GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Information Technology Security System Engineering Methodology
David Childs
April 3, 2002
GSEC Practical Requirements (v.1.3) (December 2001)

Abstract

A methodology is described for system engineering security into large information technology systems under development. The methodology is an integration of a risk management process and a generic system development life cycle process. The methodology is to be used by Security System Engineers to effectively engineer and integrate information technology security into a target system as it progresses through the development life cycle. The methodology can also be used to re-engineer security into a legacy system.

Introduction

Most large information technology (IT) systems are made secure by performing a risk management process such as the process presented in the SANS Security Essentials Course. This process includes:

- Write a security policy
- Analyze risks, or identify industry practice for due care; analyze vulnerabilities
- Design controls, write standards for each technology
- Decide what resources are available, prioritize countermeasures, and implement top priority countermeasures you can afford
- Conduct periodic reviews and possibly tests
- Implement intrusion detection and incident response (SANS, p. 6-2).

It works well for legacy systems and can be applied to new IT systems. However, for building security into large IT systems (e.g. many hundreds of users and workstations on dozens of LAN subnets and WAN links to remote locations) under development from the ground up, additional system engineering discipline is necessary. The system engineering discipline is provided by employing a methodology. A methodology is a collection of methods, procedures, and standards that defines and integrated synthesis of engineering approaches to the development of a product (SEI, p. A-39).

The proposed methodology is an integration of the risk management process with a system development life cycle process. A generic system development life cycle process consists of these phases:

- System boundary definition
- System requirements

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Functional specification
- Preliminary design
- Critical design
- Implementation
- Verification and Validation
- System acceptance and delivery.

The proposed Security System Engineering Methodology integrates these two processes for use by Security System Engineers responsible for developing IT security in large IT systems. The methodology can also be used for re-engineering the IT security for a large IT system. Following are the steps in the Security Systems Engineering Methodology.

1. Define System Boundary
2. Perform Threat Analysis
3. Develop IT Security Policy
4. Develop IT Security Requirements
5. Develop IT Security Architecture
6. Design Security Controls, Standards, and Procedures
7. Implement Security Controls, Standards, and Procedures
8. Perform Verification and Validation
9. Perform Vulnerability Analysis
10. Perform Risk Analysis
11. Prepare Risk Mitigation Strategy
12. Authorize to Process.

The remaining sections describe each step of the methodology.

1. Define System Boundary

The first step is to define the system boundary. This delineates what is inside and outside the system. Then, determine what the system is to accomplish, that is, the mission statement. Define the intended user community and interfaces required to other systems. Identify IT resources to be included.

Finally, identify the system assets and their estimated value. System assets include facilities, network components, hardware, software, information, and trade secrets. For facilities, network components, hardware, and COTS software, the value is limited to the cost of replacing the functionality plus the cost of any time and resource impacts during downtime. For application software, the value includes replacement costs, the cost of redevelopment if applicable, and downtime costs. For information, the value is the estimated cost to retrieve or reconstruct the information plus downtime cost. For trade secrets, the value is

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the estimated cost of loss of market share. Rank the system assets by estimated value.

2. Perform Threat Analysis

The next step is to identify specific threats to system assets. Threats are events or circumstances, whether internal or external, that can harm an IT system (destruction, modification, unauthorized disclosure of information, or denial of service) (SOLAR, p.6). For each asset, starting with the largest, list all known threats to the asset. Eliminate threats from the list that are not relevant to the system's environment or organization. Do not assign probabilities of occurrence during this step. General threats (e.g. denial of service) should be diagrammed with threat logic trees to trace to more specific threats (e.g. resource exhaustion). All threats should be traced to specific threats with enough granularity to easily link to vulnerabilities identified in the Vulnerability Analysis step.

