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.

Implementing an Effective IT Security Program

The purpose of this paper is to take the wide variety of US federal laws, regulations, and guidance combined with industry best practices and define the essential elements of an effective IT security program. The task may seem impossible given the thousands of pages of security documentation published by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), the National Security Agency (NSA), and the General Accounting Office (GAO), just to name a few. However, this paper...

Copyright SANS Institute
Author Retains Full Rights

AD

Kurt Garbars
GSEC version 1.4

Implementing an effective IT Security Program

Abstract

The purpose of this paper is to take the wide variety of federal government laws, regulations, and guidance combined with industry best practices and define the essential elements of an effective IT security program. An effective program includes many elements and the task seems impossible as you begin reading the literally thousands of pages of security documentation published by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), the National Security Agency (NSA), and the General Accounting Office (GAO), just to name a few. This paper will highlight important elements in a short, easy to read guide. This paper is not intended to identify every security program element in detail, but should give the reader a good basis on how to implement an effective security program. The five critical elements of a security program according to GAO Federal Information Systems Control Manual (FISCAM) are the following:

1. Periodically Assess Risk
2. Document an entity-wide security program plan
3. Establish a security management structure and clearly assign security responsibilities
4. Implement effective security-related personnel policies
5. Monitor the security program's effectiveness and make changes as necessary

This paper will use this framework as the overall structure and integrate further detail from NIST, OMB, NSA and others to clarify these areas.

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

Implementing an effective IT Security Program

There are a wide variety of federal government laws, regulations, and guidance along with industry best practices that define the essential elements of an effective security program. An effective program includes many elements and the task seems impossible as you begin reading the literally thousands of pages of security documentation published by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), the National Security Agency (NSA), and the General Accounting Office (GAO), just to name a few. The five critical elements of a security program according to GAO FISCAM are the following:

1. Periodically Assess Risk
2. Document an entity-wide security program plan
3. Establish a security management structure and clearly assign security responsibilities
4. Implement effective security-related personnel policies
5. Monitor the security program's effectiveness and make changes as necessary

We will use this framework as the overall structure and integrate further detail from NIST OMB, NSA and others to further clarify these areas.

Periodically Assess Risk

Assessing your organization's risk is one of two beginning steps in developing a security program. The other is establishing a security management structure and clearly assigning security responsibilities. The latter is more difficult in a large decentralized organization and takes much longer than you would think. This will be discussed in further detail later in this paper. As you are formalizing your structure, risk assessments and mitigations strategies are still going to need to be accomplished.

Without having an understanding of your risk you are unable to determine the proper security policies, procedures, guidelines, and standards to put in place to ensure adequate security controls are implemented. A risk assessment has three major components – threat assessment, vulnerability assessment, and asset identification. Threats can be grouped in many different ways. We will use 4 categories – malicious insider (disgruntled employee, contractor, insider theft), accidental insider (poorly trained, curious) malicious outsider (hacker, industrial espionage) and natural (fire, flood). These four threat categories coupled with the following modified list of vulnerability categories from the NSA Information Assurance Model (IAM) outlined in Bryan Hurd's paper will put you well on your way to describing two of the three elements of a risk assessment. I have also created a short list of vulnerability assessment questions that I believe get at the

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

crux of most of the security incidents I have seen in my career. This is not intended to be all-inclusive, but to get you thinking in the right areas.

1. INFOSEC Documentation

    a. Do you have a security plan, risk assessment report, contingency plan, configuration management plan, and security, test, and evaluation report?
    b. If so, what are the dates, if not when are they planned?

2. INFOSEC Roles and Responsibilities
    a. Does this system have an Information Systems Security Officer (ISSO) assigned?

    b. Do you know who your Designated Approving Authority (DAA) is? (This is the executive responsible for the security of the system)

3. Identification and Authentication
    a. What password policy does your system enforce?
        i. Number of Characters (minimum 7 or 8)
        ii. Complexity (3 of following 4- upper and lowercase, numbers, special characters)
        iii. Aging (90 days – max)
        iv. Account Lockout (5 attempts)
        v. What method do you use to encrypt passwords in transit and in storage? (key type, key length, etc)
    b. Do you have a procedure for identifying users before resetting passwords?

