Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Building an Information Assurance Framework for a Small Defense Agency

As information security continues to capture headlines in our daily lives, it is imperative that businesses have an Information Assurance Framework - a solid plan of action with the required tools, trained personnel, and tested procedures - that is capable of protecting valuable information assets. However, many organizations with low risk data have not focused on information security and have not put adequate life-cycle controls in place to ensure continuous protection. That is the case at our small defense agency. Th...

Copyright SANS Institute

Author Retains Full Rights

AD

Building an Information Assurance Framework for a Small Defense Agency

Janet Haase
GSEC 1.3
April 8, 2002

ABSTRACT

[As information security continues to capture headlines in our daily lives, it is imperative that businesses have an Information Assurance Framework – a solid plan of action with the required tools, trained personnel, and tested procedures – that is capable of protecting valuable information assets. However, many organizations with low risk data have not focused on information security and have not put adequate life-cycle controls in place to ensure continuous protection. That is the case at our small defense agency. This paper attempts to glean best practices from many sources to define the steps we must to take to implement and manage an Information Assurance Framework.]

President Bush's budget proposal for fiscal year 2003 allows an 8% increase in IT spending as compared to 2% for other spending. That sends a strong statement that IT is a critical asset to the government. With each new technology, each new system, each new user, and each new day, protection of those assets becomes increasingly important. "Awareness, planning, layers of defense and plenty of redundancy – all are necessary to secure information and keep systems operating" (Miller, 2002). Government agencies and private business that had already put those strategies to work, fared much better after the events of September 11. What an awakening! Assuredly, those business managers that had funded information security from the ground up, were glad they did.

But what about smaller agencies that were not directly affected? Agencies that operate with low risk data? Management that has not embraced the criticality of information assurance? Therein lies the challenge – how to build an Information Assurance Program, a framework that will effectively protect the common Defense network environment while not imposing undue burden on an agency that is downsizing and budget cutting annually.

Recent legislation and DoD guidance define the requirements. The Government Information Security Reform Act is requiring action. The new Draft DoD Information Assurance Policy and Instruction are capstone documents to be used for building an Information Assurance Program that is documented and measurable, specifically referred to as DoDD 8500.aa and DoDI 8500.bb. The widely accepted approach to Defense in Depth has established a methodology for addressing network and information security concerns. Using these guidelines and requirements, coupled with currently available information, we can design a framework that will support any organization and tailor it to fit our individual business needs.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

We will use the three Defense in Depth categories as the pillars of our framework, People, Operations and Technology. The first challenge is to build an overarching policy that explains who and what is involved. Then we will define additional specific use policies. However, for these documents to really be effective for our organization, the key will be defining the operational procedures for each policy. These procedures will give clear and concise guidance on how to apply the policy in our environment, with our technology. Our IA program will use the Defense Information Technology Certification and Accreditation Process (DITSCAP) as the umbrella. This program prescribes all the steps required to assess, assign, implement, and audit the information security environment.

Let's summarize the Defense in Depth categories, so we can identify what needs to be considered as we move forward. We need to consider PEOPLE. Both people who use technologies to conduct operations and people as resources that design, build, install, operate, evaluate, and maintain the protection environment. Requirements will include: evaluate and define the IA-related curriculum for systems administrators, information security officers and information security managers; establish programs to train and certify these key security resources; and establish an awareness program for the general workforce. These programs must be supported by management and must be adhered to across the board.

Additional PEOPLE issues include recruitment and retention of security resources. As we observed during the dot com boom, technical resources are scarce. Those who can be trusted with our most in-depth system and network secrets need to be retained and rewarded for their skills and their credibility. We must establish incentives and initiatives to improve that process. A key requirement in initially establishing trustworthiness is through appropriate background checks, security clearances and clearly defined in and out processing procedures. It is imperative that we create policy and requirements for implementing these programs.

The next category is OPERATIONS. OPERATIONS include the establishment of goals, actions, procedures, and standards that are driven by clear and concise policy documents. Much of this paper will refer to the establishment of an overarching policy and issue-specific policies and procedures. These documents and standards must be easily accessible and reviewed regularly for updates as well as being monitored for compliance with DoD and Federal policies and law. Sustaining security capabilities used by systems and networks may include the implementation of DoD wide requirements such as Public Key Infrastructure, secure network operations, electronic key management and distribution, and vulnerability alert compliance. We will begin evaluating these capabilities and will create plans for assessing the value and incorporating them into our environment.