3. Develop IT Security Policy

Policies are management instructions indicating a course of action, a guiding principle, or an appropriate procedure which is expedient, prudent, or advantageous. Policies are high-level statements that provide guidance to workers who must make present and future decisions (Wood, p. 5). Developing the IT Security Policy requires understanding the system's organization structure and assigning roles and responsibilities. IT Security Policy contains high-level policy governing IT security for all system asset users. First, the policy defines the scope of the system and organization bound by the policy. In this paper, it will be referred to as the organization, and the organization is decomposed into organizational units. Next, it defines who is responsible for developing, maintaining, and enforcing the IT Security Policy. In this paper, it will be referred to as the Central Security Group. Then, the following responsibilities are specified for the Central Security Group:

- Development and maintenance of IT Security Requirements
- Development and maintenance of IT Security Architecture
- Implementation of IT Security controls, standards, (low-level) policy, and procedures
- Verification and Validation of IT security requirements, architecture, and implementation.

Next, the policy should contain the high-level security responsibilities of the organization, the organizational units, and all personnel. Finally, a waiver process should be defined.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. Develop IT Security Requirements

Requirements are statements that identify the essential needs of a system in order for it to have utility and value. Requirements may be derived or based upon interpretation of stated requirements to assist in providing a common understanding of the desired operational characteristics of a system (SEI, p. A-48). IT security requirements define the essential security needs and operational characteristics of the system and the organization.

The IT security requirements should be developed by personnel in the Central Security Group serving in a system engineering role. These Security System Engineers must work closely with the System Engineers from other organizational units as they are developing their unit requirements. The organizational units must incorporate and respond to IT security requirements. Likewise, organizational units may impose peer functional or operational requirements on IT security. IT security requirements should also be developed with input and feedback from an IT Security Working Group that includes development and operations representatives from the organizational units.

The IT security requirements should include functional requirements (i.e. what is to be implemented, not how) in each of the following areas:

- Physical Security (for critical operations areas)
- Authentication
- Authorization (Access Control)
- Confidentiality
- Integrity
- Non-Repudiation
- Audits and Alarms
- Personnel
- Procedural/Administrative.

Each requirement should be given a unique identifier (object id), a title, and a source. The requirements should be “atomic” and address only one aspect of one functional area per requirement. For example, there are many requirements about passwords, e.g. time-to-live, re-use, complexity, etc. These should all be stated as separate requirements rather than grouped together. Compound requirements are difficult to work with in later steps.

5. Develop IT Security Architecture

Architecture is the organizational structure of a system or component (SEI, A-26). The IT security architecture is the organizational structure of the security controls

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

within the system. First, the system must be decomposed into security zones based on the:

- Criticality of the functions performed
- Criticality of the data processed
- Sensitivity of the functions performed
- Sensitivity of the data processed
- Logical and physical location of high-value assets
- Architecture of the IT system.

For each security zone, starting with the most critical and sensitive, define a logical and physical (if applicable) security perimeter around the zone. Determine the required data and control flows that cross these boundaries. Specify the functional security controls (i.e. functional specification) required at each boundary to implement the security requirements. Then, specify the functional security controls (i.e. functional specification) to maintain a homogeneous security level throughout the zone and meet the internal security requirements for that level.

6. Design Security Controls, Standards, Policy and Procedures

The design step usually consists of two phases, the preliminary design phase and the critical design phase. In the preliminary design phase, IT security requirements and the synthesized functional specification (from the previous step) are mapped onto specific security controls, standards, (low-level) policy, and procedures to formulate a preliminary design. Controls, standards, and procedures are defined below. Policy has already been defined.

- Controls (also known as “countermeasures,” “security measures,” and “safeguards”) are devices or mechanisms used to regulate or guide the operation of a machine, apparatus, or system (Wood, p.6).
- Standards provide specific technical requirements. Standards cover details such as implementation steps, system design concepts, software interface mechanisms, software algorithms, and other specifics (Wood, p. 5).
- Procedures are specific operational steps or manual methods that workers must employ to achieve a certain goal (Wood, p. 6).

At the end of the preliminary design phase a series of design reviews will be held, one for each organizational unit. The Central Security Group will present it’s preliminary design and show how it meets the IT security requirements, other unit’s peer requirements, can be tested, and implemented within budget and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

schedule constraints. The other organizational units will also show how they will meet the IT security requirements in their respective reviews.

In the second phase of the design step, the critical design phase, IT security requirements and functional specifications are further decomposed to more specific functional components of security controls. Make or buy decisions are made. Draft procurements are developed and cost estimates obtained. Design specifications for components to be built are developed. Draft policies adopting standards are developed. Low-level policies and procedures are grouped into functional units. Test planning begins.

