (that is to say they co-labor) to understand what information is critical, and where the information is stored, processed and transmitted. The **client generally wants** the assessment team to identify critical information (not applications or platforms), ensure system charts are accurate, avoid crossing organizational boundaries during the assessment, and provide the best possible analysis of all security and security relevant documentation. It is to the client's advantage to provide an empowered, knowledgeable point of contact (POC) who may actually become a presence on the assessment team. The client wants to ensure that all possible security documentation is provided to the assessment team by specifying content as much as possible along with the title of each document. Not all reports are titled the same, but may have the security content the assessment team is looking for. A Disaster Recovery Report may have the needed content usually found in a Business Continuity Plan, or perhaps a Business Impact Analysis written by a different assessment service provider in an earlier security strengthening effort.

The **assessment team** generally wants to identify the critical information, acquire an accurate system configuration, understand and agree upon the scope of the assessment, and review all security and security relevant documentation. So, we see that the assessment team and the client are pursuing similar goals. This is as it should be if an assessment is to be successful and produce a useful security report/deliverable within budget and on time.

The service provider/assessment team wants to ensure that the appropriate expertise is represented on the team. If assessing a financial institution, ensure that team members have an accounting or financial background. If assessing a client server environment using Novell, ensure that technical team members have the requisite technical background. Don't send a mainframe-only type of person to assess an NT or UNIX environment. The team lead is responsible for ensuring that all team members have the proper security clearances or appropriate background investigation credentials. The team lead has templates available for whatever environment is to be assessed. Ensure that the team members have all signed the required nondisclosure agreement, and any trust agreements regarding proprietary information. The team lead must ensure that the client has provided the all-important "get out of jail" authorization for doing network scans (this is best provided on the client's letterhead and must be signed by a senior management official). Other proprietary templates that may be provided to the POC initially and to senior management are as follows:

1. A "security wish-list" of security documentation to request from the client (refers to content as well as document name)
2. An "interview schedule" broken down into roles/positions to be interviewed based on subject mater areas or categories (changes only if POC authorizes)
3. A complete listing of "intended questions" to be asked (based on subject matter areas or security categories appropriate to the type of organization)
4. A sample Information Criticality Matrix to focus on identifying critical/sensitive information assets (Appendix A)
5. A sample INFOSEC Assessment Plan so the client knows what the process is and the format and content ensures no surprises for either the client or assessment team (Appendix A)
6. If possible, ask for a "letter of Introduction" for assessment team members to present to interviewees who may not have been informed of the assessment
7. Come to an agreement (obtain a signed statement if possible) as to the level of detail/granularity that is to be provided in the final report.

On-Site Activities Phase

The On-Site Activities Phase focuses on validating the information gathered, with the cooperation of the client, during the Pre-Assessment Phase. The assessment team must meet and process observations/findings before closing out the workday while on-site. The component tasks of the On-Site Activities Phase are as follows:

1. Provide an In-brief to senior management and functional area representatives

2. Perform interviews of site personnel
3. Continue to discover and gather security relevant documentation
4. Continue analysis of documentation and findings surfaced in interviews
5. Request "system demonstrations" to resolve conflicting information (this complements, and is the equivalent of the technical, hands-on approach)
6. Craft and deliver an Out-brief of initial findings (these typically appear in the Assessment Plan, the Executive Summary, and are detailed in the final report).

During the In-brief, with senior management and functional area representatives present, the Assessment Plan and Information Criticality Matrix must be reviewed and agreed upon. It is important that both the client and the assessment team agree on the content of the plan. It must be accurate and current at this point. Any changes requested by the client must be noted and added to the Assessment Plan. An updated copy is provided to management through the POC before any interviews begin.

The IAM, by itself, is a high-level documentation assessment. If the client wants the technical team onsite concurrently with the non-technical team, then this is where a technical and non-technical approach can offer value added by complementing the high-level documentation analysis effort. Having said that, it is a good practice to keep the two teams from being perceived as doing any part of the other's tasking. This is because the documentation review team requests the organization's subject matter experts or designated users to provide system demonstrations to clarify any security observations/issues. These system demonstrations provide the equivalent of the actual hands-on used in the network and host scanning technical area. Clients become confused if they see the technical team doing hands-on scanning when the documentation team has said that nobody will touch a keyboard, but instead will request demonstrations of security capabilities.

Having both teams represented at the In-brief is critical to managing the client expectations, and will affect the modular format and "stand alone or pull-out-the applicable-section" format of the final report. The SA takes one section, and functional-area representatives take other sections of the report as applicable. Each can take their applicable section of the report to work on implementing recommended counter measures. The client may find that the network scan output reports are better presented as an appendix, or the clientr may want the applicable scan report details embedded within the discussion, vulnerability, and counter measure format of the final report. These report issues must be agreed upon during the early stages of the Pre-Assessment Phase.