4. Account Management/Access Controls
    a. Do you have a method of authorizing new accounts and getting rid of old accounts?
    b. Do you have a process to limit access based on job function and/or roles?
    c. Do you regularly review your access control lists, if so how often?
    d. Do you give individuals only enough access to do their jobs? (i.e. Least privilege)

5. Session Controls
    a. Do you enforce each user to be logged on with only one session?
    b. Do you enforce password protected screen savers?

6. External Connectivity
    a. Does this system have any external connectivity?
        i. Wireless (describe controls)
        ii. Internet (describe controls- e.g. VPN, FW, etc)

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

iii. Dial-in (describe controls- e.g. authentication method, encryption, etc.)

7. Security Products
    a. Do you use a firewall (briefly describe what is and is not allowed to this box)
    b. Do you use an intrusion detection system? (host, network, briefly describe configuration)
    c. Do you use a policy compliance tool or agent?
    d. Do you use vulnerability scanning tools?
    e. Do you use encryption? If so, describe (symmetric, asymmetric, key lengths, etc.)

8. Auditing
    a. Do you have auditing turned on?
    b. What events are you auditing for?
    c. How often do you review audit logs?

9. Virus Protection
    a. Do you have virus protection installed?
    b. How often is it updated and is it automatic?

10. Contingency Planning/Backups
    a. How often do you do back-ups?
    b. Do you have procedures to restore system?
    c. How many people could restore system?
    d. How long would it take to restore system?
    e. Where do you keep your backups in relation to your system?
    f. Do you have a contingency plan that includes continuity of operations?
    g. Have you tested your back-up procedures?

11. Maintenance
    a. Have you hardened the system using NSA Hardening Guides or other Industry hardening guides? (explain)
    b. Have you applied all applicable security patches?
    c. Have you secured your systems using the SANS Top 20?

12. Configuration Management
    a. How do you do change management?
    b. Do you have a separate system to test changes?
    c. Do you have a configuration management plan?

13. Media Sanitization/Disposal
    a. Is your data sensitive, so that it should not be obtainable upon disposal?

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

b. What method do you use to dispose of data?
    i. Hard drive (Triple overwrite, degauss)
    ii. Tapes (degauss)
    iii. CDs (incinerate, chemically destroy)
    iv. Paper (shred)

14. Physical Environment
    a. Are your servers in a locked room with tight access controls?
    b. What kind of access controls does your building have?
    c. Are there any special considerations that need to be taken into consideration based on building location? (hurricanes, floods, etc)
    d. Is your system protected from environmental threats? (heat, fire, water, etc)

15. Personnel Security
    a. Are your users trained on the security of this system or have they taken security awareness training?
    b. Have your users read the rules of behavior for either this system or organizational rules or policies?
    c. Have employees and/or contractors who have privileged access to this system undergone background investigations?
    d. Do you have separation of duties between programmers and administrators? (If not, what do you use to prevent abuses)

16. Incident Handling/Security Advisory Handling
    a. Briefly describe your process to handle incidents
    b. Briefly describe your process to handle security advisories

17. Security Awareness Training/Security Training
    a. Have you provided security awareness training to all employees?
    b. Is security awareness an ongoing activity throughout the year?
    c. Are your security officers, system administrators, senior executives, system program managers, and business/functional managers trained in their security responsibilities?

The answers to these questions along with some random sampling of specific technical controls will give you a basis for your vulnerabilities. This would be an opportune time to use the Center for Internet Security's Baseline Security Tools, Microsoft Baseline Security Analyzer, the Nessus Security Scanning Tool, or any other tool you may have to identify specific vulnerabilities. Another excellent source of vulnerabilities that should be used at this stage is SANS Institute's list of the Top Twenty Internet Security Vulnerabilities.