At the end of the critical design phase another series of design reviews will be held with similar goals but with much more detail and implementation planning information.

7. Implement Security Controls, Standards, Policy, and Procedures

During the implementation step, security controls are developed or procured, installed, configured and tested. Standards, low-level policy, and procedures are written and tested. As the security controls are implemented in the system test environment, policy and procedures are adapted. In most cases, security controls must be integrated or interfaced with system components in other organizational units.

7.1 Testing

The Central Security Group will be responsible for independently unit testing all security controls, standards, policy, and procedures. In addition, support must be given to other organizational units testing their subsystems that have integrated security controls. Security policies and procedures will be updated and then finalized as all organizational units finalize their operations procedures. Security controls and procedures must be fully operational and tuned for system integration and testing (i.e. the infrastructure must be ready first).

7.2 Inventory Analysis

It is imperative to maintain an inventory of IP devices within the system boundary during implementation and into operations. How can you protect it if you don't know it exists? This should be accomplished by configuration management or system administrator processes. The IP devices discovered during verification and validation testing (e.g. ping sweeps, vulnerability scans) must be compared to the inventory to ensure all devices are tested and the accuracy of the inventory. Any inventory discrepancies found should be verified and the inventory updated as soon as possible.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The inventory should identify all IP devices by a unique property identifier, make, model, operating system, patch level, IP address, function, and criticality. Criticality was defined in the Security Architecture step. The inventory must have the appropriate authentication, authorization, privacy, and integrity controls.

8. Perform Verification and Validation

Verification is the process of determining whether or not the products of a given phase of development fulfill the requirements established during the previous phase (SEI, A-59). Validation is the evaluation of customer requirements against customer needs and expectations, and evaluation of the delivered system to meet customer's operational need in the most representative environment possible (SEI, p. A-58).

The purpose of the Verification and Validation (V&V) step is to verify that the delivered system's security controls, standards, policies, and procedures meet the security requirements and that the security requirements were necessary and sufficient to meet customer's expectations. An IT Security V&V plan and an IT Security V&V Results documents are the two outputs of this step.

8.1 IT Security Verification and Validation Plan

The IT Security V&V Plan contains the plan for formal V&V of all security requirements. It should include the following information:

- Purpose and Scope
- Roles and Responsibilities
- V&V Categories
- V&V Processes
- Mapping from Requirements to V&V Types and Procedures
- Schedule
- V&V Procedures (i.e. test procedures with pass/fail criteria).

Each requirement should map to one or more V&V procedures. Each V&V procedure should have a unique identifier, a V&V method, and a V&V category (described below). The mapping from security requirements to V&V types and procedures is best expressed as a table. See the first five columns of the example below.

Reqm ID	Requirement Name	Method	Category	Number	Test Result	Compliance	Comments	Threat Level	Vulnerability Level	Risk	Mitigation

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

8.2 Verification and Validation Types

There are four V&V methods for verifying and validating requirements. They are: test, inspection, demonstration, and analysis. Each requirement's V&V method(s) should be determined based on how it can feasibly be verified. For example, requirements pertaining to contingency plans may be verified by inspection or analysis rather than test or demonstration.

8.3 Verification and Validation Categories

Requirement to V&V procedure mappings should be grouped into categories for test efficiency. Each V&V procedures should be associated with a category. Procedures within a category can be executed together to reduce coordination and scheduling. Examples of these categories are shown below:

- Vulnerability Scanning – for requirements that can be verified by automated testing of IP devices for common security vulnerabilities
- Console Audit - manual testing performed at the workstation/device console
- Policy and Procedures Audit - inspection and analysis of policy, procedures, training, and records or personnel interviews
- Physical Security Audit – physical inspection of operational computing facilities
- Negative Testing – penetration testing.

8.4 Verification and Validation Processes and Policy

V&V activities that are complex or repetitive should have defined processes documented in the V&V Plan. Policies governing V&V procedures may be necessary also. Examples of processes are:

- Vulnerability scanning process that specifies how scans are coordinated and scheduled with operations personnel; how the scans are performed; and how the results are analyzed, reported, and preserved.

