

# The National Security Agency's IAM Assessment Reviewing Your IT Information Assets

## ***Executive Insight Series***

*by Brad C. Johnson*

---

### **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.<sup>1</sup>

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

---

<sup>1</sup> 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.

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."

In addition to describing a standard mandatory set of information types and definitions, 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. 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

#### **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.

Before the on-site assessment actually takes place, the assessment team reviews all relevant documentation and performs a preliminary analysis of the information.

#### **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 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.

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.

## **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 student's 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

## 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, Network-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](http://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](http://www.SystemExperts.com)

[info@SystemExperts.com](mailto:info@SystemExperts.com)