Before you begin the daunting task of asset analysis, you can quickly identify and mitigate some of the highest risk items that you discovered in your vulnerability phase. I know the textbook solution is to analyze likelihood of exploitation

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

against impact to asset and rank the risks accordingly, but certain hardening and patching steps should be taken immediately upon vulnerability discovery and cannot wait for the completion of a comprehensive report. This is where it is essential that common sense be used.

Now that you have defined both your threats and your vulnerabilities and fixed some of your highest risk vulnerabilities, it's on to the hard part – defining your assets, assigning value to your assets, and rating your assets according to their need for confidentiality, integrity, and availability. (CIA) I have performed both quantitative and qualitative risk assessments and have found it very difficult to perform a valuable and cost effective quantitative risk assessment. Many of the values you need to calculate to complete the risk assessment become very difficult to obtain, thereby invalidating much of the results. With that said, you need a general idea of how important the asset is to the organization in order to justify to management the cost of the security controls. In addition to cost, you need to have an understanding of which area of CIA warrants the most attention, and thus security controls. You need to develop a rating system for confidentiality, integrity, and availability that can be applied across your enterprise. For instance, your financial systems may need a high level of integrity, but have less of a need for confidentiality or availability. Your company's latest research project data may have the highest level of confidentiality whereas your e-commerce website may be most affected by availability. This analysis is very difficult and needs input from the highest levels of management in order to rank the assets appropriately.

When you have completed these three steps you can then compare the threats to your systems (which house your information) to the vulnerabilities you have found and balance that against the need and cost to protect the confidentiality, integrity, and availability of that asset. There ends up being a lot of professional judgment that goes into this analysis. Unfortunately as we become more and more connected with our internal systems as well as external systems, it is becoming increasingly important to put a fair amount of management, operational, and technical controls on all of our systems. For example, you may have an intranet web server that has no access to the Internet and does not carry any sensitive data. You do your CIA analysis and determine that there is little need for confidentiality, integrity, or availability. Management may determine that if something happens to that server it can be rebuilt and back on line in a few days with no effect on business operations. This may not be the right decision. A home user that dials in can infect that server. Not using egress filtering and allowing the system administrator to access the Internet as a client can also infect it. That server may then start attacking other servers that do have a high need for CIA. Analyzing connectivity becomes very important in this analysis.

You have defined your assets, looked at the threats against you, and determined the vulnerabilities you have. You know where your greatest risks reside. For those high risks you will need to do short term hardening, patching, etc. You will

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

not be able to wait the year or more it takes to develop sound policies, procedures, and standards in a large decentralized organization. The cyber-criminals are not going to wait until you coordinate your new firewall policy through three layers of management before you cut-off some new dangerous threat. In spite of short-term tactical necessity, sound policy, procedures, standards, and guides are critical in ensuring the long-term security of your assets.

In addition to an initial review of your security risks, risks should be assessed on a continuing basis as new threats and vulnerabilities manifest themselves and new assets are put into operation.

You have now completed the first critical element of the security program – the risk assessment. Now it is time to develop the security program plan.

Document an entity-wide security program plan

There are many different opinions on what should go into an entity-wide security program plan. I have found these six general areas to be the most valuable.

1. Security management structure and security responsibilities
2. Security Policy, procedures, guides, and standards
3. Security Training and Awareness
4. Incident Handling and Security Advisory Handling
5. Compliance Reviews and Enforcement (including vulnerability scanning and penetration testing)

<u>Security management structure and security responsibilities</u>

This is a very important step and needs management buy-in throughout the organization. It is the first step in creating an entity-wide security program plan, but it is also one of the critical elements in the overall program. There are differences of opinion these days about how to establish a security management structure. Some feel there needs to be a Chief Information Security Officer (CISO) that reports directly to the head of the organization. Others feel the security program should be run out of the Office of the Chief Information Officer (CIO) and the top security official should report directly to the CIO. Much of it depends on what the responsibilities of the CIO are within the organization. Does the CIO only set information systems policy? Do they manage IT operations? Are they centrally funded and do they control the IT budget? These are all things that need to be taken into account. If the CIO does not control the IT budget of the various organizations responsible for adhering to the policy and the head of the organization does not give the authority to the CIO to enforce the policies, it becomes very difficult to enforce compliance as part of the monitoring program.

