# Global Information Assurance Certification Paper

## System and Network Documentation


### Abstract

System and network documentation is one small part of IT documentation. Good system documentation enhances and validates security by documenting the configuration details and procedures that support a security policy. System documentation also serves as an important part of backup and disaster recovery documentation.

Good documentation must be thorough and must be kept current. Thus, updating documentation is a part of change management and many daily administration activities.

This paper has a bias towards UNIX systems, but the general concepts would apply to the Windows environment as well. The emphasis is on formal printed documentation with references to online versions and even the notes that are taped to servers and networking equipment.


### Introduction

System administration documentation is one small part of IT documentation. Unfortunately, producing quality documentation is often neglected due to higher priority work. Conversely, good documentation can also help in creating a more efficient work environment and a more stable and secure computing environment.

Some of the uses for system documentation include repeating standardized configurations, training new staff, and maintaining quality assurance.

Why should one make the effort to create and maintain documentation?

- In the security area, creating a secure infrastructure requires known, standard configurations (Limoncelli).
- Repeatability – Documentation is necessary to repeat tasks that are done well. Documentation can also help to identify tasks that need improvement.
- Audits – Documentation will be required for external or internal audits (Holtz, Patterson)
- Review – An independent review of system procedures is easier to do by reading documentation than by examining a system or conducting an interview. A review may be focused on security, efficiency, or any other aspect of system administration.
- Documentation provides the system details that are necessary in planning upgrades. Most hardware inventories do not contain information about the expandability or upgrade restrictions for any server.
- Actively protecting a system requires knowing what the system is, what the system does, how the system works, and the potential system weaknesses (Memmott).

- Documentation provides the details of the implementation of security policies and procedures.
- Documentation is necessary for daily administration, during service events, and recovery procedures (Howard, 82).
- Documentation provides a portion of disaster recovery documentation.
- Automation is used to increase our efficiency in many tasks. However, automation also reduces our familiarity with the tasks. Thus, the documentation serves to preserve knowledge.
- There are many system procedures that are only performed on rare occasions. Quickly and accurately performing many of these procedures requires good documentation. Two examples are restoring a compromised service (CERT 4) and restoring from a redundant configuration (CERT 2).
- Documentation provides knowledge of what software is security sensitive and needs to be updated regularly. This information is needed to improve system security. Details on installing updates are important since the procedures vary by package.
- Backup and recovery procedures must be documented so that multiple staff members may perform this task (CERT 3).
- Documentation provides guidance on maintaining networks and the restoration of network services (CERT 3).
- The task is not complete until it is documented (Galvin).

Security is a complex topic that requires more communication skills than traditional system administration areas. Security often crosses administrative divisions, and thus requires a cooperative effort that is aided by effective communication (Limoncelli, 161). Clearly, well-written system documentation will be a communication aid.

Documentation is not restricted to only formal printed documentation. Other forms include an online version of the printed document, online documents specific to a machine, and documents or notes that are placed near critical machines.

**Overview of IT Documentation**

Numerous policies and procedures exist to support IT operations, and a few of the more common documents are listed below.

- Security Policy
- Incident Response Policy
- Acceptable Use Policy
- Asset Inventory
- Monitoring and Privacy Policy
- Configuration and Change Management
- Software Analysis and Design Procedures
- Disaster Recovery, Business Continuity, and Contingency Planning
- System Configuration and Procedures

- Network Configuration
- Risk Assessment
- Risk Management Plan
- System Security Plan
- Certification Test Plan and Report

Several of these documents are heavily related to computer security. Depending on an organization's size, the documentation set may range from a few simple documents to many large reports. These documents may specify the existence requirements and standards for system and network documentation.

**UNIX System and Network Documentation**

System documentation includes procedures and configuration details used in the setup and maintenance of systems. The audience for system and network documentation is other system administrators and anyone conducting a security audit. The document should satisfy the goals of providing sufficient content to replicate installations and describe configurations, but the document does not need to satisfy management's sense of style and formality. Writing something that might haunt you during a job review or reflect poorly on your employer is not encouraged.

Start each chapter with a "to-do" section and end each chapter with a list of changes. The to-do section can list items that need to be documented, future systems or network plans, and policy decisions that may need to be made as details about systems are either uncovered or found to be out of compliance. A to-do section is very useful when the current documentation is weak. Alternatively, an outline could be used as guidance for future enhancements.