- Vulnerability scanning policy could specify the scanning tool type, version, and rule set to be used in each type of testing; that there would be no denial of service testing on critical systems supporting operations; and who has authorization to see scanning test results.

The process for conducting V&V procedures and reporting V&V results should be defined. The procedures are executed by testers identified in the V&V Plan Roles and Responsibilities according to the plan's schedule. The process should also define how the large amount of result data is to be aggregated, summarized, and reported across organizational units.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

8.5 Vulnerability Scanning

The vulnerability scanning of a large, geographically dispersed, operational system is at best a difficult proposition. The following procedure has been effective. For a given organizational unit:

- Identify the unit's points of contact, for example, the Operations Chief and the Lead System Administrator
- Identify all devices and subnets to be scanned from inventory
- Choose the network entry point for scanning device
- Coordinate with the points of contact for a window of opportunity
- Notify all stakeholders of the scheduled activity
- Conduct vulnerability scan
- Verify all devices scanned, reschedule for missed devices
- Perform sanity check on scan results
- Transfer scan reports (considered sensitive data) to central Security Group

8.6 Verification and Validation Procedures

V&V procedures should include the following:

- Unique identifier
- Title
- Requirements to be verified
- Purpose, with enough detail for a tester to execute
- Procedure
- Pass/fail criteria
- Results
- Comments.

The procedures should be formatted on a paper or electronic form suitable for efficient completion by testers and also archival.

8.7 Verification and Validation Results

The V&V results are reported in an IT Security V&V Results document. It contains summary results of execution of all V&V procedures for all security requirements and any additional V&V activities conducted, for example penetration testing.

As each V&V procedure is executed, the results are documented on the test procedure in its paper or electronic form. These are not included in the results document, but are archived by the Central Security Group for the required amount of time. The results of each procedure are summarized as a continuation of the table in the V&V Plan. See Columns six, seven, and eight in the example

Reqm ID	Requirement Name	Verification Method	Category	Number	Test Results	Compliance	Comments	Threat Level	Vulnerability Level	Risk	Mitigation

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

below.

The Test Result (Column six) values are either Pass, Fail, or Partial meaning the requirement was met, not met, or partially met respectively. For large systems, the results may vary across organizational units and need to be tracked by unit. Therefore, there may be multiple entries in test results. Compliance (Column seven) may be used to shown actual result values (e.g. 35 fails out of 546 systems) or a percentage failure or success. This is useful for giving management a feel for the scope of an unmet requirement. Comments (Column eight) may used to track the responsible tester, test date, and other notes.

The table of results is then summarized in a requirements compliance report which specifies:

- Total number of IT Security Requirements
- Number of requirements not tested
- Number of requirements met
- Number of requirements partially met
- Number of requirements not met.

Any additional verification activity results can be documented as Appendices in the V&V Results document.

9. Perform Vulnerability Analysis

A vulnerability is a weakness in an IT system that can be exploited to compromise or violate security processes or controls (SOLAR, p.8). The unmet and partially met security requirements from the V&V results are considered system vulnerabilities. Each vulnerability is assessed from an operations, development, and security perspective to determine if it is a false positive, caused by a required operations configuration, or needs to be fixed. The false positives are documented and removed from further consideration. The remaining vulnerabilities are assigned a qualitative value indicating potential damage or consequences to the system. The values are shown in the table below (SOLAR, p. 12).

Vulnerability Level	Vulnerability Level Definitions (Consequence/Damage)
0	The impact is negligible or the system is not vulnerable to this particular threat. At this point, the analyst may drop from the list any impacts evaluated at 0.
1	The impact is slight. At this value, the impact is so slight that the analyst may recommend that the manager consider accepting the risk.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2	The impact is moderate. An impact of this magnitude must be accounted for in the overall security solution.
3	The impact is great. If this vulnerability is exploited, an impact to the system's mission will occur. This impact must be accommodated by proper controls.
4	The impact would be catastrophic. It is imperative that this impact be specifically accommodated in system security processes and controls.

The vulnerability level is recorded in the V&V Results Table in Column ten as shown in the example below. When the test result is Pass (i.e. the requirement is met), the vulnerability value is 0.