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

These same issues filter all the way down the organization. It is necessary to have a central security program office that can coordinate all of these agency-wide activities. A key question that needs to be asked is, who is ultimately responsible for the security of the system? Under the government structure you generally have a minimum of five – six key players involved which include the CISO, system program manager, information system security officer, system administrator, designated approving authority, and the business/functional manager. The following is an example of a high-level breakdown of responsibilities:

Chief Information Security Officer – Responsible for the overall, management, implementation, and enforcement of the IT security program.

System Program Manager – Responsible for overall lifecycle planning of system including acquisition, operations, etc. They need to ensure security is funded for and implemented in their systems.

Information Systems Security Officer (ISSO) – Responsible for administrative and operational aspects of security for the system. This includes creation and maintenance of all security documentation, ensuring that systems are hardened and patched, monitoring system security controls, handling incidents, etc.

System Administrator – Responsible for the day-day care and feeding of the system to include security hardening and patching, backups, etc.

Designated Approving Authority (DAA) – They are the senior executive that has ultimate responsibility over the funding, configuration, and operation of the asset. The buck stops here. They are the ones that accept the risk of operating the system and need to have the authority to shut it down if it is not secure. They need to be held accountable and liable if they do not show due diligence.

Data Owner or Business/Functional Manager – Helps set the requirements for the level of protection needed for their process or data.

Depending on the size of the organization, there can also be information systems security managers that manage and coordinate the various activities of their ISSOs. They also act as a liaison between the central security office and the individual system security officer.

Now that we see an example of an ideal structure on paper, I would like to describe where this structure has some challenges in actual implementation. A couple of big challenges are related to the DAAs. In organizations that have matrix management, coupled with both centralized and decentralized processes and information technology, it is a challenge to determine exactly who the DAA is. Another challenge lies in the fact that the DAAs sometimes take on more risk than they really should be allowed to. Up until now, both corporate America and

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

government have not held their senior executives accountable for security breaches very often. Until some of them are held liable for lacking due diligence, this trend will continue.

Another big area is the relationship between the system administrator and the information systems security officer. The ISSO is responsible for ensuring the security of the system, but in many cases they either do not have management backing or they do not have the technical expertise to ensure the systems are operating securely. They rely on the system administrator who is primarily concerned with keeping the system running. In some cases, the system administrator is the security officer. This often increases the technical security controls of the system, but this person is generally very overworked and is not able to create the plan and procedural documents that ensure the long term security of the system and keep the auditors happy. There is also the question of separation of duty and the fact that many system administrators are contract employees who may have less than a vested interested in the company. Until management takes security more seriously and some of the reporting requirements are reduced, I think we are heading down a dangerous path. Everyone from auditors to budget managers to customers are demanding more prove of how secure the systems are, but the more reporting you have to do the less time you have to secure the system. I believe we need to move toward a more minimalist approach to documentation and only document the processes that are absolutely necessary. I have seen too many hundred page security documents sitting on shelves and too much time wasted creating them.

Finally, even though the security responsibilities are defined, individuals need to have their yearly performance reviews or in the case of senior management their bonuses incorporate security related incentives and/or disincentives. Since few system administrators, system program managers, or senior executives are rated on their security posture, things will be slow to change.

