SystemEXPERTS

LEADERSHIP IN SECURITY

A Perspective on
Practical Security
2004

National Security Agency (NSA) INFOSEC Assessment Methodology (IAM)

SystemExperts Corporation
Brad C. Johnson

Abstract

Presidential Decision Directive 63 requires, among other things, the National Security Agency (NSA) to perform assessments of United States government (computer and network based) systems. To meet this need, the NSA developed a process known as the INFOSEC Assessment Methodology, or IAM. This process is now being used by both governmental and non governmental organizations.

The goal of an IAM project is to help the target organization improve its INFOSEC posture. The canonical IAM evaluation covers 18 core topic areas (classes).

The evaluation takes place in three phases:

1. Pre-Assessment
2. On-Site
3. Post-Assessment

The NSA is allowing a small set of companies to provide seminars to qualified individuals interested in becoming certified in the IAM process. This paper addresses the basic tenets of the IAM and issues relating to being IAM certified.

Inside

- Understanding the intent of the National Security Agency and the INFOSEC Assessment Methodology
- What are the important tasks in an IAM assessment?
- What are the key concepts underlying IAM assessment?
- What are the primary deliverables from an IAM project?
- How do you become IAM certified?

SystemExperts Corporation

Boston **New York** **Washington D.C** **Tampa**
San Francisco **Los Angeles** **Sacramento**

Toll free (USA only): +1 888 749 9800
From outside USA: +1 978 440 9388

www.systemexperts.com mailto:info@systemexperts.com

Introduction

Presidential Decision Directive 63, which outlines responsibility for protecting United States (US) critical infrastructure, was signed in 1998. It also defines the framework for the National Infrastructure Assurance Plan, which among other things requires the National Security Agency (NSA) to perform assessments of US government systems. To meet this need, the NSA developed a process known as the INFOSEC Assessment Methodology, or IAM. [1] To deal with the enormous volume of target evaluations, the NSA decided to create an IAM training program to "teach" a limited number of organizations how to lead this process. This program was called the INFOSEC Assessment Training and Rating Program, or IATRP.

There are 18 core topic areas (classes) in the canonical IAM evaluation. However, these can be modified "on the fly" to be appropriate for a targeted organization's environment. The evaluation takes place in three phases.

Let us take a closer look at some of the details of the IAM.

What is IAM?

Beyond the acronym, the IAM process is a standard way to evaluate an organization's most critical IT infrastructure asset: its business information. It is a process that was developed from real life experiences, situations, and environments to be used by the NSA in evaluating government IT environments of all sizes. It was not created in the vacuum of a conference room. Put another way, this is a practical "standard."

The IAM is a step forward in security standards and assessments because it is not just a set of definitions and requirements like ISO 17799 or SAS 70. It also is not obviously overwhelming like some of the NIST Security Standards (e.g., 800-60). This is not to downplay those standards; they have their own important roles in the world of security IT and evaluations. The point is that the IAM has many positive attributes that make it valuable for organizations performing security information evaluations.

In addition to describing a standard mandatory set of information types and definitions (see below for more details), it is also a description of how to prepare for an assessment, a process for executing the assessment, and a description of how to document the entire project.

The IAM Process

The IAM process is an assessment, not an audit. That is a critical distinction for the creators of this methodology. The goal of an audit is normally to check for compliance to some standard. If you are checking for compliance, it implies that there will be an articulation of failures and therefore consequences of the failures. Many organizations do not like audits because audits have this inherently black-and-white characteristic: that is, you passed or you failed. To make matters worse, most organizations rush to assign blame for the failures.

The goal of an IAM evaluation is to help the target organization improve its INFOSEC posture. If an audit is required, an IAM evaluation might be the appropriate stepping stone in preparing for such an activity.

In plain and simple terms, the IAM process has three well-defined phases:

1. Pre-Assessment
2. On-Site
3. Post-Assessment

Despite the names that are used for each phase, the fact is, there is a lot of assessing going on in all three phases. They would have been better named with regards to the On-site visit instead of the word "Assessment" (i.e., name them Pre-Onsite, On-site, and Post Onsite).

Pre-Assessment

The purpose of the pre-assessment phase is to understand the realities of the target organization's environment. This includes learning about the mission statement, critical requirements and constraints, and beginning to know the key staff members. It also includes beginning to understand the critical information assets and information systems that are in place.

This is also the stage where scope of the work is determined, necessary documentation is acquired, and many of the practical logistics are worked out.

Before the on-site assessment actually takes place, the assessment team reviews all relevant documentation and performs a preliminary analysis of the information. The formal process of documenting the IAM evaluation also begins at this time.

[1] Please note that a number of the terms used in this white paper are defined by US government directives, the NSA, or the IAM assessment specification and methodology.

On-site Assessment

The on-site activities are quite intensive. This phase can last several weeks and includes interviews, group discussions, and research into policies, procedures, and other INFOSEC related documents. This is also the time that the Information Criticality matrix, Impact Attributes, Impact Definitions, and System Criticality matrices are reviewed and agreed upon with the target organization.