Interviews must be handled by team members who interface well with people, in other words, they must not be short-fused, or have a disposition that could be interpreted as being "somewhat abrupt." Always interview with another assessor writing the responses. Often, team members have different strengths, some are better updating desktop oriented control files that are critical to the success of the team effort. The assessment team lead must effectively utilize the appropriate personnel in producing an effective assessment. For control purposes, it is best to have one team member responsible for updating all

Assessment Plan changes and final report enhancements. Do not stretch this person into other team tasks unless absolutely necessary. You do not want one of the client's concerns to be missed in the Out-brief or the final report. Remember that the Assessment Plan, when properly updated, maintained, and communicated, ensures that there are no surprises for senior management.

Interviews last anywhere from 30 minutes to two hours depending on the subject matter expert being interviewed. Interviewees must be comfortable and the interviewer must ensure, that nothing said during the interview will be associated with their name in any reports. It is considered a good practice to start with the senior management staff in order to learn what management "says and/or believes" is going on within the organization. Next, spend significant time with the System Security Administrators (SSAs) and the System Administrators (SAs). Then move to the user community. Between these three groups, exits very differing views of the organizational reality of how things are really accomplished. Be sensitive to the fact that there are probably some very good reasons (constraints such as lack of funding, and/or lack of staff) for why the organization has been "bending rules" instead of following industry best practices. Be diplomatic, be sensitive, but record shortcomings and valid observations of vulnerabilities.

Post-Assessment Phase

Suffice to say that the final phase is where you bring additional resources and expertise to the effort. Writing the final report is the objective here. You and the assessment team are back home at this point. Ensure the technical team members work closely with the non-technical Policy level team members in putting the observations/findings into a logical flow with the proper level of detail/granularity expected by the client. (Appendix B)

Conclusion

Security professionals have sought an industry-accepted format/methodology, a "common sheet of music to sing from" if you will, in order to provide a qualitative INFOSEC assessment. The IAM is such a methodology. It provides system owners a certain level of confidence that their information is protected through confidentiality, integrity and availability. Technical scans complement the IAM by providing technical direction as to how a network/host scan can provide needed evidence of the security vulnerabilities referred to in the documentation review level. We need to work together to strengthen America's critical infrastructure. Improving the American Infrastructure's security posture depends on all of us. The need for INFOSEC touches all Americans, at all levels of government, private sector, and academia. These three components must work together, that is to say, collaborate, take ownership, and share information if the greater vision needed to protect America's most critical resource, Americans is to be a reality before it becomes a disaster. Perhaps an information-age Pearl Harbor is looming in our future, perhaps not. The lesson to be learned is this: INFOSEC is not a destination, it is a journey; perhaps an unending journey!

Bibliography

Presidential Decision Directive 63, March 2000
http://www.ciao.ncr.gov/CIAO_Document_Library/paper598.htm)

NSA Information Technology Transfer Authority, August 1999
http://www.NSA.gov:8080/ISSO/IAM/index.htm

Critical Infrastructure Assurance Office, "Practices for Securing Critical Information Assets," January 2000
http://www.ciao.gov/CIAO_Document_Library/Practices_For_Securing_Critical_Information_Assets.pdf

APPENDIX A

INFOSEC Assessment Methodology (IAM)
Assessment Plan Outline With Examples

1 IMPORTANT POINTS-OF-CONTACT
(POC name, phone number, and email)

2 MISSION
(A description of the organization and its mission)

3 ORGANIZATIONAL INFORMATION CRITICALITY
(A representation of the organization's information criticality determined by discussion with the client)

Information Criticality Matrix: This is a sample of the matrix recommended for use within the INFOSEC Assessment Methodology (IAM). Note that it is geared toward ***information*** and not applications. Common mistakes are to list platforms such as Cisco or Windows, applications such as email or office automation tools, and components.

Organizational Information Type	Confidentiality	Integrity	Availability
Personnel	**H**	**M**	**M**
Logistics Control	**H**	**M**	**L**
Fund Accounting	**H**	**L**	**L**
User Manual	**H**	**L**	**L**
Internal Directives	**H**	**L**	**L**
OVERALL HIGHEST RATING:	**H**	**M**	**M**

Value of Importance Definitions: importance factors of High, Medium, and Low are defined below, as related to a paramilitary organization.

High — Mission failure, Loss of life, infringement of personal liberties
Medium — Embarrassment to the Agency/Mission
Low — Inconvenience in performing duties, temporary disruption or Interruption of service

Information Criticality Requirements: the following represents the final value of information criticality, i.e., the highest value of all the information types.

