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.

A Guide to Government Security Mandates

To reverse a trend of weak security in government computer systems, Congress has passed legislation that requires federal agencies to more effectively manage the security of its IT systems. A fundamental component of this improved security management is System Certification. System Certification provides a holistic view of the state of security for each system by identifying the risks associated with the system, identifying the countermeasures implemented to mitigate those risks, explaining how security is implemented,...

Copyright SANS Institute
Author Retains Full Rights

AD

Government System Certification

A Guide to Government Security Mandates

Christian Enloe
GIAC Security Essentials Certification (GSEC)
Tyson's Corner, VA (December 2002)
Practical Assignment Version 1.4b, Option 1

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ABSTRACT **3**
INTRODUCTION **4**
GOVERNMENT SECURITY REQUIREMENTS 4
CERTIFICATION & ACCREDITATION **5**
DEFINING SYSTEM BOUNDARIES 5
RISK ASSESSMENTS 6
SELF-ASSESSMENTS 7
Level Definitions *9*
How To Answer the Self Assessment Questions *10*
SYSTEM SECURITY PLANS 11
System Owner *11*
Secondary Point of Contact (POC) *11*
Business Function of the System *11*
System Interconnections *12*
Information Sensitivity *12*
Self-Assessment Control Areas *12*
CONTINGENCY PLANS 13
Business Impact Analysis (BIA) *13*
Recovery Steps *14*
PLAN OF ACTION & MILESTONES 15
CONCLUSION **17**
LESSONS LEARNED **18**
REFERENCES **20**

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

To reverse a trend of weak security in government computer systems, Congress has passed legislation that requires federal agencies to more effectively manage the security of its IT systems. A fundamental component of this improved security management is System Certification. System Certification provides a holistic view of the state of security for each system by identifying the risks associated with the system, identifying the countermeasures implemented to mitigate those risks, explaining how security is implemented, planning for system downtimes and emergencies, and providing a formal plan to improve the security in any one of these areas.

This document identifies each major component of the System Certification process and provides an overview of each. This document endeavors to provide the reader with a solid understanding of the certification process, the order in which the steps should be completed, and some lessens learned from actual experience.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction

On July 28, 2000, the United States General Accounting Office (GAO) requested that the Subcommittee on Government Management, Information and Technology summarize the results of recent information security audits at federal agencies. The report by Subcommittee Chairman Stephen Horn, dated September 6, 2000, summarized information security weaknesses identified in audit reports issued from July 1999 through August 2000. In the report, he states "evaluations of computer security published since July 1999 continue to show that federal computer security is fraught with weaknesses and that, as a result, critical operations and assets continue to be at risk." [1]

To combat this trend of security weakness in the midst of ever increasing computer interconnectivity and reliance on electronic data, the President signed into law the Government Information Security Reform Act (GISRA), P.L. 106-398, Title X, Subtitle G, on 10/30/2000 as part of the Defense Authorization Act of 2001. [2] GISRA requires agencies to better manage their security and document their progress through a self-assessment and an independent review by the Inspector General (IG).[3] Although GISRA expired on November 29, 2002, Federal Information Security Management Act (FISMA) was enacted as part of the Homeland Security Bill. FISMA permanently extends the IT Security requirements of GISRA.

Government Security Requirements

FISMA was created to ensure proper management and security for the information resources supporting Federal operations and assets. It is particularly important as we move towards a more effective electronic government. FISMA covers programs for both unclassified systems and national security systems. The requirements outlined in this document are for the protection of unclassified systems. Many new agency responsibilities were outlined in GISRA, such as the following:

- Agency-wide Security Program
- Incident Response Capability
- Annual Program Review
- Reporting Significant Deficiencies
- Annual Agency Performance Plan.

[1] General Accounting Office – http://www.gao.gov/new.items/ai00295.pdf
[2] General Services Association – http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/legupdate4.doc
[3] Federal Computer Week - http://www.fcw.com/fcw/articles/2001/1210/web-gisra-12-13-01.asp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Certification & Accreditation

An integral component in the effort to comply with government requirements concerning the above areas is Certification and Accreditation (C&A) of government systems. *Certification* refers to "a judgment of the IT system's compliance with stated security requirements", while *Accreditation* is the "authorization of an IT system to process, store, or transmit information, granted by a management official," according to the NIST Draft Publication 800-37 "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems".[4] The *Certifier* is usually the System Owner, while the *Accreditor* may be the Chief Information Officer and/or other high-ranking officials. Annual C&A provides the information and data necessary for compiling annual program reviews, reporting significant deficiencies, and for the annual agency performance plans. [5] Due to length requirements, this document will focus on the requirements for successful system reviews. These requirements are as follows:

- Defining System Boundaries
- Risk Assessments
- Self-Assessments
- System Security Plans
- Contingency Plans
- Plan of Action and Milestones (POA&M)

The following sections will focus on each of these critical steps in detail.