Post-Assessment

Post-assessment is often the longest phase as it includes time-consuming final analysis and documentation. In many situations, the post-assessment will reveal the need for further analysis, research, and consensus-building with the target organization.

What the IAM is not!

It is also important to remember that an IAM evaluation, like any assessment tool or process, has limits. As defined by the NSA, there are four non-goals of this type of INFOSEC assessment.

- Inspection: You do not "show up" and perform an unannounced evaluation. You are willingly invited.
- Evaluation: There is no hands-on testing in the IAM process. If you need that done, that would be handled by an INFOSEC Evaluation Methodology project (IEM).
- Certification: Performing an IAM does not "certify" the target organization.
- Risk Assessment: The focus of this assessment is on vulnerabilities and their impact. There are no quantitative measurements generated, as you would expect to see in a normal risk assessment.

Key Concepts

When performing the evaluation there are two key characteristics of the information that is being reviewed: Impact Attributes and Impact Definitions. There are three common Impact Attributes that are mandatory for any assessment, but keep in mind there is no limit on the number that can be optionally defined and included.

In practical terms, however, the fewer Impact Attributes the better to help keep the work focused on resolution and avoid analysis paralysis. For each of these attributes, at some point you will need to agree on its relative impact to the organization.

The Impact Definitions are also not fixed, and need to be appropriate for the organization being reviewed. In general, though, the default definitions have stood the test of time, critique, and experience and should only be altered if absolutely necessary.

Let us look at the mandatory attributes and definitions.

Impact Attributes

- Confidentiality: Protecting information from unauthorized access.
- Integrity: Safeguarding the accuracy and integrity of information.
- Availability: Having information available when it is needed.

Impact Definitions

The following definitions are not simple conditions and as you will quickly see, they are focused on serious matters.

- High: Huge fines or penalties, loss of life, significant down-time, or significant loss of business.
- Medium: Significant loss of customer confidence, loss of strategic advantage, large fines or impact on business, or emergency medical treatment.
- Low: Upset customers, small fines or impact on business, limited loss of revenue, or potential legal proceedings.

All of these are serious impacts regardless of the definition category. That demonstrates an important aspect of an IAM evaluation. The IAM evaluation is about *critical* information issues, requirements, and attributes. A successful evaluation will not disintegrate into minutia or low-level disagreements. All of the items involved are obviously essential and important to all people at all levels in the target organization.

What the IAM is all About

Of course, all parts of the IAM assessment are important, however, when the dust settles, there are four components that are challenging to create, produce, and define but provide the target organization with the most direct value.

These components include:

1. Information Criticality matrix
2. System Criticality matrices
3. Baseline INFOSEC evaluation areas
4. Technical Assessment Plan (TAP)

Information Criticality

Information Criticality is defined by listing the most important information categories (assets) that drive the success or failure of the organization. In the IAM process, this data is compiled into an Information Criticality matrix. Sometimes, it is easier to explain something by describing what it is not. There are several common difficulties in creating the Information Criticality matrix.

1. Information, not Applications and not Computers: The goal is to define the actual categories of information not the applications that use them (e.g., the email application or the payroll application) nor the computers that the information runs through or resides on (e.g., the mainframe or the central hosts).

2. Mission vs. Support: Remember that we are trying to define the information that supports the success of the organization in performing its core mission. While organizations generate a substantial amount of support information and implement systems and procedures to manager operations, we have to stay singularly focused on information that is absolutely directly related to the success and control of the business or organization.

3. Categories, not Types: At first, it is almost natural to start listing various types of information assets (what would be considered the next level down from categories). The problem is, there tends to be dozens of information types (sub-categories), but really at the heart of it, there are only a few basic information categories.

Okay, so what are good examples of information criticality categories? They might be customer information, human resources data, contracts, network and communications, or corporate finances. You can see that these are meant to be broad information categories and you have to keep in mind they need to be that coarse or you will have serious difficulty in completing the assessment.

System Criticality

System Criticality is defined by identifying what systems directly impact the customer or your organization. At this point, we are talking about computer systems like servers, routers, firewalls, and other key network components. It is necessary to focus on those systems that store and use critical customer information (not just temporarily "holds" it or supports it).

Baseline INFOSEC Classes and Categories

There are three baseline INFOSEC categories and 18 classes within those categories that need to be evaluated as part of a thorough IAM on-site assessment. The categories are:

1. Management: 4 classes (such as contingency planning and configuration management)

2. Technical: 9 classes (such as authentication, session controls, and network connectivity)

3. Operations: 5 classes (such as labeling, physical environment, and education and training)

Technical Assessment Plan

The Technical Assessment Plan, or TAP, is the final deliverable of the entire IAM process. Not only does it include a record of all logistical information (timeline, points of contact), and documents that were reviewed, but more importantly it contains the Information Criticality matrix, the System Criticality matrices, results from the interviews and the baseline assessments and recommendations.