Security Policy, procedures, guides, and standards

It is now time to document your security policy. All security documentation to follow will be based off of your security policy. (Some more direct than others). Where do you start? There are a number of good places to help you formulate and document the requirements to go into your policy including public law (especially if you are a government agency), your risk assessment, OMB A-130, NIST 800-26, and Charles Cresson Wood's "Information Security Policies Made Easy". A combination of high level and detailed policies are necessary to achieve your security goal. I know there are a couple of different camps on how detailed policies should be – ranging from "All systems shall authenticate their users before they are allowed access" to "All systems shall employee a minimum of 8 character passwords, using a combination of special characters, letters, and numbers which are changed every 90 days and not repeatable up to 10 iterations." To keep your enterprise consistent, I favor the latter, but being that

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

detailed may not work in some organizations. Allowing flexibility in policy using risk-based decision-making is also very important

A method of policy development I have found useful recently is to align the policy into the three control areas defined in NIST 800-12 and NIST 800-18. These are management controls, operational controls, and technical controls. They are then further broken out into 17 control elements as defined in NIST 800-26. These are defined on the left with the vulnerability assessment categories mapped to them on the right.

Table 1

Management Controls	**Vulnerability Assessment Mapping**
1. Risk Management	Risk Assessment Itself
2. Review of Security Controls	InfoSec Documentation
3. Lifecycle	Configuration Management
4. Certification and Accreditation	InfoSec Documentation
5. System Security Plan	InfoSec Documentation InfoSec Roles and Responsibilities
Operational Controls	
6. Personnel Security	Personnel Security
7. Physical Security	Physical Environment
8. Production, Input/Output Controls	Media Sanitization/Disposal
9. Contingency Planning	Contingency Planning/Backups
10. HW/SW Maintenance	Maintenance
11. Data Integrity	Virus Protection
12. Documentation	InfoSec Documentation
13. Security Awareness and Training	Security Awareness and Training
14. Incident Response	Incident Handling/Security Advisory Handling
Technical Controls	
15. Identification and Authentication	Identification and Authentication
16. Logical Access Controls	Account Management/Access Controls Session Controls
17. Audit Trails	Audit
	Security Products External Connectivity

These are high-level mappings and specific requirements map to other very specific sub-requirements. The process gets convoluted very quickly. If you stick to these 17 areas for your well-defined policy it will organize your security program priorities and give you a means to enforce your security program. In

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

addition to these 17 areas it is critical that Roles and Responsibilities are defined in your policy. These are loosely mapped to the System Security Plan control item in the table. It is crucial that you get buy-in from upper management on your policies. They will make or break your security program. If they do not take the security policy seriously neither will their system program managers or their employees. It is important to build rapport with the key managers. I cannot overemphasize the importance of this. It is also important to get approval from labor relations and human resources when defining disciplinary and enforcement criteria for your policies.

Once you get the policy approved it is now time to start developing procedures, guides, and standards. Without procedures, guides, and standards the system program managers and their information security officers will not have the tools in order to implement your policies. Procedures, Guides, and Standards have very specific definitions, but in practice they can sometimes get blurred. Procedures are specific steps that one must follow to accomplish a task. Guides are best practices to implement a policy, but there is flexibility in their use, and standards set specific technical criteria that most be adhered to, such as how to harden and configure a Windows 2000 server.

Security Training and Awareness

Now that you have all of these great policies, procedures, guides, and standards it is time to start telling people about them and training them on them. This is where security awareness and training become critical. If all of your hard work just sits on a shelf somewhere collecting dust you have wasted a lot of time. Security awareness needs to visible on a regular basis. An annual security awareness-training course is an absolute necessity to keep people up on the latest security information, but equally important are short email updates, newsletters, and other reminders. It is also of utmost importance to train your security officers, system administrators, senior executives, system program managers, and business managers. They are the key players that will implement the comprehensive policies that you have created. After awareness and training, the next step is to get individuals such as the system administrators and security officers formal training such as SANS.