Defining System Boundaries

A system cannot be assessed and certified without first determining where its boundaries and interfaces with other systems are. This requires an analysis of both technical boundaries and organizational responsibilities. Constructing physical and logical boundaries around a set of processes, communications, storage, and related components, identifies a system. An SSP is required for each set of elements within these boundaries that constitute a single system. As a general rule, systems have one or more of these characteristics:

- Be under the same direct management control
- Have the same general business function(s) or business objective(s)
- Have essentially the same security needs

All components of a system do not need to be physically connected. For example, a system may consist of a group of stand-alone PC's in an office, or multiple configurations installed in locations with the same environmental and physical safeguards. Both scenarios describe very different, but valid systems.[6]

[4] NIST Draft Publication 800-37 - http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf
[5] White House - http://www.whitehouse.gov/omb/memoranda/m01-08.pdf
[6] Dept. Health & Human Services - http://www.cms.hhs.gov/it/security/docs/ssp_meth.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Risk Assessments

"Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."[7] A Risk Assessment is used to identify elements within the environment that may be subject to threats that could compromise the confidentiality, integrity and availability of information assets. A security Risk Assessment is based upon the value of an organization's assets. The Risk Assessment consists of asset identification, threats identification, vulnerability identification and/or assessment, risk definition and prioritization, and countermeasures identification that mitigate the identified vulnerabilities.

A Risk Assessment answers the following questions:

- What am I trying to protect? - This step identifies valued assets.
- What do I need to protect against? - This measures threats and vulnerabilities.
- What is the likelihood that a threat will be materialized? – This measures risk.
- What is the cost of protection (time and money)? This determines the appropriate types of countermeasures.

The paragraphs below explain the major terms associated with risk assessments: assets, threat, vulnerability, risk, and countermeasures:

Information assets include information, as well as the people and technology that support information processes. These assets can be grouped by type of data, application, technology component, people or intangibles, such as company reputation. One of the goals of the asset identification should be to develop a correspondence between information assets and the technologies (servers, software and processes) that manage, store, process, and transport these assets.

A threat is any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service. A threat can be caused by environmental conditions, such as a flood or failed utility or by human behavior, either accidental or intentional.

A vulnerability is a weakness in system security policy, procedure, management, system design, implementation, or internal controls that can be exploited. For example, a database located outside of a firewall with a null password is a vulnerability that might be exploited by the threat of a hacker. Similarly, servers located under leaky pipes are vulnerable to the threat of water damage.

A risk is the probability that a particular threat will exploit a particular vulnerability of a system. Assessing the risk includes determining how valuable that asset is to the organization, the damage it would cause if it would occur, and the likelihood of that threat occurring.

[7] NIST SP800-30 - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Risk can be reduced by implementing countermeasures. Countermeasures are controls that either decrease the likelihood of threat occurrence, or diminish its impact. Countermeasures can be in many forms, including effective policies and procedures and the installation of software tools and updates. It is important to ensure that these controls are properly enabled and that service packs and/or patches are up-to-date.

In summary, security risks are based on the likelihood that your system will be targeted by a specific threat. By taking into account the likelihood of identified events, risks can be defined, and as likelihood and impact increases, risks increase.

Self-Assessments

While Risk Assessments identify the appropriate risks for an organization or agency and helps to determine what kinds of countermeasures are appropriate to mitigate the organization's risk, Self-Assessments act as a report card for how well an organization is managing the security of each system; or more specifically, how each risk is being managed. How well the risks are being managed is identified by what countermeasures (or controls) are implemented.

Office of Management & Budget (OMB) recommends system owners use NIST's Special Publication 800-26 "Security Self-Assessment Guide for Information Technology Systems" to perform annual system self-assessments. The special publication "is a how-to guide that complements the CIO Council's Federal IT Security Assessment Framework. The council developed the framework to help agencies determine where, within six levels of effectiveness, their security programs fall and what areas can be improved. "[8]