Naturally, the changes section will list recent modifications and new material. A version control system such as CVS or RCS can also accomplish the same task, though it is also nice to list the changes within the document itself.

Some of the information in the documentation will be obtained from system commands and utilities. If the commands are complex, the commands should be listed. Scripts that are used to provide details should also be noted. Tables or figures containing information that may get out of date should list the date the information was obtained.

The outline below is for a company that has a document repository that is publicly available through the web and hosts most of the services on Sun servers. Most of the content is appropriate for other types of businesses and users of different equipment and software.

1. Introduction
    a. Overview
    b. Related Documentation
        i. Security Policy

        ii. Acceptable Use Policy
    c. Documentation
        i. Standards
        ii. Producing the Document
        iii. Updates and Revision Control

The introduction should be a fairly short chapter. The location of files should be stated along with the processes used to produce and maintain the document. Revision control in this instance is related only to the system and network documentation.

2. User Accounts
    a. Authority for Account Creation
    b. Overview of Accounts
    c. Creation
    d. Revocation
    e. Passwords

Security aspects include system enforcement of password policies, authority to create accounts, procedure for setup and transmission of account information, and steps for terminating an account.

3. Asset Inventory
    a. Hardware
        i. The usual parameters, locations, etc.
        ii. Maintenance contracts and warranties
    b. Network
        i. Equipment
        ii. Maintenance
    c. Software
        i. Software Listing
        ii. Licensing
        iii. Maintenance and Support
        iv. Software Repositories
    d. Services
        i. Database
        ii. Application Servers
        iii. Web Servers
        iv. NFS and Samba
        v. CVS
        vi. FTP
        vii. Printing
        viii. Streaming Media
        ix. Email

An accurate asset inventory is essential. You cannot maintain software and equipment if you do not know that it exists.

4. Operating System Installation and Configuration
    a. Solaris
    b. Jumpstart
    c. Local Customizations
    d. File System Layouts
    e. OS and Disk Layouts for Redundancy

5. Network
    a. Hardware
    b. Firewall
    c. Logical and Physical Views
    d. Monitoring
    e. DNS Management
    f. Namespace Policies
    g. Contact Information

The most fundamental form of network documentation is labeling (Limoncelli, 391). Network documentation for a static environment will be easier to maintain than for a dynamic environment. Cables should be labeled only if the labels are kept correct, as no labels are better than incorrect labels.

6. Configuration and Change Management
    a. Scheduling, Planning, and Announcing
    b. System Modifications
    c. Diary
        i. Moving diary notes into the primary system documentation
    d. Software Installations
    e. Evaluation Software
    f. Production Software
    g. Software Updates

Change management is a process to ensure effective planning, implementation, and post-change testing of modifications made to a system (Limoncelli, 195). Changes must be well documented and require a back-out plan. The documentation then allows the same change to be repeated on other systems or to be used in the event of a system restore.

7. System Monitoring and Logging
    a. System logging
    b. System accounting
    c. Log Watchers
    d. Log Analysis

Several forms of system monitoring and logging will occur. Some logging occurs due to the default setup of the system. Other logging occurs based on the applications that are

installed and the degree of logging enabled. Log files can be processed for system accounting of CPU, I/O, and disk usage. Applications such as Oracle and Apache also have logs that may be analyzed.

Log watching programs can be setup to alert on security-related events and hardware failures. Another security aspect of logs is that logs provide a baseline for normal system activity. Securing a system often requires changing the default setup of system logging, and these changes will need to be replicated on nearly all hosts.

8. System and Network Security
    a. Overview
    b. Related Policies
        i. Security
        ii. Acceptable Use and Monitoring
        iii. Incident Response
    c. Backup and Disaster Recovery Issues
    d. Configuration Issues
    e. Security Patches
    f. Intrusion Detection
        i. Network Intrusion Detection
        ii. Host Intrusion Detection
        iii. File Integrity Monitoring
        iv. Log Monitoring
        v. Forensic Tools
    g. Role-based Access Control
    h. Passwords
    i. Web Security
    j. Products with Security Issues
    k. Security Resources
    l. Alerts
    m. Organizations
    n. Tools
    o. Vendor (Security) Contact Summary or refer to appendix

This chapter can be quite lengthy depending on the security requirements of an organization. The chapter is not standalone since many aspects of security may be discussed as part of the operating system installation and configuration. In this outline, the firewall is discussed in the chapter on networking, but it would be just as appropriate to include the firewall in the security chapter.