The OPERATIONS category also includes the requirements and standards for ensuring defensive measures are in place and being used. These actions might include

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

readiness assessments and audits, threat and vulnerability assessments, and ensuring the cornerstone principles of confidentiality, availability and integrity are defined and operational.

The third category is TECHNOLOGY. TECHNOLOGY programs employ a strong arsenal of essential security tools and skills, many of which were taught in the SANS Security Essentials Course. Technology perspectives are broken down into five key areas as defined in many DoD documents. These perspectives are summarized as follows:

Defend the Networks and Infrastructures – addresses the availability, confidentially, and management requirements of large networks, to include cryptographic equipment, wireless security capabilities, intrusion detection at network level and VPNs.

Defend the Enclave Boundary – addresses perimeter defense mechanisms such as firewalls and guards, intrusion detection at enclave level, vulnerability scanners, virus detection at enclave level and multi-level security tools.

Defend the computing environment – addresses security measures for workstations, servers, applications and operating systems. Measures would include encrypted email, file protection, secure web browsing, virus detection for workstations, Public Key enabling of applications, smart cards, biometrics, and other system specific security measures for key business systems.

Supporting infrastructures – include those DoD/government/agency level programs that can be shared to ensure a more secure operating environment for all. This includes global directory services, PKI infrastructure, joint analysis and coordination of handling incidents and sharing information on virus and hacker attacks.

Last, but not least is our System Security Methodology or Framework. This addresses the Information Assurance Life Cycle approach to how we intend to manage and reduce our security risks. In today's internetworked environment, where more and more business is taking place, firewalls and intrusion detection systems are not enough to ensure continual protection. "In order to adapt as new technologies and new opportunities impose changing demands on the network infrastructure, security management must become a closed-loop cycle of continuous security improvement" (Internet Security Systems, 2000).

The best example would be the DITSCAP umbrella methodology that includes everything from risk assessment and management issues, to complete certification and accreditation of all systems and the network. How do we implement and ingrain the DITSCAP philosophy into an organization that has not recognized the importance of certifying and accrediting its systems? We have defined the pillars of our framework and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the categories for our architecture, but we must determine what all this will mean to our business.

In order that the Information Assurance program is effective, it must become an integral part of our agency's overall business strategy. When security management is accepted as a core business operation, it necessitates the development of guidelines and creates the security practices necessary to support the business strategy. The guidelines become the overarching security policy that in turn drives the development of an overall security management architecture (Internet Security Systems, 2000).

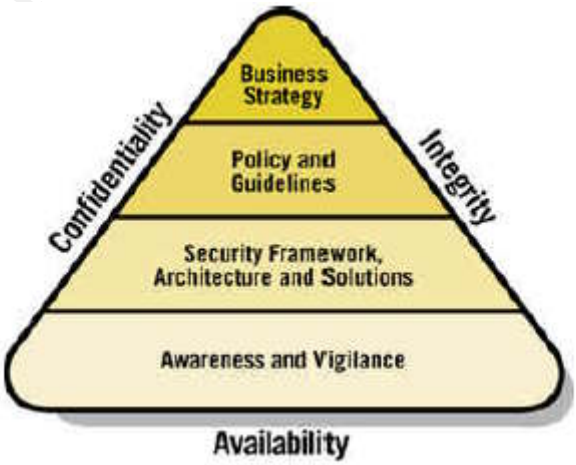
The fundamental principles of information security are: Confidentiality, Availability, and Integrity. We must look at each of these principles and relate them to our strategic business objectives. What do the principles mean?

- Confidentiality - The capability to protect corporate data from unauthorized access.

- Availability – The capability to provide access to network resources and data despite disruptive events or conditions.

- Integrity – The capability to provide services and process data with the assurance that it is accurate and uncorrupted.

The following diagram from Internet Security Systems, depicts the relationships between the principles and the building blocks. Basically, in terms of the Defense in Depth categories or pillars, Awareness and Vigilance represent PEOPLE, Security Framework, Architecture and Solutions represent TECHNOLOGY, and Policy and Guidelines represent OPERATIONS. The key is the top of the triangle, which requires us to relate the Business Strategy, our strategic goals and initiatives, back to the prevailing requirements of Confidentiality, Integrity, and Availability.



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

This sounds simple, but do we really know what information resides on our networks, where it is located, who has access to that information and the cost of compromise to any given set of data? Do we know what business risks are present in our organization? We can assess our security needs by asking questions for each of the fundamental principles.

Although most of our agency data is low-risk and confidentiality is not a major requirement, we must still consider our personnel data (social security numbers), our customer data (social security numbers, credit/debit card numbers), and our financial data. To determine confidentially issues:

- What employee data is considered confidential, grade, salary, background investigations, performance reviews?
- What customer data could be compromised?
- What data are we legally required to keep private (lawsuits, contract information, privacy data)?
- Where is this various data stored? Which systems, databases?
- Would it have a negative impact on the agency if this data were revealed to unauthorized users?
- What data, if available to hackers on the Internet, would open us up to attack (network diagrams and configurations, DNS tables, personnel directory)?
- How is the confidentially of this data protected?
- What data, if available to a disgruntled employee or contractor, would open us up to attack (root passwords, combinations to cabinets with back-up tapes)?

Although high availability is not critical for our business to operate, we must consider the impact on our employees and our business partners if our data is unavailable for any reason. To determine availability issues:

- What is the impact on employee productivity if the network was down for an hour, a day, or a week?
- Is our business hurt if we aren't able to interact with our business partners for an hour, a day, or a week?
- What is the impact if we are unable to conduct key business functions, such as contracting, ordering, receiving, pricing, or bill paying without network availability for a day?
- Would our image be tarnished if our Web site were unavailable for a day, a week?
- How much money in salaries would be lost if we were without the network for a day?
- Do we have contingency plans to restore network and computer operations?

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Integrity may be the most difficult to measure in a quantitative sense, but it is key to understand its impact on our business operations. Our relationships with our business partners, our government partners, our customers and our employees will be seriously affected if our data is not accurate. To help determine possible integrity issues:

- How would we be affected if our data were corrupted?
- If we posted incorrect prices for goods?
- If we transmitted incorrect voucher amounts for paying our vendors?
- If we ordered inaccurate quantities of goods?
- If top-level management email accounts were corrupted?
- Would our business partners lose trust in us?
- Would our customers lose faith in us?
- What happens if our Firewall, Intrusion Detection Systems or other devices that implement and monitor security become corrupted?
- How do we determine the level of corruption and go about correcting it?

We must be prepared to relate our business strategic objectives to these fundamental principles. In order to do this, we will have to perform an informal risk analysis. To assess risks, we must identify our vulnerabilities and the threats that can exploit those vulnerabilities. We must first identify what we have. We will begin by identifying all network devices, applications, services, and data on the network. Then we will identify who has access and at which level. As we document each resource and who has access, vulnerabilities and threats should automatically be revealed. Once the threats and vulnerabilities have been identified, we can begin to determine the risks associated with the threat/vulnerability pairs (Gryparis, 2001):

Impact: The degree of damage that could be done
Probability: The likelihood that a vulnerability could be exploited by a threat

We will need to measure in qualitative terms, the assessment of the probabilities, and the impacts that will yield the level of risk. The results of this effort will be our risk assessment document. The risks must be defined from a business point of view and stated in terms of dollars. Management must determine which risks are acceptable to them and which are not. Once they understand the risks, they must support the dollars and resources required to mitigate the unacceptable ones. This will provide for the foundation of a solid information assurance program.

We are now ready to write our overarching Information Assurance Policy. This document will become our capstone security document. The policy must (Rowland, 2001):

- Describe the purpose or WHAT must be done and adhered to well enough that the HOW can be identified, measured, and evaluated.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Be clear, concise, and realistic
- Be consistent with higher level policy
- Protect the agency's information
- Protect the people who use and administer Information Technology by empowering them to do the right thing
- Be well-publicized and easily accessible to all agency personnel

We must identify all issue-specific polices and the procedures required by our organization. Most likely these would include the following:

- Password Management
- Virus Protection and Prevention
- Network Connection
- Incident Handling
- Acceptable Use
- User Access
- Data Backup and Off-Site Storage
- Remote Access Policy
- Firewall Policy
- PKI Policy

In accordance with department guidelines, each of these policies will follow a consistent and standard format, as summarized below.