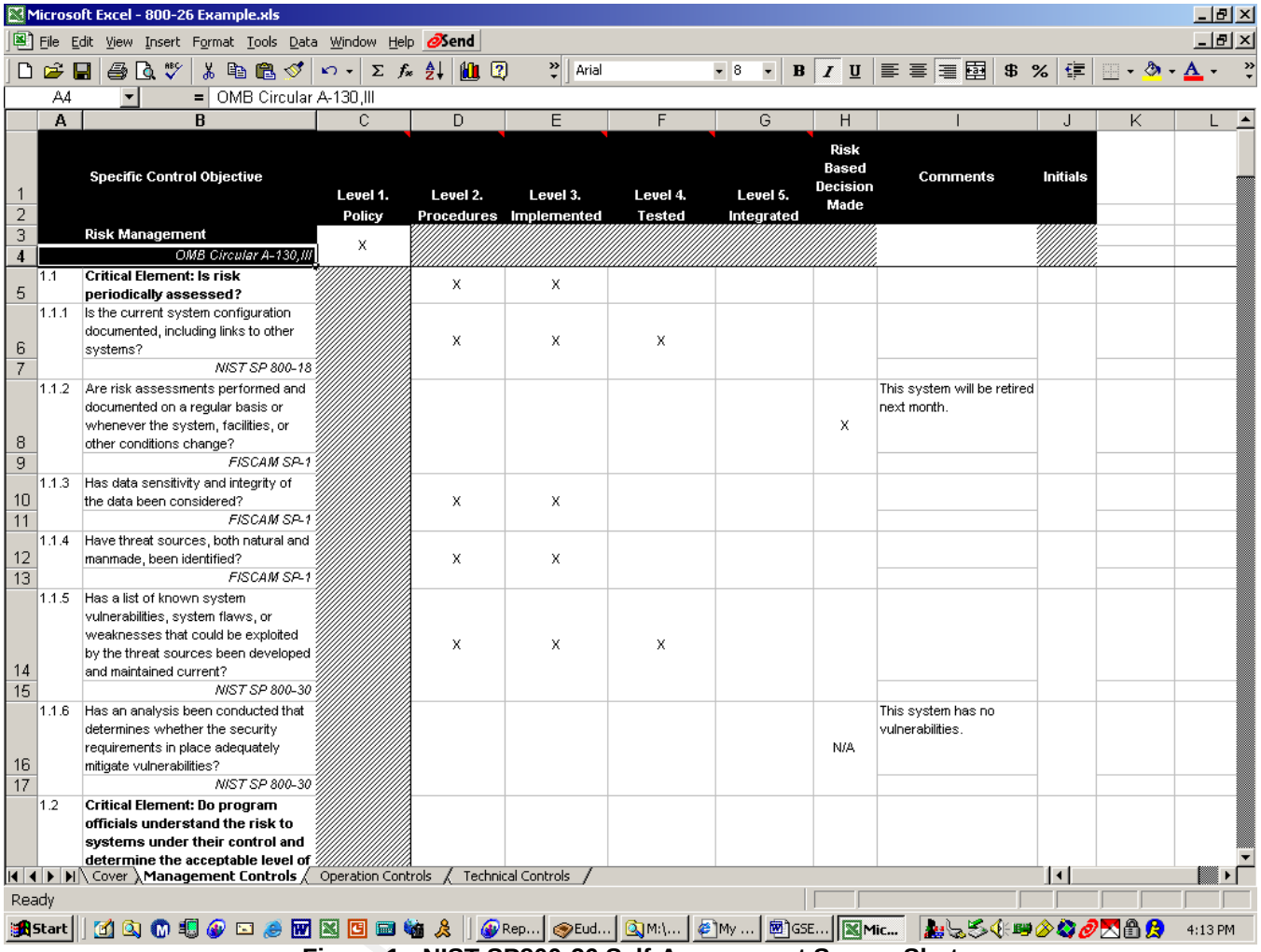
There are a total of 17 control areas (or topics) contained in the questionnaire; each topic contains critical elements (summary questions) and supporting security control objectives and techniques (supporting questions) about the system. All topics are grouped within three major categories, Management, Operational, and Technical.[9] The 17 control areas are as follows:

- Risk Management
- Review of Security Controls
- Systems Development Life Cycle
- Authorized Processing
- System Security Planning
- Personnel Security
- Physical and Environmental Protection
- Production, Input/ Output Controls
- Contingency Planning
- Hardware and System Software Maintenance
- Data Integrity
- Documentation
- Security Awareness, Training and Education
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails

[8] FWC.com - http://www.fcw.com/fcw/articles/2001/0917/pol-guide-09-17-01.asp
[9] NIST SP800-26 - http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The assessor must read each control objective and technique question and determine whether the system's sensitivity level warrants the implementation of the control stated in the question. To understand further, view the Self-Assessment screen shot (Figure 1) and the six levels are defined in the following section.



	Specific Control Objective	Level 1. Policy	Level 2. Procedures	Level 3. Implemented	Level 4. Tested	Level 5. Integrated	Risk Based Decision Made	Comments	Initials
	Risk Management *OMB Circular A-130,III*	X							
1.1	**Critical Element: Is risk periodically assessed?**		X	X					
1.1.1	Is the current system configuration documented, including links to other systems? *NIST SP 800-18*		X	X	X				
1.1.2	Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*						X	This system will be retired next month.	
1.1.3	Has data sensitivity and integrity of the data been considered? *FISCAM SP-1*		X	X					
1.1.4	Have threat sources, both natural and manmade, been identified? *FISCAM SP-1*		X	X					
1.1.5	Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? *NIST SP 800-30*		X	X	X				
1.1.6	Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? *NIST SP 800-30*						N/A	This system has no vulnerabilities.	
1.2	**Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of**								

Figure 1 - NIST SP800-26 Self-Assessment Screen Shot

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Level Definitions

The Self-Assessment questions are to be answered according to which level applies to them (Refer to Figure 1 for a visual representation). There are six levels, which are described below:

- Level 1 (Policy) – This box can be checked if a security policy exists regarding the control.