Confidentiality - H
Integrity - M
Availability - M

4 SYSTEMS(S) INFORMATION CRITICALITY

(A representation of the information criticality for each organizational system determined by discussion with the client)

Information Criticality Matrix: This is a sample of the matrix recommended for use within the INFOSEC Assessment Methodology (IAM). Note that it is geared toward ***information*** and not applications. Common mistakes are to list platforms such as Cisco or Windows, applications such as email or office automation tools, and components.

System 1 of 2 Information Type	Confidentiality	Integrity	Availability
Personnel	**H**	**M**	**L**
Logistics Control	**H**	**M**	**L**
OVERALL HIGHEST RATING:	**H**	**M**	**L**

Value of Importance Definitions: importance factors of High, Medium, and Low are defined below, as related to a paramilitary organization.

High — Mission failure, Loss of life, infringement of personal liberties
Medium — Embarrassment to the Agency/Mission
Low — Inconvenience in performing duties, temporary disruption or interruption of service

Information Criticality Requirements: the following represents the final value of information criticality, i.e., the highest value of all the information types.

Confidentiality - H
Integrity - M
Availability - L

System 2 of 2 Information Type	Confidentiality	Integrity	Availability
Fund Accounting	**H**	**L**	**M**
User Manual	**H**	**M**	**L**
Internal Directives	**H**	**L**	**L**
OVERALL HIGHEST RATING:	**H**	**M**	**M**

Value of Importance Definitions: importance factors of High, Medium, and Low are defined below, as related to a paramilitary organization.

High — Mission failure, Loss of life, infringement of personal liberties
Medium — Embarrassment to the Agency/Mission
Low — Inconvenience in performing duties, temporary disruption or interruption of service

Information Criticality Requirements: the following represents the final value of information criticality, i.e., the highest value of all the information types.

Confidentiality - H
Integrity - M
Availability - M

5 CLIENT CONCERNS

(Special considerations, concerns, and/or constraints levied by the client organization)

5.1 Telecommunications
5.2 Firewall Policy
5.3 Identification and Authentication
5.4 Virus Protection

6 SYSTEM CONFIGURATION

(Specific Hardware/Software/Communication connections)

6.1 This is a result of working with the client to map the network using automated tools and physical observation of wiring closets, concentrators, and all connected and standalone equipment.

7 INDIVIDUALS AND POSITIONS TO BE INTERVIEWED

(Position titles and responsibilities of personnel scheduled to be interviewed)

7.1 Positions (titles/roles) for interview by the assessment team:

Applications Programmers
Communications Administrator
Communications Operator
COMSEC Custodian
Configuration Management Personnel
Database Managers
Non-privileged Users
Privileged Users
Security Administrator
Security Maintenance
Systems Administrator
Systems Operators
Systems Programmers
Systems Security Officer

8 DOCUMENTS REVIEWED

(A list of system documents reviewed by the assessment team)

8.1 Examples of documents needed by an assessment team to perform an assessment:

[Organizational information explaining the business/mission of the organization

System Architecture documents explaining the functions, connections, and operations of systems within the organization]

Business Continuity Plan
Concept of Operations (CONOPS)
Configuration Plan
Disaster Recovery Plan
Memorandum of Agreement
Memorandum of Understanding
Recovery and backup procedures
Security Administrator s Manual
Security Concept of Operations (SCONOP)
Security Features User s Guide
Security Policy
Security Test Plans
Service Level Agreements
Standard Operating Procedures (SOPs)
User s Guide
Union/Bargaining Unit Agreements
Vendor documentation
Diagrams of the system to include:
- remote connections
- local area networks
- wide area networks
- gateways
- modems
- network switches/routers
- firewalls
- guards

9 TIME-LINE OF EVENTS

(A sequence of important events and their associated dates. Some events include, the date of the receipt of the request letter, date of a response letter, Pre-assessment, site visits, etc.)

APPENDIX B

INFORMATION SYSTEMS SECURITY ASSESSMENT

OF

ORGANIZATION S NAME
CITY AND STATE WHERE COMPANY IS LOCATED

MONTH AND YEAR

PREPARED BY:

Your Organization's Name and Address Here

THE INFORMATION CONTAINED IN THIS REPORT WAS DERIVED FROM PROPRIETARY DATA PROVIDED BY (the client's ORGANIZATION NAME)

EXECUTIVE SUMMARY

A. Every report must contain an Executive Summary. The Executive Summary should give a brief overview of the assessment and your findings. Basically, the Executive Summary is divided into several paragraphs. The paragraphs contain information on the following:

1. A brief overview of the organization (i.e., what the organization does with their expertise, primary clients, number of people employed, etc.).

2. An explanation as to why an assessment was done (i.e., at organization s request). The dates of the assessment and a statement that the assessment is not an inspection, certification, or risk analysis. The purpose of the assessment and the methodology used to conduct the assessment. You need to also state here that the implementation of any of our recommendations is strictly voluntary on their part and at the discretion of the organization management. The implementation of any recommendations contained herein does not guarantee the elimination of all risks.