9. Software
    a. Overview
    b. Inventory
    c. Software Repositories
    d. Software Documentation
    e. Licensing

f. Media
g. Documentation Procedures and Standards

10. Backup and Recovery
    a. Overview
    b. Policies and Procedures
    c. Backup Configuration and Procedures
    d. Disaster Recovery
    e. Contingency Planning
    f. Contact Information

11. Web Services
    a. Hosts
    b. Individual configurations
    c. Reconfiguring, Starting, and Stopping
    d. Modules and SSL configuration
    e. Web Statistics, log rotation

Appendices for this documentation may include vendor contacts, security contacts, and details that are not necessary in the main body of documentation. The documentation layout will vary based on business needs and the individualism of those maintaining documentation. Certainly, there is more than one way to do it. The most important issue to have sufficient detail and match the current configuration.

**Documentation Formats and Tools**

UNIX is dominated by text-based documentation or formats that originated in text files. A good example is the numerous computer books available from publishers, many of which were produced using TeX, Troff, or similar software. Administration of UNIX is often command-line based and uses many text configuration files. By originating a document in a text format, it becomes quite easy to include configuration files, scripts, commands, and command output. In some instances, scripts can be use to generate sections of a document.

For systems documentation, printed and web formats are both desired. A printed document is easiest to read, but online documents are easier for reference as questions arise (Nemeth). Do not forget that you may not want to share system and network documentation with the outside world or even outside your work group. Therefore, assign the proper classification level to the document and protect accordingly.

Web formats include PDF and HTML. The online documentation should be generated using automated or nearly automated procedures using the same source document(s) that produced the printed documents. If producing the online version requires substantial effort, this may lead to a mismatch between the most recent version and the online version.

In the TeX arena, pdflatex will generate PDF output. Alternatively, LaTeX2HTML will generate HTML. Persons using other tools may need to generate PostScript first and then use Adobe Acrobat to produce PDF. Some people consider PDF difficult to read online. So, consider the option of generating one PDF file that is suitable for printing and another PDF file that is more suited for online viewing. The version for online viewing should have larger fonts and a shorter page length. A substantially wider page is not recommended as this may decrease readability.

Additionally, there is a need to include figures. A variety of tools exist on both UNIX and Microsoft platforms. Use whatever accomplishes the job. The only requirement is that there must be a single location in which all files related to systems documentation are maintained. This will help avoid problems when the document requires updating, but key files cannot be found.

If you feel that you can live without embedding figures in the main document, even nroff or POD could be used as the format of the source document. Figures could still be maintained as a separate attachment.

Documentation could also originate as HTML. Tools such as HTMLDOC allow better printing of HTML than can be obtained using most browsers. And, there is no law against using Word or Word Perfect to document a UNIX system. Abiword, Koffice, OpenOffice, and StarOffice now exist as capable WYSIWYG options in UNIX.

Other less formal documents exist to aid in system and network maintenance.

Network wiring must be extensively documented. Wiring should be labeled and network diagrams should be present in all wiring closets, or attached to equipment racks. Forms, paper, and pencils should be kept in wiring closets to allow network technicians to easily update diagrams and notes. Notes should later be transferred to online storage (Nemeth).

Within a machine room, servers need to be clearly labeled and should be identifiable from a distance. Server documentation also includes any notes or booklets that include architectural information or special boot instructions. As with networking, peripherals and cables need labels. Printers also benefit from similar documentation.

Another form of online documentation for systems includes notes specific to a machine and maintained on that machine. These notes include the major events in a system's life (upgrades, hardware repairs, major software installations, crashes, etc.). Evi Nemeth recommends creating a **diary** file for each machine, and even suggests creating an email alias so that the diary can be carbon copied on email among system administrators (Nemeth, 860). Some of the information added to the diary file should eventually be included in the formal documentation.