- Level 2 (Procedures) – If Level 1 is checked AND procedures, based on the guidelines outlined in the policy, have been documented, then Level 2 can be checked. The procedures must be stored in a central location (file cabinet or shared directory) and available for all appropriate system personnel. It is not sufficient to have informal processes that are performed, but not documented. Procedures must be documented and available upon request.

- Level 3 (Implemented) – If Level 1 and 2 are checked AND the documented procedures are actually being followed, Level 3 can be checked.

- Level 4 (Tested) – If all previous levels are checked AND the procedures are periodically reviewed, evaluated, or tested to ensure they are current and complete, Level 4 may be checked. It can also mean that a specific control measure or software is actually tested.

- Level 5 (Integrated) – Level 5 can be checked only if all of the above criteria are met and the security measures are fully integrated into a comprehensive program.

- Risk-Based Decision - A risk-based decision can be made if the sensitivity of the system does not warrant implementation of the recommended control. An example is that integrity verification software is not required for a desktop system with low Confidentiality and Integrity ratings. In this case, implementation of the integrity verification software (Tripwire) would not be consistent with the identified risks. It would be overkill so a risk-based decision would be made not to implement that control in this situation.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

How To Answer the Self Assessment Questions

Some guidelines to follow when conducting a Self-Assessment are as follows. The SP800-26 Questionnaire is not intuitive and learning how to answer each question is half the battle. Following these instructions will help an assessor fill out the Self-Assessment questionnaire successfully.

1. There are three possible responses to each question, they are:

   A) "*I need and have this"* – mark an 'X' in the box for each appropriate level.

   B) "*I don't have this, but I need it*" (such as documented procedures or implementation of a process) – do not mark an 'X' in the box, but write in the comments box how and when you are going to comply.

   C) "*I don't need this for any of the following reasons:"*

   - It simply does not apply - write 'N/A' in the Risk Based Decision Box and write comments explaining why it is not applicable
   - It applies, but is not required for my situation - mark the risk-based decision box with an 'X' and write comments as to why you will not implement it.
   - It applies, but another group takes care of this - mark the risk-based decision box with an 'X' and write comments as to why you will not implement it.

2. Columns must be checked in order. For example, level 3 columns may only be checked when level 2 columns are also checked. This ensures that documented procedures exist for each security measure performed.
3. Before the critical element boxes (bolded questions) can be checked, each supporting question should be checked. If one supporting question is not checked, (answered as "B" above) then the critical element cannot be checked.
4. When the risk-based decision field is checked, note the reason in the comment field and have the system owner review and initial each risk-based decision. Additionally, the system security plan for the system should contain supporting documentation as to why the control has or has not been implemented.
5. At the end of each set of questions, there is an area provided for notes. This area may be used to document the justification as to why a control objective is not being implemented.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

System Security Plans

The next step in the process is the System Security Plan (SSP). The SSP ultimately becomes the central system security document, describing the system's attributes and security profile in detail, but unlike many of the other components, in text form. The main value of the SSP is that, if done correctly, it explains not just what controls are and need to be in place to secure the system, but HOW each applicable control item in the SP800-26 is implemented. NIST's SP800-18 "Guide for Developing Security Plans for Information Technology Systems" details instructions for creating a SSP, however, a valuable SSP contains the following information:

- System Owner
- Secondary Point of Contact
- Business Function of the System
- System Interconnections
- Information Sensitivity
- Self-Assessment Control Areas

Each of these sections are described in detail in the following sections:

System Owner

The System Owner is the person who is ultimately responsible for the system. The person is usually a manager who is responsible for the business functions of the system, but is also responsible for management of the technology as well.

Secondary Point of Contact (POC)

The Secondary POC is the person who may be actually responsible for the day-to-day aspect of the system functions. He/she is not ultimately responsible for the functions, but plays a large role in maintaining the value of the system. He/she also serves as a decision maker regarding the technology and security of the system and can act in behalf of the System Owner in an emergency.

Business Function of the System

It is important to understand the business function of the system in order to understand the business impact of security controls and the appropriate level at which the system should be secured. A good example of this is that although it may be a "good security policy" to not allow sensitive information on employee laptops, however, the nature of the business that the system serves requires frequent travel and the use of agency laptops. If the security policy was enforced, the ability of the employees to perform their duties would be greatly impacted and the business function would suffer. Most likely, in this scenario, employees would find a way to break the rules in order to get their work done, or they would do it in secret.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appropriate countermeasures would not be implemented and the security of their information would eventually be compromised.