3. A brief statement identifying what the system does that was assessed (i.e., command and control system, pay and finance system, etc.). Also include the sensitivity of the information being processed on that system.

4. The major findings and recommendations you found during the assessment. It should be the major areas where the organization needs to improve their security posture. As this is the executive summary, this is not the place to discuss these areas in detail. Findings and Recommendations will be discussed in detail in the INFOSEC Analysis section.

5. The last paragraph closes the Executive Summary. This is also where you thank the organizations personnel that assisted you during the assessment. An acknowledgement of the primary client personnel that assisted in the assessment can be included in this paragraph. Include the team members names and phone numbers should the organization have any questions.

B. The pages of the Executive Summary should be numbered as i, ii, etc. The Executive Summary is the first thing to appear after the cover page of the report.

TABLE OF CONTENTS

Below is an example of a Table of Contents. The Table of Contents should follow the Executive Summary. The basic sections should include an Introduction, a System/mission Description, INFOSEC Analysis, and a Conclusion. This sample Table of Contents also includes some suggested Appendices that you may want to include in your report (i.e., Threat section, Diagrams of their systems). The Table of Contents should be numbered in sequence with the Executive Summary (i.e., iv).

Table of Contents

I. INTRODUCTION

A. The Introduction should include a paragraph which gives the name and location of the organization where the assessment was performed and a discussion about what they do for a living. This is basically the organization s mission and function in life and why they have their systems. The paragraph should also specify the organizations main clients and the number of employees working at the facility.

B. This section should also include a paragraph like what is in the Executive Summary stating why we performed the assessment; the dates of the assessment; and the fact that the assessment was not an inspection, accreditation, certification or risk analysis. The purpose of the assessment, how the assessment team obtained the information (interviews, system demonstrations, etc.), and that through these efforts the team was able to identify security problems and proposed solutions should be in this section as well.

C. The Introduction page is the beginning page for the report and should be numbered as page 1.

II. SYSTEM DESCRIPTION

This section should describe the system being assessed. It should include two types of information; what the system is used for, and the configuration. Most of this information can usually be transferred over from the Assessment Plan.

The first part should include information about the importance of the clients mission, the information criticality, and the system applications and functionality. The various matrixes and value assignments from the Assessment Plan should all be included.

The last section is a complete system description/configuration, including the number of workstations, PCs, etc., the hardware platform, and the software being used on the system. It can also include the number of active accounts and the number of users, if available. The types of features used on the system should also be included (i.e., TCP/IP, TELNET, SMTP, FTP, etc.), as well as what firewalls, if any, are implemented by the company and how they are implemented.

The description should state what connections the company has in place. Also included is brief description of the connection (i.e., 256kb leased carrier line, cisco routers, firewalls, etc.). Is the connection through a organization headquarters or direct? Include a description of the organization s modem connections. The number of modems, types of modems, hours of operation, modem access, I&A requirements, dial-back capability, etc. should all be included in this section.

III. INFOSEC ANALYSIS

The INFOSEC Analysis includes all of the findings from the assessment. Each finding has a corresponding discussion, describing more details about the vulnerability the finding represents, and recommendation, presenting mitigation mechanisms or procedures.

A. **Findings** should be one or two sentences stating the vulnerability.

B. **Discussions** cover details about the existence of a particular problem/vulnerability, why this could be a problem; and what could possibly happen if the problem is allowed to continue. Any solutions to the stated vulnerability that the client had initiated or planned should be included in this section.

C. **Recommendation** statements should be clear and concise. Make sure the recommendations are consistent with your finding. In other words, make sure your recommendation would correct your finding. The recommendation should be what is necessary to mitigate or if possible, completely remove the vulnerability. Sometimes additional recommendations should be given when the removal of the vulnerability is too costly, impractical, or has too high an impact on operations. However, the first and foremost recommendation should be to remove the vulnerability, if possible. This allows whoever is responsible for the operation of the system to make the judgment as to which recommendation to implement.

IV. CONCLUSION

A. This section should state whether or not the INFOSEC posture of the company needs attention. A summary of what the majority of the findings resulted from should also be in this paragraph (i.e., due to lack of documented policies and procedures, employees practices, etc.). You should take this opportunity to state that the organization could improve the security posture by taking into consideration the enclosed recommendations.

B. As security is often thought to be costly and an overhead to an organization, you may want to include some words which state how good information system security saves a company money in the long run.

C. This is where you state again that our recommendations are suggested guidelines, not requirements, to help the company improve its overall security posture. Implementation of any of the recommendations should be at the discretion of the company s management.

D. OPTIONAL: Some positive statements, if any, about what the organization is doing right.

E. This should be the standard point-of-contact paragraph.