Reqm ID	Requirement Name	V&V Method	Category	Number	Test Result	Compliance	Comments	Threat Level	Vulnerability Level	Risk	Mitigation

The vulnerabilities to be fixed are further analyzed from each of the operations, development, and security perspectives to determine if the fix requires a minor configuration change, a lien, or a waiver. Some minor configuration changes can be introduced into operations after appropriate testing without waiting for a full development cycle and delivery of the next operations version. Most vulnerability fixes are liens that have a task description, impact, priority, and date of completion. Liens must be negotiated with appropriate development and operations organizational units. Vulnerabilities that cannot be fixed because a certain configuration is required for system operations or there is no budget/schedule available require a waiver. During this step, the vulnerability fixes are just proposals. The assessment is recorded in Column twelve, Mitigation, in the example above with values N/A (false positive), lien, or waiver. The final resolution comes later in Risk Mitigation.

10. Perform Risk Analysis

The next step is to perform a risk analysis by qualitatively assessing the risk for each identified vulnerability. A qualitative risk value is determined using the following relationship between threat and vulnerability:

Risk = Threat X Vulnerability,

where risk value is the product of the estimated probability of occurrence of a threat and the estimated value of the damage to the system. Specific threats

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

were identified in the Perform Threat Analysis step. Now, each threat must be given an estimated probability of occurrence relative to the identified vulnerabilities. The threat occurrence values are shown in the table below (SOLAR, p. 11).

Threat Level	Threat Level Definitions (Possibility of Occurrence)
0	The threat is not viable. Threats assigned a probability value of 0 may be dropped from the list at this point.
1	The threat is viable but is not likely to occur. The probability of the threat actually occurring is low
2	This threat is not only viable but likely to occur. The probability of the actual occurrence of the threat is moderate.
3	The threat is significant, and it is imperative that it be considered in the risk analysis. The probability of the actual occurrence of the threat is high.
4	The threat is certain to occur. This threat must be accommodated in the security controls.

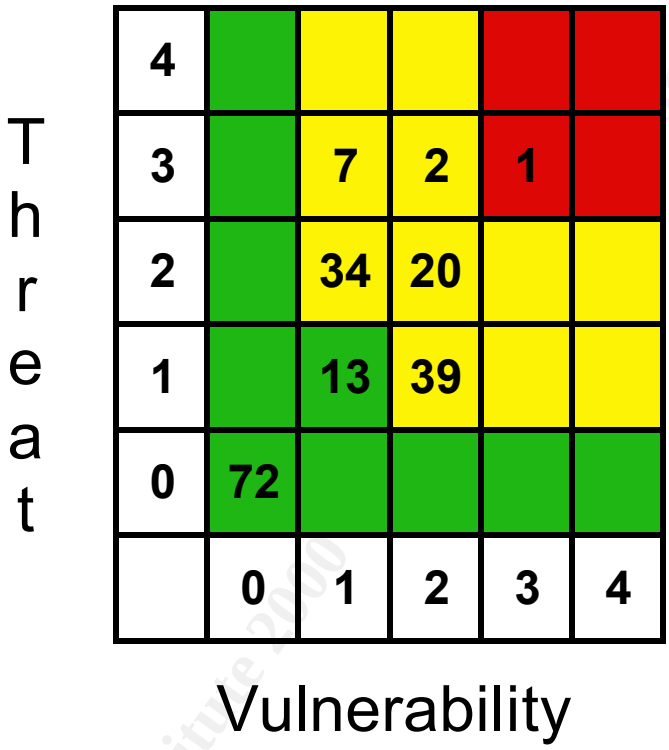
For each vulnerability in the V&V Results table, assign a threat value and calculate the risk value. Record these values in Columns nine and eleven as shown in the example below.

Reqm ID	Requirement Name	Method V&V	Category V&V	Number	Test Result	Compliance	Comments	Threat Level	Vulnerl Level	Risk	Mitigatio

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The V&V Results table is then sorted first on the Risk Column in descending order and second on the Vulnerability Level Column in descending order. The highest risk vulnerabilities will end up at the top of the table with 16 being the maximum risk value and 0 being the lowest. The risk values are then tallied up and presented in a Cumulative Risk Matrix as shown below.