System Interconnections

It is important to know the inputs and outputs of a system and know what network and other systems are interconnected to the system. Knowing the network is important because it identifies where additional firewalls may be present (or should be present) and what other systems are on the network, especially if the system resides on a subnet. Knowing the systems that interconnect and the security of those systems is extremely important. For example, your system may be locked down tight, but if your system is connected to an insecure system through a trust relationship, the other system may be used as a host to gain unauthorized access into your system.

Information Sensitivity

This section declares the rating for Confidentiality, Integrity, and Availability (CIA) as High, Medium, or Low and provides justification for the ratings. Justifications are based on the types of data stored in or transmitted through the system, the impact of data tampering, and whether or not high availability requirements exist. These ratings are critical in determining the appropriate controls that should be implemented.

Self-Assessment Control Areas

This is the section with the most valuable information. It is truly the meat of the document, providing the details necessary to assess how well security is really managed. There are 17 subsections, one for each of the 17 Self-Assessment Control Areas. The information provided in these subsections should coincide directly with the answers to the Self-Assessment and describes how each applicable question in the Self-Assessment is implemented. It is not sufficient to simply state what controls are being implemented. This has already been identified in the Self-Assessment. To clarify this point, here are two examples:

Example 1: In the Risk Management section, the Self-Assessment states that they system is at Level 4 (Testing) for conducting a Risk Assessment. In the SSP, this section should describe how the Risk Assessment was conducted (i.e. using an agency provided template), that it is conducted annually, and that it has been conducted at least twice. The second time the process was evaluated to ensure that the implementation was effective for appropriately identifying the system's risks. This description satisfies the level ratings applied to this element because the assessor has showed that the Risk Assessment has been implemented (Level 3) and tested/evaluated (Level 4).

Example 2: In the Logical Access Controls section, the Self-Assessment states that the system is at Level 2 for periodically reviewing access control lists. This means that a policy and procedures for this control are documented. However, they are currently not following the procedures, or they would be at Level 3. The SSP should state what is currently being done in

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

this area and that implementation of periodic access reviews are planned. If the implementation plan exists, that should be in the SSP as well.

Contingency Plans

Contingency planning refers to interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.[10] Contingency Plans come in all sizes, levels of detail, and can cover various areas such as Disaster Recovery and Continuity of Operations. Federal agencies should refer to the NIST Special Publication 800-34 "Contingency Planning Guide for Information Technology Systems". This publication describes contingency planning and disaster recovery in great detail and offers templates to complete various aspects of contingency plans. In its most basic form though, a Contingency Plan should contain the following two sections.

- Business Impact Analysis (BIA)
- Recovery Steps

The following sections will focus on these two areas in detail.

Business Impact Analysis (BIA)

A key component to the contingency planning process is the BIA. A BIA provides the steps to identify critical information required during an emergency to smoothly restore operations to an acceptable level. The steps are as follows:

- Critical IT Resources (Business Processes, IT Assets, and Personnel)
- Disruption Impacts and Allowable Outage Times
- Recovery Priorities

Each of these will be discussed in detail in the following sections. The NIST SP800-34 states that a "Contingency Plan Coordinator" should be the one coordinating this effort and identifying the critical resources, downtimes and recovery priorities. Although this may be ideal, a group with knowledge of the system (system administrators, computer security officer, data owners) can be just as successful in achieving these goals.

Critical IT Resources

Critical system resources include the most important business functions or services provided by the system to its customers (whether internal or external). Similar in nature to a project schedule's Critical Path, the identification of these resources answers the following question: which function(s) would severely impact the organization or group if that service were no longer available? Once you have identified the critical functions, prioritize them.

[10] NIST SP800-34 - http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Once the business functions that are most critical are prioritized and documented, it's easy to identify the technology that supports those business functions. That should be documented as well.

Also important is identifying the people who support the system that would absolutely need to be available during an emergency? Who knows the ins and outs of the system? Who knows the technical aspect of the system? Who owns the data stored within the system? These are important questions to ask when conducting a BIA. The critical resources supporting the system should be documented as well, with emergency contact information.

The end result is a list of prioritized critical business functions, the technology supporting/enabling those critical business functions, and the people required to be available when an emergency arises.

Disruption Impacts and Allowable Outage Times

After the critical components to the system have been identified and documented, think about the impacts of a disruption in each of the business functions listed. These may vary greatly between the different functions.

For example, two sales functions within the same system were both deemed critical. The allowable downtime for the external-facing sales function is 48 hours, due to a manual order-taking process that can be implemented during the downtime to keep orders flowing, while a downtime in the internal order system may stop orders from being processed all together. The allowable downtime for the internal order system is only 4 hours due to the loss of revenue encountered when orders are not being processed.

Recovery Priorities

The next step is to bring both of the previous sections together to create an order in which each business function is to be recovered. In the example stated above, it would be most beneficial to the organization for the internal order function to be restored first, followed by the external sales function. This would result in the least amount of time where no orders can be processed.