**The Documentation Process**

Creating good system and network documentation is hard. Maintaining the documentation is more difficult as most documentation efforts are considered lower priority than “real work” (Nemeth, 859). At a high level, documentation simply requires writing. The issue gets more complex as we try to integrate maintaining or creating documentation as activities are conducted. Writing after the fact does not produce the quality and detail that is desired. Often, writing well afterwards does not even get done.

Some of the information in the documentation will be obtained from system commands and utilities. If the commands are complex, the commands should be listed. Scripts that are used to provide details should also be noted. Tables or figures containing information that may get out of date should list the date the information was obtained. Files used to generate figures need to be present in the same location as the main document.

The nature of the business is that things change. As changes are implemented, the documentation needs to be updated. Processes should be defined to the extent that system changes and new system procedures will be documented in a timely manner. Formal processes do not need to be defined, and administrators should be given the flexibility to supply documentation in a manner that meets everyone’s needs.

Some of the document processes will be defined as a part of change management and revision control.

Documentation can be handwritten initially or produced electronically. Digital creation is preferred as this is much easier to incorporate into the online document. In many cases, digital creation is easy since work one can do systems work in one window and write documentation in another. Cut and paste can be used to great advantage. Eloquent prose and elaborate formatting are not necessary at this point. Formatting and revision can occur later as small document pieces are added to formal documentation.

In certain situations, documentation will be handwritten as a windowing environment or second computer is not available. For these cases, discipline is required to ensure that critical information is eventually added to the system and network documentation.

Creating good documentation is a collaborative process. The one person who really understands the system and network very well probably does not have to time to devote to extensive documentation activities. Thus, a large system and network document is often based on the contributions of several people. Collaborative activities include writing and also reviewing. The opinions of persons not producing the document can also be useful.

Given that multiple people will contribute documentation, one person can function as the master author. The master author can accept or solicit contributions and incorporate those works into the main document. Another option is to use a revision control system such as RCS or CVS that allows multiple authors. Perhaps, the same system that is

used for revision control of system configuration files can be used. Hopefully, your change management policy does mandate the use of such software.

The online document(s) specific to a machine, i.e. the diary file, are another source of information for the formal documentation. A master author needs to be informed when changes are made to the diary, or the author needs to periodically check the diary files for new notes. During such a check, it would be wise to note in the diary what information has been transferred.

Collaborative document creation software does exist, although the better options may be available only for Microsoft Windows. Web-based systems are also available. These include wiki, twiki, phpwiki, and phpprojekt, and a few people feel that some of these systems are superior to commercial options such as Lotus Notes.

The documentation needs to be maintained in at least four locations (Howard, 82). Documentation should be on the machine being documented, on backup tapes, on an unrelated computer, and as a hard copy. This allows access to the information in nearly all situations.

**Suggestions for Future Work**

1. Address system documentation from an MS Windows perspective.
2. Expand the list of documentation tools with commercial options. Eventually, good collaborative tools will exist.
3. Explore who is really doing it right. Ask Slashdot!
4. Discuss documentation standards from an audit standpoint. Consider the standards for compliance with banking regulations, HIPAA regulations, insurance requirements, or in the context of ISO certification.

**Conclusion**

Good system and network documentation is crucial to many aspects of system security and provides many other benefits to an organization.

- Documentation is required for repeating and automating installations.
- Documentation contains the implementation details that are required in security and change management policies.
- Documentation is a necessary component of disaster recovery.
- Documentation will be required for any audit, and may also be a part of satisfying banking or insurance requirements.
- Documentation preserves one source of intellectual capital in your organization and can reduce the adverse affects of staff turnover.
- Documentation can be using to educate new employees.

Remember that some documentation is much better than none. Regardless of the tools and processes used to maintain documentation, a high level of content is always preferred over a document that looks good but lacks content.

**References**


1. CERT. "Develop and promulgate an acceptable use policy for workstations." URL: http://www.cert.org/security-improvement/practices/p034.html (April 21, 2002).

2. CERT. "Establish policies and procedures for responding to intrusions." URL: http://www.cert.org/security-improvement/practices/p044.html (April 21, 2002).

3. CERT. "Develop a computer deployment plan that includes security issues." URL: http://www.cert.org/security-improvement/practices/p065.html (April 21, 2002).