Cells in the matrix are assigned colors based on the risk posture for the system. Green is used for cells of no (i.e. security requirements met, vulnerability equals 0) or low risk. These vulnerabilities will be fixed and risk mitigated on a best efforts basis. Yellow is used for moderate risk. These vulnerabilities must be fixed over time, but the risks usually are mitigated in the short term by perimeter security controls, policy, or procedures. Red indicates high risk and vulnerabilities that must be fixed immediately. The numeric value shown in each cell is the count of risk values in the V&V Results table with the given threat and vulnerability values.

11. Prepare Risk Mitigation Strategy

In the previous steps, the risk value and a proposed risk mitigation was assigned for each vulnerability in the V&V Results table. The risk mitigation is either a minor configuration change that will eliminate the vulnerability, a lien that when

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

completed will eliminate or reduce the risk, or a waiver that leaves the vulnerability and the risk in place (i.e. no risk reduction). For the high and medium risk vulnerabilities, the planned risk mitigation must be reviewed with technical and management personnel from the development, operations, and security of the organizational unit.

Agreement must be achieved on a test and deployment schedule for minor configuration changes. Upon agreement, commitment of resources, and scheduled deployment the vulnerability value goes to 0, along with the risk value.

Liens must be approved by the Central Security Group and management of the organizational unit. The approving manager must have budget and schedule responsibility and authority over the entire organizational unit. Liens require a commitment of resources, scheduled deployment, and priority from development and operations of the organizational unit. In some cases, the lien is against the Central Security Group to deploy a security control, standard, or procedure. Approval of a lien indicates acceptance of risk for a definite period of time.

Liens should be documented on a standard form, given a unique identifier, and include all the approving signatures. The lien forms (paper or electronic) should be retained in a secure repository. The Central Security Group should review the lien status periodically and update the risk analysis as changes occur.

Waivers are similar to liens except that the risk acceptance is for an indefinite period. Therefore, waivers must be approved by the management of the organization in addition to the organizational unit management.

12. Authorize to Process

The final step is giving the organizational units authorization to process. This is accomplished by the Central Security Group conducting a formal review with the organizational and unit management to present the results of the V&V, Vulnerability Analysis, and Risk Analysis. All liens and waivers must be approved prior to the review. The Cumulative Risk Matrix is presented and any high-risk vulnerabilities are described with the associated mitigation plan. If the organization management is willing to accept the cumulative risk, they will sign an authorization to process and the system is approved for transition to full operations. If the risk is not acceptable, the Central Security Group will coordinate another iteration starting at the Vulnerability Analysis step.

References

NASA, AO/Chief Information Officer, “NASA Automated Information Security Handbook,” NHB 2410.9A, June 1, 1993.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

NASA, AO/Chief Information Officer, "NASA Procedure and Guidelines Security of Information Technology," NPG 2810.1, August 10, 1999. http://www.c4i.org/NASA/

NASA, SOLAR, "Managers Responsibility for ITS Risk Management," https://solar.msfc.nasa.gov:443/ so…c/its/private/mrm/html/mrmiden.htm (June 11, 2001).

National Security Agency, Systems and Network Attack Center, "The 60 Minute Network Security Guide," Version 1.0 October 16, 2001. http://nsa2.www.conxion.com/support/ download.htm

SANS, "Risk Management The Big Picture – Part VI," GIAC Security Essentials Course, SANS, 2001.

Software Engineering Institute (SEI), Carnegie Mellon University, "A Systems Engineering Capability Maturity Model," Version 1.1, November 1995. http://www.sei.cmu.edu/pub/documents/95reports/pdf/mm003.95.pdf

United States General Accounting Office, Account and Information Management Division, "Executive Guide – Information Security Management," GAO/AIMD-98-68, May 1998. http://www.gao.gov/special.pubs/ai9868.pdf

United States General Accounting Office, Account and Information Management Division, "Information Security Risk Assessment," GAO/AIMD-99-139, August 1999. http://www.gao.gov/special.pubs/ai99139.pdf

Willson, Nigel and Blum, Daniel, "Network Strategy Methodologies & Best Practices – Security Project Cookbook," The Burton Group, Version 1, August 14, 2001.

Wood, Charles Cresson, "Information Security Policies Made Easy," Houston, Pentasafe, May 2001, 5-22.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	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	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	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 Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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 Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event