As shown through the example above, the order in which business functions should be restored may not always be obvious. In this case once might first think the external sales function should be restored first. By following the BIA steps, a logical thought process concerning the business functions of the system is followed and it ensures that an organization is never caught off-guard without a plan to restore its most critical operations.

Recovery Steps

Conducting the BIA provides the knowledge necessary for creating and implementing a recovery plan based on what is truly critical to the system. The next step is to create a detailed action plan based on this information. This action plan would be specific to the type of system, such as a desktop system vs. a Unix server farm. The plan of action needs to be appropriate

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

for the business needs as well as the technology of the system. For example, a contingency plan for a desktop may be to have established a process for quickly purchasing a new PC or to join a centralized desktop management support group in anticipation of something going wrong. A contingency plan based on high powered servers, that are not easily purchased and configured, would be to fail-over to another server that is standing by in case of a problem. These procedures must designate roles and dictate exactly what each role is to perform.

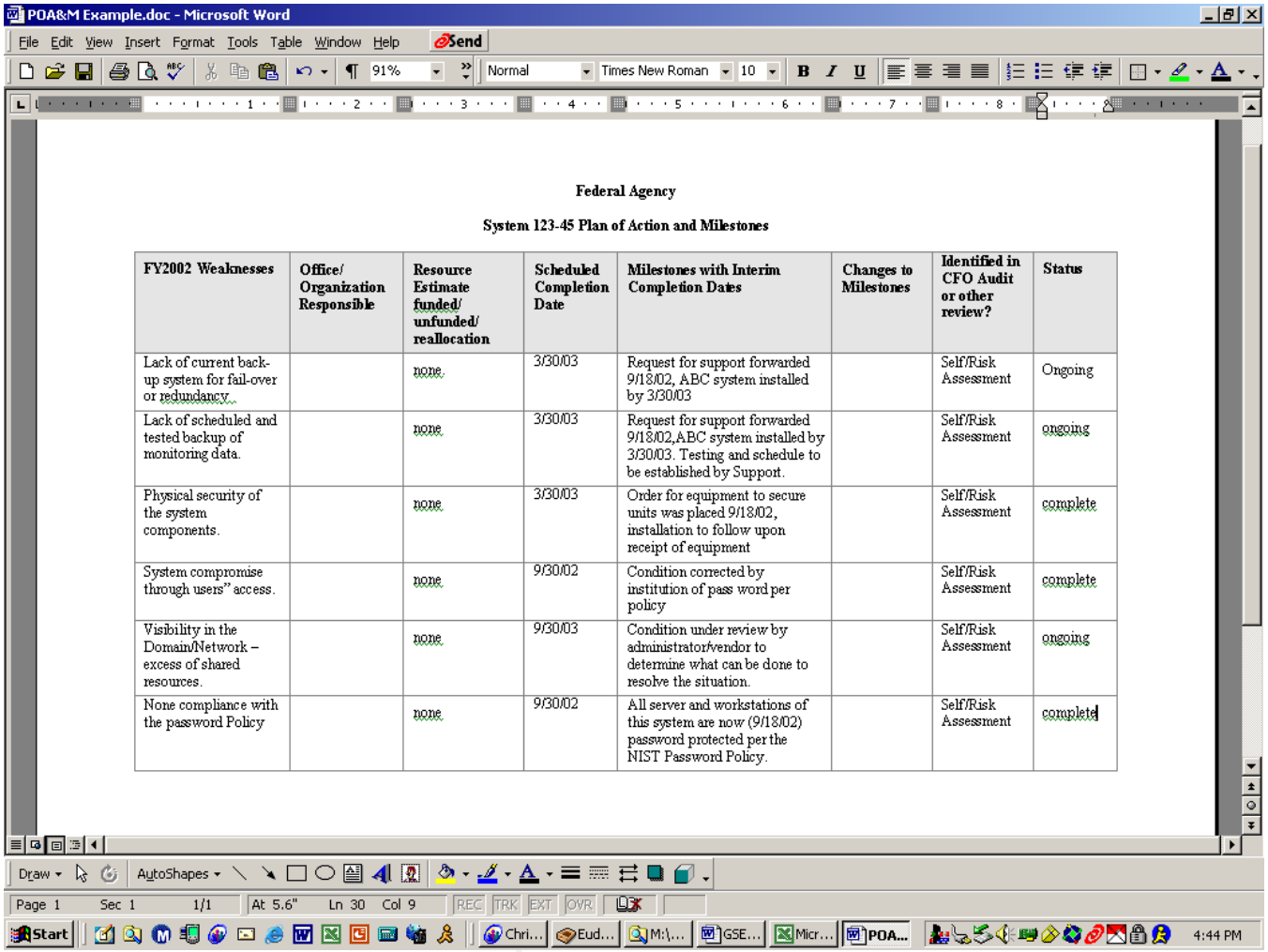
Plan of Action & Milestones

The last step in the process is to create an overall action plan to implement the necessary policies, procedures, or technical controls needed to reduce the risks identified during the entire C&A process. This action plan should include actions to resolve all deficiencies and have realistic goals that can be achieved in a reasonable timeframe, normally within one year. The action plan will include completion dates that: 1) describes how the agency plans to address any issues/weaknesses; and 2) identifies obstacles to address known weaknesses.[11]

OMB created the Plan of Action and Milestones (POA&M), with specific instructions to ensure that all federal agencies submit a consistent action plan, see Figure 2 below. Each agency must submit one POA&M for each system as well as a summarized program-level POA&M.