4. CERT. "Identify data that characterize systems and aid in detecting signs of suspicious behavior." URL: http://www.cert.org/security-improvement/practices/p091.html (April 21, 2002).

5. Crabb-Guel, Michele, Bishop, Kensiski, Pomeranz, et. al. "The Network Security Roadmap Poster." SANS Institute. 1999. URL: http://www.sans.org/newlook/publications/roadmap.htm.

6. Galvin, Peter Baer. "Solaris Administration Best Practices." Sys Admin. April 2002. URL: http://www.samag.com/print/documentID=24672 (April 30, 2002).

7. Holtz, Gary. "Systems Security and Your Responsibilities: Minimizing Your Liability." July 23, 2001. URL: http://rr.sans.org/legal/liability.php (April 21, 2001).

8. Howard, John S. and Deeths, David. Boot Disk Management – A Guide for the Solaris Operating Environment. Sun Microsystems Press. 2002.

9. Jenkins, George. Information Systems Policies and Procedures Manual. Prentice-Hall. 1997.

10. Limoncelli, Thomas A. and Hogan, Christine. The Practice of System and Network Administration. Addison-Wesley. 2001.

11. Memmott, Falan. "The Value of Documentation: A Useful System Security Plan Template." April 21, 2001. URL: http://rr.sans.org/policy/document.php (April 21, 2002).

12. Morgan, Conrad. "A Survival Guide for Security Professionals." March 20, 2002. URL: http://rr.sans.org/practice/survival.php (April 21, 2002).

13. Nemeth, Evi and Snyder, Garth and Hein, Trent. Linux Administration Handbook. Prentice-Hall. 2002.

14. Patterson, Patrick. "Preparing for a Security Audit." November 27, 2001. URL: http://www.carillonis.com/en/publications/Preparing%20for%20a%20Security%20Audit.pdf (April 24, 2002).

15. Zeltser, Lenny. "Auditing UNIX Systems, A Case Study." August 2001. URL: http://www.zeltser.com/sans/gcux-practical/unix_security_audit.pdf (April 30, 2002).

**Additional Resources**

Abiword. URL: http://www.abisource.com.

CVS. URL: http://www.cvshome.org.

Document Version Control – A brief description of the numerous version control systems available: SCCS, RCS, CVS, Subversion, and more. URL: http://www.cbbrowne.com/info/textversion.html.

GNU RCS. URL: http://www.gnu.org/software/rcs/rcs.html.

Google Configuration Management Resources. URL: http://directory.google.com/Top/Computers/Software/Configuration_Management.

Groff. URL: http://www.gnu.org/software/groff/groff.html.

HTMLDOC. URL: http://www.easysw.com/htmldoc.

Koffice. URL: http://www.koffice.org.

OpenOffice. URL: http://www.openoffice.org.

PHP. URL: http://www.php.org.

PHProjekt. URL: http://www.phprojekt.com.

StarOffice. URL: http://www.sun.com/staroffice.

Subversion – Trying to be a better CVS. URL: http://subversion.tigris.org.

TeX User Group. URL: http://www.tug.org.

Texinfo. URL: http://texinfo.org.

Troff Resources. URL: http://www.kohala.com/start/troff/troff.html.

TWiki – A Web Based Collaboration Platform. URL: http://www.twiki.org.

WikiWeb – Web Based Collaboration Tools. URL: http://www.wikiweb.com.

Last Updated: June 24th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| Community SANS Omaha SEC401* | Omaha, NE | Aug 14, 2017 - Aug 19, 2017 | Community SANS |
| Community SANS Trenton SEC401 | Trenton, NJ | Aug 21, 2017 - Aug 26, 2017 | Community SANS |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| Community SANS San Diego SEC401 | San Diego, CA | Aug 21, 2017 - Aug 26, 2017 | Community SANS |
| Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style | Virginia Beach, VA | Aug 21, 2017 - Aug 26, 2017 | vLive |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Mentor Session - SEC401 | Minneapolis, MN | Aug 29, 2017 - Oct 10, 2017 | Mentor |
| SANS Tampa - Clearwater 2017 | Clearwater, FL | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS San Francisco Fall 2017 | San Francisco, CA | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| Mentor Session - SEC401 | Edmonton, AB | Sep 06, 2017 - Oct 18, 2017 | Mentor |