Incident Handling and Security Advisory Handling

Incident handling and security advisory are the next important area. Central management and reporting of all incidents is important to getting an understanding of the agency's security posture. It is not only important to coordinate potential multi-faceted attacks, but a central focal point can also develop expertise as they gain experience with agency specific issues. It is very important as part of the policy, procedure, and training phases, that everyone in the agency understands incident handling procedures. A central distribution point for security advisory handling is also critical to a successful security

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

program. Distributing and tracking security advisory compliance assures a secure technical configuration. This assurance can be obtained from a combination of self-reporting, auditing and automated tools.

Compliance Reviews and Enforcement

It's now time to ensure that all of your policies, procedures, and standards are being adhered to. This will be accomplished through a variety of methods to include self assessments and reporting, vulnerability and penetration testing, site security reviews, and an enterprise tool that queries agents on every desktop and server to give the security configuration status.

Compliance reviews consist of yearly reviews of all applicable system security documentation including security plans, risk assessment reports, security test and evaluation reports, contingency plans, and configuration management and change control plans. They also consist of reviews of a subset of the other 17 control areas in the NIST 800-26 questionnaire such as password controls, access controls, personnel controls, physical controls, etc. The management and operational controls can generally be accomplished through documentation reviews while the more technical controls are verified through vulnerability scanning, host reviews, and penetration testing. Due to the proliferation of new threats weekly, it is prudent to do some kind of technical testing at least every 3 months. If enterprise management security tools are implemented systems can be assessed on a continuing basis.

Implement Effective Security Related Personnel Policies

This is also a very challenging area because it forces you to coordinate and get concurrence with many different organizations to make it work. It involves labor relations, human resources, legal, and contracting people. The following control areas for personnel security are outlined in GAO FISCAM.

1. Background checks
2. Reinvestigations
3. Nondisclosure agreements
4. Regular vacations and shift rotations
5. Termination and Transfer Procedures
    a. Return of equipment, ID, keys, etc.
    b. Termination of User IDs and Passwords
    c. Identifying Non-disclosure period effectiveness
6. Skills needed are identified in job descriptions and employees are rated against those skills
7. Employee has a training plan and training is documented and monitored

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

I have found that other than training which is covered in other areas, that background checks and termination and transfer procedures are critical in minimizing insider risk. This is especially true with the proliferation of contractor and temporary employees. Regular vacations and shift rotations are a great idea, but in this day of massive downsizing and doing more with less it is not always practical to have the only person that knows the job be gone at a critical time. I realize that there should always be backups for everything, but management does not always want to budget for it.

Monitor the Security Program's Effectiveness and Make Changes as Necessary

Monitoring the effectiveness of the security program can be one of the most challenging aspects of running a security program, but also one of the most important. This is where the rubber meets the road. You have assessed the overall risk, created a program plan and security policies. You have given out guidance and trained the individuals in implementing the policy. Now it's time to see if you have actually increased the security posture of your organization. In large organizations and limited centralized IT Security staff you will have to rely on a combination of self-reporting and hands on reviews. These can include the following:

1. NIST 800-26 reviews with supporting documentation
2. Vulnerability and system scanning of technical controls and system vulnerabilities
3. Random onsite checks of operational and technical controls
4. Specific security policy compliance reviews
5. Audit finding reviews

Although the entire version is very cumbersome, a tailored version of the NIST 800-26 "Self Questionnaire" is a good place to start. It lets individual major applications and general support systems report back centrally on the status of their security controls. It is broken down into the 17 control areas defined in table 1. It further asks you whether or not you have created policies, created procedures; implemented, tested, and fully integrated each of these control areas into the security of your system. As you implement each of the five levels - policy, procedures, implementation, test, and integration you move further up the maturity level. This is very similar to the Software Engineering Institute's Capability Maturity Model (CMM) for software development.

It is critical that you use a common sense approach when implementing this or you can get very bogged down in a lot of documentation that does not really increase your security posture. Quickly getting at the critical elements by having your system security officers first perform a risk assessment and create a security plan for their system will greatly enhance the usability of this tool.

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

The other methods listed above can also be implemented via a variety of actual hands-on review and/or tabletop review of documentation. Much of it depends on the amount of resources you have and how successful your experience is with self-reporting. In many cases, self-reporting does not uncover serious vulnerabilities.

We have now completed a variety of program monitoring and have come up with a variety of weaknesses based on a lack of implementation. The next step is to uncover why. Is it because the policy and guidance is not clear? Is it a lack of resources, expertise, or management support? Do some people just not care about security?

The answer is all of the above. That is why it is critical to get out and talk to your system administrators, security officers, business and system program managers and upper level executives. You have to work with them to come up with a viable solution to their problems with implementation. You have to make sure that your office becomes a central focal point and that different divisions can leverage off your expertise as well as the expertise of others in the organization. You have to attack the most critical areas first and leave the rest for another day. They will vary somewhat for different systems, but the SANS "Top Twenty" is a real good place to start. It is critical to get buy-in from the top down and the bottom up to maintain an effective security program. If people do not believe in the process they will go through the motions, but you will not be very successful. On the other hand, you will always have individuals who do not want to follow the rules no matter what and you do need to be able to enforce the policies on those individuals.

Summary

There are five areas of a security program as defined in FISCAM.

1. Periodically Assess Risk
2. Document an entity-wide security program plan
3. Establish a security management structure and clearly assign security responsibilities
4. Implement effective security-related personnel policies
5. Monitor the security program's effectiveness and make changes as necessary

Each of these areas uses various techniques and controls to ensure effectiveness. This paper has attempted to outline and summarize best practices used based on guidelines, regulations, and personal experience. It was not intended to comprehensively address every issue and nuance in running a security program. There are thousands of pages of documents, which are referenced in this paper that will provide you with more specific information as you are implementing your security program.

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

References

Carnegie Mellon. "Software Engineering Institute (SEI) Capability Maturity Model (CMM)". URL: http://www.sei.cmu.edu/cmm/cmms/cmms.html (26 Aug 2002)

Center for Internet Security. "Benchmarks and Scoring Tools for Windows 2000 and Windows NT". July 2002.
URL: http://www.cisecurity.org/bench_win2000.html (26 Aug 2002)

Hurd, Bryan E. "The Digital Economy and the Evolution of Information Assurance". 5-6 June 2001. URL:
http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW1C3(20).pdf (26 Aug 2002)

Microsoft. "Microsoft Baseline Security Analyzer". URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp (26 Aug 2002)

National Institute of Standards and Technology (NIST). "An Introduction to Computer Security: The NIST Handbook". NIST SP 800-12. October 1995.
URL: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (26 Aug 2002)

National Institute of Standards and Technology (NIST). "Federal Information Technology Information Technology Security Assessment Framework". 28 November 2000. URL:
http://www.cio.gov/Documents/federal%5Fit%5Fsecurity%5Fassessment%5Fframework%5F112800%2Ehtml (26 Aug 2002)

National Institute of Standards and Technology (NIST). "Generally Accepted Principles and Practices for Securing Information Technology Systems". September 1996.
URL: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf (26 Aug 2002)

National Institute of Standards and Technology (NIST). "Guide for Developing Security Plans for Information Technology Systems". NIST SP 800-18. December 1998.
URL: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF (26 Aug 2002)

National Institute of Standards and Technology (NIST). "Risk Management Guide for Information Technology Systems". NIST SP 800-30. January 2002.
URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (26 Aug 2002)

National Institute of Standards and Technology (NIST). "Security Self-Assessment Guide for Information Technology Systems". NIST SP 800-26. November 2001.
URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf (26 Aug 2002)

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

National Security Agency (NSA). "Infosec Assessment Methodology".
URL: http://www.iatrp.com/ (26 Aug 2002)

Nessus. "Nessus Security Scanner".
URL: http://www.nessus.com/documentation.html (26 Aug 2002)