[11] Memorandum to Heads of Agencies - http://csrc.ncsl.nist.gov/policies/M-01-241.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Federal Agency

System 123-45 Plan of Action and Milestones

FY2002 Weaknesses	Office/ Organization Responsible	Resource Estimate funded/ unfunded/ reallocation	Scheduled Completion Date	Milestones with Interim Completion Dates	Changes to Milestones	Identified in CFO Audit or other review?	Status
Lack of current back-up system for fail-over or redundancy.		none	3/30/03	Request for support forwarded 9/18/02, ABC system installed by 3/30/03		Self/Risk Assessment	Ongoing
Lack of scheduled and tested backup of monitoring data.		none	3/30/03	Request for support forwarded 9/18/02,ABC system installed by 3/30/03. Testing and schedule to be established by Support.		Self/Risk Assessment	ongoing
Physical security of the system components.		none	3/30/03	Order for equipment to secure units was placed 9/18/02, installation to follow upon receipt of equipment		Self/Risk Assessment	complete
System compromise through users" access.		none	9/30/02	Condition corrected by institution of pass word per policy		Self/Risk Assessment	complete
Visibility in the Domain/Network – excess of shared resources.		none	9/30/03	Condition under review by administrator/vendor to determine what can be done to resolve the situation.		Self/Risk Assessment	ongoing
None compliance with the password Policy		none	9/30/02	All server and workstations of this system are now (9/18/02) password protected per the NIST Password Policy.		Self/Risk Assessment	complete

Figure 2 – POA&M Screen Shot

© SANS Institute

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

Fulfilling the requirements of system C&A provides the foundation for all FISMA security requirements. Each major component builds upon the other to create a comprehensive security profile for each system. These profiles are commonly referred to as certification packets. Each certification packet provides the Accreditor with the information needed to make a risk-based decision regarding whether the system's security is managed appropriately. Managed security makes the system less vulnerable to attack, and as each system's security improves, so improves the security of its agency and the government as a whole.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Lessons Learned

Throughout this process, many lessons have been learned that are useful for sharing. All of these tips are interconnected, but each has merit and is individually noteworthy.

1. Start the Process Early – When certification deadlines are on the horizon, plan to start the process early in the year, rather than waiting. For example, if certification packets are due at the end of the fiscal year (September), don't wait until Spring to introduce these new requirements to the masses. System certification is a lot of work and takes time to understand what they are to do and how to do it. Start the process in January, or earlier, by introducing the requirements due throughout the year and give people time to do it right.

2. Pre-fill All Centralized Processes - Before requiring anything from the system owners, review each component well for policies, procedures, and controls that are and should be implemented centrally. Pre-fill as much as possible, leaving only specifics regarding each specific system to be completed individually by system owners. Examples of centralized processes are physical security, HR, infrastructure security/maintenance (network, domain, firewalls), Rules of Behavior, Incident Response, etc. In most cases, the majority of systems will follow the centralized rules with no exceptions. Require documentation/action only if a system goes above and beyond the rules set by the organization. This will minimize work and provide consistency throughout the certification documentation.

3. Fully Explain the Point Behind the Process – The real benefit of this exercise is the increased security knowledge of all involved, as this process forces the entire organization to open their eyes to threats, impacts, and vulnerabilities, sometimes for the very first time. This is valuable knowledge that carries forward into all they do. Teach them that this is not a paper exercise created to appease auditors. Just the opposite, each component is valuable and critical to the mission of the organization. Security has been ignored for many years, and luckily, without too much impact. However, even the most disconnected people know that this is changing. IT Security is as important now as any other aspect of their job, because if not prepared, all they have worked for can be lost with one attack. The certification process, although painful at first and sometimes time consuming, teaches all involved the fundamentals of good security and how it applies to each system in the organization.