Compliance vs. Certification

In the world of security, as with most areas, words can either add clarity or create confusion. Let us talk about a couple of words that are often used vaguely or without discipline and create confusion: *compliance* and *certification*.

There are security standards (something that you may wish to comply with) and there are security skills (something you may wish to "master" and become certified in).

In general, skills can sometimes be evaluated to determine if the individual (or sometimes a whole organization) is qualified enough to acquire a designation of certification over a particular topic area. For example, you can become certified on aspects of Red Hat Linux administration (RHCE: Red Hat Certified Engineer) or in this case for IAM, you can become certified on general security evaluation methodologies like the one defined by the NSA for performing INFOSEC assessments.

Armed with either a certification or the general needed skills and background, you can then perform an analysis of some particular area against a well-defined set of requirements – that is, to determine if it is in compliance with those stated requirements. Sometimes these requirements have been defined by an over-arching organization like a standards body and sometimes these are defined locally by your own organization.

No Easy Answers

In some situations, an assessment can be performed by qualified individuals or ones that also happen to have a certain certification. In other situations, an assessment *must* be performed by somebody with the appropriate certification designation.

In either case, it is often difficult to choose the right people to do this work. Look for firms that are adept at grounding their technical assessments in underlying business needs, that are knowledgeable about your regulatory environment, and are genuine experts in the networking and computer technologies you use.

IAM Certification

It is important to note that only individuals are certified, not whole organizations or companies.

IAM Certification Process

The individual must first register with an approved testing organization. After the registration, one will receive an IAM eligibility packet that must be completed and sent back to the testing organization. An important part of this eligibility packet is a description (resume) of the students' background, with a particular focus on security positions, experiences, and responsibilities. The testing organization, in cooperation with NSA requirements and procedures, reviews this submission which includes basic background review material. If the submission is accepted (which for a qualified individual, may be the most critical part of the acceptance process), the student is allowed to sign up for the intensive two-day seminar. This seminar is very interactive and requires the participants to be actively involved in individual and group activities. At the conclusion of the seminar, you must pass a written test in order to become certified.

IAM Certification Requirements

The basic requirements that must be met before an individual will even be considered for the seminar are as follows:

- United States citizenship
- 5 years of IAM related security experience
- 2 years of INFOSEC related experience
- Pass NSA basic background check requirements

Resources

The starting point for doing your own research on IAM needs to include two critical organizations; the NSA and IAM.

Look here for an overview of the IAM training and rating program as originally defined by the NSA:

http://www.nsa.gov/releases/relea00038.cfm

Look here at the IAM home page which includes a list of all IAM certified individuals as well as a list of those companies that are approved to sponsor an IAM certification class:

http://www.iatrp.com/iam.cfm

Remember that IAM certification is only awarded to specific individuals. You will need to look for the specific names of people who have been certified. This search capability is not overly robust so ensure that you have looked appropriately for the named individuals! As of this time, the individuals from SystemExperts (Brad Johnson and Jason Reed) who are certified received their certifications on "03/29/04".

SystemEXPERTS
LEADERSHIP IN SECURITY

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and Windows security at USENIX, Networld-Interop, CSI, and InternetWorld are among the highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio. Every single full-time staff member is certified in some critical security area.

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients. *www.systemexperts.com/services.html*

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. We can perform "White Hat" penetration testing, web application vulnerability assessments, dial exposure ("war-dialing") reviews, firewall analysis, host hardening analysis, IP services inventorying, wireless LAN inventory, VPN assessments, and denial of service reviews to name some of the more frequent testing we do.

Security Blanket, Emergency Response & Incident Response "Scrimmage"

It is not a question of *if* your organization will be the target of a hacker; it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment. We can also help you prepare for these inevitable events by practicing your response through our acclaimed Incident Response "Scrimmage" Training Exercise.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest intrusion, firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in Windows, UNIX, and other heterogeneous environments. We also provide interim staffing up to the CISO level.

Interactive Security Workshops & Code Reviews

Using a highly interactive workshop style methodology, our consultants will work with your team to perform a quick but comprehensive review of the security of applications or systems in their full environmental and business context and help you to understand and apply industry best practices. You may use this as the jumping off point for planning and prioritizing security initiatives. Our clients value this Workshop approach because of the knowledge transfer that occurs – the discussions make their team better.

SystemExperts uses this Workshop methodology in a wide range of services including overall security architecture reviews, design reviews, compliance reviews such as CISP or ISO 17799 assessments, Application Service Provider (ASP) reviews, PeopleSoft security reviews, and security code reviews. In the case of code reviews, we perform the detailed analysis of security-critical code modules after completion of the on-site interactive assessment of the application's architecture.

Security Policy, Best Practices, & Strategy

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice. Over the past ten years, we have assisted some of the largest financial institutions in the world in developing overall security architectures.

Intrusion Detection & Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 888.749.9800

Boston Los Angeles New York San Francisco Tampa Washington DC Sacramento

www.SystemExperts.com info@SystemExperts.com