Office of Management and Budget (OMB). "Management of Federal Information Resources". OMB Circular A-130. 28 November 2000.
URL: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html (26 Aug 2002)

SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities". Version 2.504. 2 May 2002. URL: http://www.sans.org/top20.htm(26 Aug 2002)

United States General Accounting Office (GAO). "Federal Information System Control Audit Manual". GA0/AIMD-12.19.6. June 2001.
URL:http://www.gao.gov/special.pubs/ai12.19.6.pdf (26 Aug 2002)

Wood, Charles Cresson. Information Security Policies Made Easy. Houston: Pentasafe Security Technologies, Inc, May 2001.

© SANS Institute 2002, Author retains full rights.

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

Last Updated: October 24th, 2016

Upcoming SANS Training

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

SANS Sydney 2016	**Sydney, AU**	**Nov 03, 2016 - Nov 19, 2016**	**Live Event**
SANS Gulf Region 2016	**Dubai, AE**	**Nov 05, 2016 - Nov 17, 2016**	**Live Event**
DEV534: Secure DevOps	**Nashville, TNUS**	**Nov 07, 2016 - Nov 08, 2016**	**Live Event**
SANS Miami 2016	**Miami, FLUS**	**Nov 07, 2016 - Nov 12, 2016**	**Live Event**
DEV531: Defending Mobile Apps	**Nashville, TNUS**	**Nov 09, 2016 - Nov 10, 2016**	**Live Event**
European Security Awareness Summit	**London, GB**	**Nov 09, 2016 - Nov 11, 2016**	**Live Event**
SANS London 2016	**London, GB**	**Nov 12, 2016 - Nov 21, 2016**	**Live Event**
Healthcare CyberSecurity Summit & Training	**Houston, TXUS**	**Nov 14, 2016 - Nov 21, 2016**	**Live Event**
SANS San Francisco 2016	**San Francisco, CAUS**	**Nov 27, 2016 - Dec 02, 2016**	**Live Event**
SANS Hyderabad 2016	**Hyderabad, IN**	**Nov 28, 2016 - Dec 10, 2016**	**Live Event**
MGT517 - Managing Security Ops	**Washington, DCUS**	**Nov 28, 2016 - Dec 02, 2016**	**Live Event**
SEC560 @ SANS Seoul 2016	**Seoul, KR**	**Dec 05, 2016 - Dec 10, 2016**	**Live Event**
ICS410 @ Delhi	**New Delhi, IN**	**Dec 05, 2016 - Dec 09, 2016**	**Live Event**
SANS Dublin	**Dublin, IE**	**Dec 05, 2016 - Dec 10, 2016**	**Live Event**
SANS Cologne	**Cologne, DE**	**Dec 05, 2016 - Dec 10, 2016**	**Live Event**
SANS Cyber Defense Initiative 2016	**Washington, DCUS**	**Dec 10, 2016 - Dec 17, 2016**	**Live Event**
SANS Frankfurt 2016	**Frankfurt, DE**	**Dec 12, 2016 - Dec 17, 2016**	**Live Event**
SANS Amsterdam 2016	**Amsterdam, NL**	**Dec 12, 2016 - Dec 17, 2016**	**Live Event**
SANS Security East 2017	**New Orleans, LAUS**	**Jan 09, 2017 - Jan 14, 2017**	**Live Event**
SANS Brussels Winter 2017	**Brussels, BE**	**Jan 16, 2017 - Jan 21, 2017**	**Live Event**
Cloud Security Summit	**San Francisco, CAUS**	**Jan 17, 2017 - Jan 19, 2017**	**Live Event**
SANS Las Vegas 2017	**Las Vegas, NVUS**	**Jan 23, 2017 - Jan 30, 2017**	**Live Event**
Pen Test HackFest Summit & Training	**OnlineVAUS**	**Nov 02, 2016 - Nov 09, 2016**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**