4. Set Realistic Deadlines – Allow time for people to understand what is expected, think about the state of security for their systems, and don't forget that they have their normal responsibilities as well. If the deadlines are too tight, people will quickly run through the assessments just to complete the requirements. When this occurs, a valuable benefit is lost, personnel taking security seriously, learning best practices, and identifying and understanding the impacts of not mitigating risks.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

5. Review and Provide Feedback - The process is not necessarily over when the certification packets are submitted to the IT Security Office or CIO Office. This is especially true during the first year. Many who complete these assessments for the first time may not fully understood how to correctly, and thoroughly, complete them. A thorough review is recommended to identify areas that need to be revisited. Sometimes they need help understanding what a self-assessment question means, sometimes they are simply "too busy" to complete an assessment. All components need to be reviewed and feedback provided to ensure that all system owners understand how to effectively manage the risks for their systems.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

1. General Accounting Office. "INFORMATION SECURITY Serious and Widespread Weaknesses Persist at Federal Agencies." Report to the Chairman, Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives. 6 Sept. 2000. URL: http://www.gao.gov/new.items/ai00295.pdf (22 Jan. 2003).

2. General Services Association. "Protecting America's Critical Infrastructure: How Secure are Government Computer Systems?" House Committee on Energy and Commerce Hearing. 5 April 2001. URL: http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/legupdate4.doc (22 Jan. 2003).

3. Hasson, Judi. "Davis aims to solidify GISRA". Federal Computer Week. 13 Dec. 2001. URL: http://www.fcw.com/fcw/articles/2001/1210/web-gisra-12-13-01.asp (22 Jan. 2003).

4. Ross, Ron. Swanson, Marianne. "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems." NIST Special Publication 800-37. October 2002. URL: http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf (22 Jan. 2003).

5. Lew, Jack. "Guidance On Implementing the Government Information Security Reform Act." Memorandum For The Heads Of Executive Departments And Agencies. 16 Jan. 2001. URL: http://www.whitehouse.gov/omb/memoranda/m01-08.pdf (22 Jan. 2003).

6. Dept of Health and Human Services. "System Security Plans (SSP) Methodology." Centers for Medicare & Medicaid Services. 6 Nov. 2002. URL: http://www.cms.hhs.gov/it/security/docs/ssp_meth.pdf (22 Jan. 2003).

7. Stoneburner, Gary. Goguen, Alice. Feringa, Alexis. "Risk Management Guide for Information Technology Systems." NIST Special Publication 800-30. October 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (22 Jan. 2003).

8. Frank, Diane. "Final security guide arrives." Federal Computer Week. 17 Sept. 2001. URL: http://www.fcw.com/fcw/articles/2001/0917/pol-guide-09-17-01.asp (22 Jan. 2003).

9. Swanson, Marianne. "Security Self-Assessment Guide for Information Technology Systems." NIST Special Publication 800-26. November 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf (22 Jan. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10. Swanson, Marianne. “Contingency Planning Guide for Information Technology Systems.” NIST Special Publication 800-34. June 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf (22 Jan. 2003).

11. Daniels, Jr., Mitchell. “Reporting Instructions for the Government Information Security Reform Act.” Memorandum For The Heads Of Executive Departments And Agencies. 16 Jan. 2001. URL: http://csrc.ncsl.nist.gov/policies/M-01-241.pdf (22 Jan. 2003).

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: November 30th, 2015

Upcoming SANS Training

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

Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SANS Dubai 2016	**Dubai, AE**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Las Vegas 2016	**Las Vegas, NVUS**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Cyber Defence Delhi 2016	**Delhi, IN**	**Jan 11, 2016 - Jan 22, 2016**	**Live Event**
SANS Brussels Winter 2016	**Brussels, BE**	**Jan 18, 2016 - Jan 23, 2016**	**Live Event**
SANS Security East 2016	**New Orleans, LAUS**	**Jan 25, 2016 - Jan 30, 2016**	**Live Event**
SANS Copenhagen 2016	**Copenhagen, DK**	**Feb 01, 2016 - Feb 06, 2016**	**Live Event**
Cyber Threat Intelligence Summit & Training	**Alexandria, VAUS**	**Feb 03, 2016 - Feb 10, 2016**	**Live Event**
SANS Scottsdale 2016	**Scottsdale, AZUS**	**Feb 08, 2016 - Feb 13, 2016**	**Live Event**
SANS Secure Japan 2016	**Tokyo, JP**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS Munich Winter 2016	**Munich, DE**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS McLean 2016	**McLean, VAUS**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
ICS Security Summit & Training	**Orlando, FLUS**	**Feb 16, 2016 - Feb 23, 2016**	**Live Event**
SANS Secure India 2016	**Bangalore, IN**	**Feb 22, 2016 - Mar 05, 2016**	**Live Event**
SANS Anaheim 2016	**Anaheim, CAUS**	**Feb 22, 2016 - Feb 27, 2016**	**Live Event**
RSA Conference 2016	**San Francisco, CAUS**	**Feb 28, 2016 - Feb 29, 2016**	**Live Event**
SANS London Spring 2016	**London, GB**	**Feb 29, 2016 - Mar 05, 2016**	**Live Event**
SANS Philadelphia 2016	**Philadelphia, PAUS**	**Feb 29, 2016 - Mar 05, 2016**	**Live Event**
HIMSS	**OnlineMAUS**	**Dec 01, 2015 - Dec 02, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**