1. Purpose – a brief statement explaining the purpose of the policy, what it is.
2. Applicability and Scope – a brief statement of who this policy applies to, for example: all systems users in the organization, or all systems administrators.
3. Policy – In a high level and summary format, states the policy for each area covered, for example: "All DoD information systems, services and applications shall comply with established DoD ports and protocols guidance and management processes" (Draft DoDD, 2002)
4. Responsibilities – Lists each responsible party and what their role is in applying and implementing the policy.
5. Procedures – This is where actual procedures for implementing the policy are found. If the procedures are lengthy in nature, they will be stated as an enclosure or appendix to the policy document.
6. Effective Date – States the effective date of the policy, which is usually immediately.

Once the policies are published, we will have to establish our plan for compliance audits and management reviews. Using the DITSCAP process as our guidelines, we have designed the following management review cycle and will attempt to establish it in our agency in the future:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Review Cycle for Managers		Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Risk Management Review	monthly												
Roles and Responsibilities Review	Q1												
Personnel Security Requirements	Q1												
Certification Requirements Review (CRR)	Q1												
Minimal Security Activity Checklist	Q2												
Configuration Management	Q2												
Ports, Protocols, and Services	Q2												
Security CONOPS	Q3												
Self Assessments (audit/vulner. testing)	Q3												
DR / COOP Plans	Q3												
Incident Response Plan	Q4												
Security Education/Training/Awareness	Q4												
HQ-DeCA Sys Security Policy (35-31)	Q4												
Site Accreditation Review	Q2												
The Complete SSAA													

The following bullets summarize what has been presented and accomplished in this document:

- Identified the high-level IA requirements that are mandated for us to follow
- Identified the Defense in Depth categories that become the "pillars" of our framework
- Listed requirements for our program that will be the building blocks that support each pillar
- Identified our methodology for a security life-cycle approach – DITSCAP
- Identified the necessary steps to build our business case
- Related the fundamental information security principles of Confidentiality, Availability and Integrity back to our business concerns
- Identified the need for a complete risk assessment that will quantify the need for the 3 principles
- Realized the importance of an over-arching Information Assurance policy
- Identified specific-use policies required by our agency
- Identified the need for sound technical guidance and procedures
- Developed a review cycle calendar for use by management

The management review process will provide the closed-loop cycle of continuous security improvement that is imperative in today's networked world. We have now

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

identified the methodology and framework that need to be implemented. We have progressed through the key elements of our Information Assurance Program and what we need to do to begin the arduous process of making it a reality. Understanding, that this will not happen overnight, but will build over time with the awareness of all employees and the support of management.

© SANS Institute 2002, Author retains full rights.

Resource List

1. Miller, Jason. "Bush Bumps IT Budget by 8%", Government Computer News, February 18, 2002, pgs 1, 12-13.
2. "Creating, Implementing and Managing the Information Security Lifecycle, Security Policy, E-business and You". Internet Security Systems (white paper), 2000.
3. Gryparis, Mark. "How to Bootstrap Information Security in Your Organization". Online May 30, 2001. http://rr.sans.org/start/bootstrap.php
4. Rowland, Carolyn. "Selling Security to Management in a Low-Risk Environment". Online. April 21, 2001. http://rr.sans.org/start/selling_sec.php
5. Memory, Bev. "Security Awareness – Everyone's Business". Online. April 18, 2001. http://rr.sans.org/start/everyone.php
6. Roberti, Michael. "Building an Enterprise Security Architecture". Online. April 4, 2001. http://rr.sans.org/policy/sec_arch.php
7. Dulany, Kevin M. "Security, It's Not Just Technical". Online. January 15, 2002. http://rr.sans.org/policy/tech.php
8. Draft Department of Defense Directive, "Information Assurance (IA)", Number 8500.aa, February 1, 2002.
9. Draft Department of Defense Instruction, "Information Assurance (IA) Implementation, Number 8500.bb, February 1, 2002.
10. Pillar, Charles. "U.S. to Curb Computer Access by Foreigners", Los Angeles Times (latimes.com), March 7, 2002. http://www.latimes.com/news/nationworld/nation/la-030702ban.story

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 3rd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced