Global Information Assurance Certification Paper

A Technical Writer's Guide to Documentation in the Information Security Arena

GIAC Security Essentials

Certification (GSEC)

Practical Assignment

Version 1.4c

Option 1 - Research on Topics

in Information Security

Marcus D. Andrews, February 18, 2005

University of Mary Washington

Abstract

As documentation requirements increase with each passing Legislative Act or new industry standard, the demand for skilled writers is growing. This paper is meant to serve as a tool to assist writers in understanding what Information Security entails and to illustrate the role of documentation in Information Security.

Table of Contents

Introduction

This paper provides a roadmap for the technical writer who is entering into the field of Information Security. A writer will be looked upon to use their skills to assist the security team with the volumes of required documentation. Whether writing security policies or incident reports, it is important that they understand that each document is a vital piece of the overall security initiative.

As federal legislation governing security increases in volume, the amount of required documentation is increasing as well. It is in the best interest of any writer to familiarize themselves with the laws and standards that are utilized in their work environment.

Technical Writing Tips

The majority of this document is dedicated to providing a technical writer with information that is useful for preparing themselves for work in the Information Security field. However, there are five steps that a writer must remember in order to be successful [1]. These steps are:

1. Preparation
2. Research
3. Organization
4. Writing a draft
5. Revision

Preparation

In order to perform any task, preparation is required to perform it well. Whether drafting an installation guide or an organization-wide policy, you must prepare yourself in order to be able to perform your duties. Some of the keys to preparation involve answering the fundamental questions of who, what, when, where, and why. These questions apply to all aspects of technical writing.

With documentation, you must quickly establish the objective of the document you are preparing. Doing this assists in gaining and maintaining the focus of your audience. Most people will not use a document if they have to search through it to find what its purpose is. This should be established at the very beginning of a document and must be done clearly and precisely.

Showing the importance of a document to your audience is another area that involves preparation. Users of the documentation must be aware of how the information contained within a document impacts them directly.

Perhaps the most important aspect of preparation is learning about your audience. You want to learn who your audience is and tailor your documentation to them. By having a thorough understanding of your audience, you can more effectively meet their needs and ensure that the documentation will be utilized and not ignored.

Research

You cannot be an effective writer if you have no knowledge of the topic on which you are writing. You must research your intended subject. If you are tasked with writing about Windows XP security flaws, you must research that topic. Whether interviewing subject matter experts, reviewing trade publications, searching the Internet, or reviewing existing documentation, it is essential that you have an understanding of the topic you are covering. This document should assist you with this task.

To be an effective information security practitioner, you must constantly be aware of the changes that occur in the field of information security. Some of the resources available to you are information security organizations, such as The SANS (SysAdmin, Audit, Network, Security) Institute (http://www.sans.org).

SANS provides many programs that can assist you in gaining knowledge of the many facets of information security. A listing of these programs with detailed information is located at http://www.sans.org/aboutsans.php. There are many other resources available to you, some of which are found in this document.

Another great research source is your organizations existing documentation. In today's environment, it is unlikely that you will encounter a system that does not have some associated documentation.

Organization

Due to the complex requirements created by federal laws and regulations, the volume and scope of documentation has grown tremendously. The documents are intended to address the many aspects of information security. While this is a daunting task, it is made easier by the fact that templates are available for almost any document that you will be tasked to create. Whether in the form of existing documentation, organizational resources (such as SANS), or federal guidelines, there are many places where you can locate templates to assist you in fulfilling your organizations documentation requirements.

Writing a Draft

No one is expected to create a perfect document on the first attempt. After you have prepared, researched, and organized your document, you should begin drafting the document. This draft document should contain as much information as possible. It serves as the unrefined culmination of everything that you have gathered and should address the fundamental requirements of the document.

The draft will help to identify any gaps between the information required in the document and what you have gathered. The draft should initially provide the "meat" of the document. The introduction and conclusion of the document should be addressed afterwards.

Even though the draft may not be pretty, it will be refined once you perform your revisions.

Revision

Revising a document involves answering many questions. Is the grammar and punctuation correct? Have any gaps in the document been filled? Is everything spelled correctly?

While these are all essential elements of the revision process, two of the most important elements that must be addressed are content and usability. Content deals with whether or not the document provides all of the information that is required of it. If the document is meant to guide a user on how to install software, does it address all of the necessary steps? If it is a document written in response to a federal guideline, it must address all of the requirements outlined by that guideline. If a document is left incomplete, it is ineffective.

Usability is an element of documentation that a writer must be extremely aware of. If a document is written in a manner that confuses a user, it is useless. As a technical writer, you will serve as the medium that takes complex data and presents it in layman terms. Knowledge of your topic and your audience are key factors that will determine whether your documentation is effective.

While there are many other elements that constitute being an effective technical writer, these five steps are the basis for them all. By adhering to these steps, you are prepared to play a major role on an information security team. To further assist you in your effort to assist the team, use the information contained in this document to expand your knowledge of information security, the laws and standards that make documentation so important, and the roles that documentation plays in information security.

Information Security

Information Security is "the process of protecting data from accidental or intentional misuse by persons inside or outside of an organization [21]." In today's connected environment, an organization, regardless of size, needs to establish and maintain a secure posture against potential threats. This can only be achieved through vigilance and knowledge. Implementing an Information Security Program fulfills this requirement.

An established model for an Information Security Program is the CIA model. CIA stands for Confidentiality, Integrity, and Availability. These objectives are covered in further detail below:

- Confidentiality addresses the secrecy of information. Information, such as financial records or proprietary software code, is not generally made available to the public, and their release could prove catastrophic to an organization's ability to conduct business. This information must be protected at all times whether it is on a server or being transmitted to an authorized user. The key to confidentiality is the ability to hide information from, and deny access to, unauthorized people.

- Integrity is the assurance that an organization's information is accurate, reliable, and unchanged. Integrity is based upon the assumption that information in an organization's possession has not been altered or contaminated while being stored or transmitted.

- Availability is the assurance that users can access their information assets. Availability ranges from users having adequate access rights to the information (access control) to ensuring that the system has adequate fault tolerance to protect against denial of service. Denial of service can occur as a result of three events: Natural (earthquakes, tornados, etc.), Intentional (hackers flooding a network with bogus data), or Unintentional (accidentally powering down a server).

Confidentiality, Integrity, and Availability are the primary goals of Information Security. However, you should be aware that another element of the security

model you should know is nonrepudiation. Nonrepudiation provides the reassurance of knowing that any data that is transmitted or received is done so by an authorized user. This has grown in importance with the advent of e-commerce and digital signatures.

Security Laws and Regulations

In an effort to combat the evolving threats faced by organizations today, a number of laws, regulations, and standards have been developed and implemented to guide organization's security practices. From these laws, regulations, and standards, organizations have developed and implemented policies, programs, and methodologies to assist them in protecting themselves from, and responding to, threats, and in conducting business.

Well-written, accurate security policies and standards stand at the center of an organizations security program. Everything that is done in a company or agency must be validated by its policies and implemented according to the established standards. They must be current, concise, and clear. As a writer, you will be looked upon to ensure that your organization's documentation meets these criteria.

Because of the large number of federal laws and regulations that deal with information security, it is not possible to discuss all of them in this document. However, some of the more prominent legislative pieces are discussed in further detail. Depending on the industry or audience your organization serves, these laws, as well as others mentioned within this document, may have a direct impact on the direction of your information security program.

Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) of 2002 [7] provides a framework designed to ensure the effectiveness of information security controls used to protect federal assets. It also provides guidance for the development and maintenance of standards for minimum-security standards.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act [20] is the product of the many large corporate corruption scandals that have shaken the country in recent years (such as Enron). It has been defined as "…a set of standards for tracking and reporting requirements intended to hold top executives' feet to the fire on corporate financial statements [2]." The Sarbanes-Oxley Act requires that public companies implement strict financial reporting and auditing guidelines along with security controls to minimize the occurrences of fraud and abuse.

Health Insurance Probability and Accounting Act

The Health Insurance Probability and Accounting Act (HIPPA) [9], passed in 1996, requires that the private health and medical data of patients must be protected according to federal privacy standards. The procedures outlined in this legislation provide enhanced protection of electronically exchanged patient data, improved patient access to their medical records, patient notification of HIPAA privacy practices, places limits on how a patient's personal medical information may be used by health providers, and also prevents a patient's information from being used for marketing purposes without their consent. Other patient protections are provided in this Act.

Security Standards

In addition to the federal laws that govern an organization's policies, security standards establish how an organization will manage its security programs.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) [14] is a non-regulatory division of the U.S. Department of Commerce. NIST provides guidance in the areas of technology, measurements, and standards.

Writers, and any other information security practitioners, should strongly familiarize themselves with the NIST 800 series of Special Publications [15]. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications.

International Organization for Standardization

The International Organization for Standardization (ISO) 17799 [12] is a "Detailed security standard organized into ten major sections, each covering a different topic or area:

1. Business Continuity Planning
2. System Access Control
3. System Development and Maintenance
4. Physical and Environmental Security
5. Compliance
6. Personnel Security
7. Security Organization
8. Computer & Operations Management
9. Asset Classification and Control
10. Security Policy"

Department of Defense Information Technology Security Certification and Accreditation Process

The Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) [6] is "a standard that provides guidance for protecting and securing the information systems that comprise the Defense Information Infrastructure."

The Systems Security Engineering Capability Maturity Model

The Systems Security Engineering Capability Maturity Model (SSE-CMM) [26] "describes the essential characteristics of an organization's security engineering

process that must exist to ensure good security engineering." SSE-CMM emphasizes security activities throughout the system life cycle.

The Role of Documentation in Information Security

"Documentation is essential to the smooth working of any security organization [3]"

Security programs require a large amount of documentation. From policies to server build configurations, the technical data that is captured in these documents not only provide management with insight into the security process, but they also enable the security team to quickly respond to problems that may arise.

Examples of some of the types of documentation that will be generated by the security team are:

- Data flows
- Disaster Recovery Plan
- Audit Logs
- Network Diagrams
- Security Policies and Procedures
- Port Scan Logs
- Access Logs
- Antivirus Updates
- Patch Schedules

"A very important aspect of network security, and one that is often overlooked, is documentation. Documentation is part of each step in the security lifecycle [3]."

This is a point that rings true in most environments. However, it is a writer's responsibility to ensure that the documentation is not neglected and is written according to the highest quality standards.

While this document does not detail every aspect of information security that requires documentation, two of the areas that rely strongly upon it are the Systems Development Life Cycle and Incident Handling.

Systems Development Life Cycle

Security is an integral part of the Systems Development Life Cycle (SDLC) and should be taken into consideration throughout the development process. The SDLC outlines the processes involved in the development, implementation, operation, and maintenance of an information system.

Some of the security documentation that may be required as part of the SDLC are:

- System Risk Assessment
- System Security Plan
- Contingency Plan
- Security Plan of Action and Milestones
- Certification and Accreditation
- Security Self-Assessment
- Privacy Impact Assessment

System Risk Assessment

The System Risk Assessment is prepared in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30,

"Risk Management Guide for Information Technology Systems [22]." Security risk assessments are performed to:

- Identify risk.
- Assess risk.
- Identify the steps to reduce that risk.

These documents will have to be maintained regularly in order to keep pace with system changes as well as emerging risks.

System Security Plan

The System Security Plan is prepared in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, "Guide for Developing System Security Plans [24]." The System Security Plan indicates what measures will be utilized in the protection of an information system and directly addresses any system vulnerabilities discovered during the security risk assessment.

Contingency Plan

The Contingency Plan is prepared in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, "Contingency Planning Guide for Information Technology Systems [23]." The Contingency Plan is used to ensure that an organization's information systems can continue to function in the event of a localized event or large-scale disaster.

The Contingency Plan should be routinely reviewed, tested, and updated regularly. Guidelines for this task can include:

- Whenever there are changes to business operations.
- Whenever there are major system changes.

- Whenever there are changes in federal (OMB, NIST) guidelines.

Security Plan of Action and Milestones

The Security Plan of Action and Milestones, also referred to as a Corrective Action Plan, is prepared in response to the Office of Management and Budget (OMB) directive that required the submission of "'a plan of action with milestones' to address all weaknesses identified by program reviews and evaluations [28]."

The most current OMB memorandum that addresses this is M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004 [30].

Certification and Accreditation

Certification and Accreditation can be separated into two major phases, certification and accreditation. Certification involves implementing, documenting, and testing the management, operational, and technical security controls of an information system. As part of this phase, some of the essential documents are:

- System Design Documentation
- Test (Function, Penetration) Documentation

Accreditation is the point in the process where a system is given one of three possible ratings:

- Authority to Operate
- Interim Authority to Operate
- Denial of Authority to Operate

An authorizing party grants authority to Operate if it is determined that a system

adequately addresses and mitigates risk. Interim Authority to Operate is granted if a system has not adequately addressed identified risks at the time of certification, but must remain in operation. This is done with the assumption that the identified risks can be mitigated in a set time frame. If a system of a federal agency fails to receive accreditation, a Denial of Authority to Operate is granted. That system can be shut down until any deficiencies are corrected. Federal agencies make every effort to ensure that this does not occur.

Certification and Accreditation is performed in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems [19]."

Security Self-Assessment

Security Self-Assessments are performed to ensure that the security controls of an information system are:

- Working properly
- Compliant with current requirements
- Utilizing current security practices

Security Self-Assessments also confirm whether the security documentation is complete and reflects any changes to the system.

Security Self-Assessments are performed in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, "Security Self-Assessment Guide for Information Technology Systems [25]."

Privacy Impact Assessment

Privacy Impact Assessments are performed to determine the vulnerability and risks associated with private, personal employee or customer information on information systems. The results of these assessments are then used to

eliminate or contain these risks and to strengthen the security of the information system.

Privacy Impact Assessments are performed in accordance with various federal laws and mandates, including, but not limited to the following:

- Privacy Act of 1974 5 U.S.C. 552a (As Amended) [17];
- Children's Online Privacy Protection Act [4];
- Health Insurance Portability and Accountability Act of 1996 (Privacy Rule, 67 FR 14775) [9];
- Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.) [18];
- Office of Management and Budget Memorandum No. M-99-18 "Privacy Policies on Federal Web Sites," June 2, 1999 [28];
- Office of Management and Budget Memorandum No. M-00-13 "Privacy Policies and Data Collection on Federal Web Sites," June 22, 2000 [29];
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, November 28, 2000 [27];
- OMB Circular A-11 (Exhibit 300) [16].

Incident Handling

Incident Handling is one area where, without question, organized, well-written documentation is essential. Incident Handling details how an organization plans to respond in the face of a security threat, natural disaster, terrorist event, etc. Having these plans in place and regularly reviewing and updating them help in ensuring an orderly and rapid response to an incident or event.

Incident Handling is performed in accordance with a number of federal laws and mandates, including, but not limited to the following:

- Homeland Security Presidential Directive (HSPD) 3, March 11, 2002 [10];

- The Federal Information Security Management Act (FISMA) (Section 3546) (Title III of The E-Government Act of 2002) [7];
- Computer Fraud and Abuse Act of 1986 [5];
- Information Technology Management Reform Act of 1996 (ITMRA) (also referred to as the Clinger-Cohen Act) [11];
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, November 28, 2000 [27];
- National Institute of Standards and Technology (NIST) Special Publication 800-61, Computer Security Incident Handling Guide, January 2004 [8].

"A great investigation can be rendered largely ineffective if the resulting documentation is subpar […] In fact, a report that is disorganized and poorly written may actually hinder the advancement of your case [13]."

If it is determined that an incident or event occurred due to illegal activity, the documentation gathered during the course of handling the incident is crucial. The facts surrounding the event must be accounted for accurately and enough information must be included to clearly show malicious intent or negligence.

Conclusion

It is my hope that the information contained in this paper serves the need of providing valuable information to not only writers, but to anyone involved with, or interested in Information Security. In order for anyone to do their jobs effectively, they must have the appropriate skills and knowledge required for their position. This paper is meant to shed light upon the resources that are available to you, and to assist you in finding them.

If you are currently tasked with grappling the mountains of documentation that this field requires, know that what you do is essential and it is important that you utilize your skills for the benefit of you security team and your organization. As your knowledge and experience grow, you will have the opportunity to branch out and perform many other vital functions. Hopefully this document can assist

you in this journey. In closing, I would like to leave you with this quote, "Whatever you are, be a good one." – Abraham Lincoln

References

[1] Alred, Gerald J., Charels T. Brusaw, and Walter E. Oliu. Handbook of Technical Writing, 6th Edition. New York: St. Martin's Press, 2000

[2] Bolles, Gary A. "Technology: Sarbanes-Oxley Comply With Me." CIO. 8 Aug 2004
<http://www.cioinsight.com/article2/0,1397,121308,00.asp>

[3] Bragg, Roberta, Rhodes-Ousley, Mark, and Strassberg, Keith. Network Security: The Complete Reference. New York: McGraw-Hill/Osborne, 2004

[4] Children's Online Privacy Protection Act
<http://www.ftc.gov/ogc/coppa.htm>

[5] Computer Fraud and Abuse Act of 1986
<http://www.usdoj.gov/criminal/cybercrime/1029NEW.htm>

[6] Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)
<http://iase.disa.mil/ditscap/DITSCAP.html>
<http://www.blackbirdtech.com/caditscap.html>

[7] Federal Information Security Management Act of 2002 (FISMA)
<http://www.csrc.nist.gov/policies/FISMA-final.pdf>

[8] Grance, Tim, Karen Kent, and Brian Kim. "Computer Security Incident Handling Guide." NIST Special Publication 800-61.
<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

[9] Health Insurance Portability and Accountability Act (HIPPA)
<http://www.cms.hhs.gov/hippa>
Privacy Rule, 67 FR 14775
<http://thomas.loc.gov/cgi-bin/query/z?c104:H.R.3103.ENR>

[10] Homeland Security Presidential Directive (HSPD) 3.
<http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html>

[11] Information Technology Management Reform Act of 1996 (ITMRA) (also referred to as the Clinger-Cohen Act
<http://www.oirm.nih.gov/itmra/itmra96.html>

[12] International Organization for Standardization (ISO) 17799
<http://www.iso17799software.com>
<http://www.iso17799software.com/what.htm>

[13] Mandia, Kevin, Prosise, Chris, and Pepe, Matt. Incident Response and Computer Forensics, 2nd Edition. New York: McGraw-Hill/Osborne, 2003

[14] National Institute of Standards and Technology (NIST)
<http://csrc.nist.gov>

[15] National Institute of Standards and Technology (NIST) 800 Series Publications (SP)
<http://csrc.nist.gov/publications/nistpubs>

[16] OMB Circular A-11 (Exhibit 300)
<http://www.whitehouse.gov/omb/circulars/a11/2002/S300.pdf>

[17] Privacy Act of 1974 5 U.S.C. 552a As Amended
<http://www4.law.cornell.edu/uscode/5/552a.html> (full text)
<http://www.usdoj.gov/04foia/04_7_1.html> (for an overview and summary of Privacy Act case law)

[18] Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)
<http://www.4law.cornell.edu/uscode/12/ch35.html>

[19] Ross, Ron, Marianne Swanson, Gary Stoneburner, Stu Katzke, and Arnold Johnson. “Guide for the Security Certification and Accreditation of Federal Information Systems.” NIST Special Publication 800-37.
<http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>

[20] Sarbanes-Oxley Act

<http://banking.senate.gov/pss/acctrfm/conf_rpt.pdf>

[21] Scalet, Sarah D. Security and Privacy Research Center Glossary. May 10, 2002.

<http://www.cio.com/research/security/edit/glossary.html>

[22] Stoneburner, Gary, Alice Goguen, and Alexis Feringa. “Risk Management guide for Information Technology Systems.” NIST Special Publication 800-30.

<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

[23] Swanson, Marianne, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas. “Contingency Planning Guide for Information Technology Systems.” NIST Special Publication 800-34.

<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>

[24] Swanson, Marianne. “Guide for Developing Security Plans for Information Technology Systems.” NIST Special Publication 800-18.

<http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF>

[25] Swanson, Marianne. “Security Self-Assessment Guide for Information Technology Systems.” NIST Special Publication 800-26.

<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>

[26] System Security Engineering Capability and Maturity Model (SSE CMM)

<http://www.sse-cmm.org/model/model.asp>

[27] United States. Office of Management and Budget. Circular A-130, “Management of Federal Information Resources,” November 28, 2000

<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>

[28] United States. Office of Management and Budget. Memorandum No. M-99-18 “Privacy Policies on Federal Web Sites,” June 2, 1999

<http://www.whitehouse.gov/omb/memoranda/m99-18.html>

[29] United States. Office of Management and Budget. Memorandum No. M-00-13 “Privacy Policies and Data Collection on Federal Web Sites,” June 22, 2000

<http://www.whitehouse.gov/omb/memoranda/m00-13.html>

[30] United States. Office of Management and Budget. Memorandum No. M-04-25 “FY 2004 Reporting Instructions for the Federal Information Security Management Act,” August 23, 2004

<http://www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf>