Global Information Assurance Certification Paper

Andy R. Newton
May 17, 2001
GSEC Practical Assignment Version 1.2d
Course material taken in Raleigh NC

A high level implementation of an Information Security Assurance(ISA) process for security certification of business sensitive and critical systems.

Overview

The Security Certification process serves as a formal review process to ensure that adequate security controls are incorporated into systems under development or being integrated as in the case of Commercial Off The Shelf (COTS) products. Security Certification should apply whether the system is a complete computer system with networking capability with its own hardware or infrastructure. It should also apply to new application or COTS product to be run on an existing platform or infrastructure.

The Security Certification process should be based on company policy that has been approved by management. The process can be view as a vehicle to implement existing organizational policies by providing a methodology for IT personnel, contractors and system owners to follow when building information systems.

Methodology for Implementation

In order for an ISA process to be successful, an organization must create strong policy in support of ISA. Not having a written policy in place with senior management support will doom an ISA process to failure. The policy must be specific and specify which internal business areas and organizations are subject to ISA. The policy should address business partners such as contract development organizations and outsourced production hosting facilities. A comprehensive policy should include administrative sanctions for anyone who avoids the ISA process when building systems.

If a company wide data classification policy is in not place, one should be developed as part of ISA policy. Without knowing the sensitive or criticality of data in an organization, an ISA process will be ineffective and will defeat the purpose of security certification. System owners should be responsible for data classification.

Funding

Internal system owners are responsible for adequately funding and budgeting for security for each projects. This includes the cost of completing, testing and implementing security requirements. They are responsible for the security of their systems.

The cost and benefits of security should be reviewed to ensure that the cost of controls do not outweigh expected benefits. Security should be concerned with mitigating instead of totally eliminating risk. It should also be proportionate to the sensitivity, criticality and extent of potential harm. For example, it would not be cost effective to implement a

control costing Eighty Thousand Dollars on a sensitive system that cost Twenty Thousand to build. Other options such as risk transfer through purchase of insurance may be a better option.

Certification
Security Certification is the comprehensive review of the security aspects of a system to determine the extent to which a system meets its security requirements. It's a process that produces a technical opinion with supporting documentation. The resulting documentation is used by the accreditor in making a decision whether or not to accredit a system. Before a system is accredited, the accreditor will need accurate information about a system on which to base a decision. This information includes likely threats or vulnerabilities that may compromise the system, the specific portions of the system or data, which need protection, the mechanisms used to provide protection, and how well those mechanisms operate. This is the goal of certification .

Accreditation
Security accreditation is the official management authorization to operate a system. The accreditor's role is to review the certification packages consisting of completed requirements, the certification report and make a recommendation to the system owner as to whether a system meets the company's security standards for operation in production. The accreditor may consult with subject matter experts as part of the decision making process in accrediting a system.

Acceptance
The last step in the accreditation process is for the system owner to accept the system for production. The system owner is the internal organization or department that funded the development of the system. At this stage, the system can be accepted as is and placed in production or be rejected because it does not meet expectations in which case necessary modifications will have to be made. The acceptance decision should be communicated to the accreditor in writing.

Certification Core Team
Several individuals make up the Core Team for systems undergoing development, integration or enhancement. The purpose of this team is to define security requirements, identify security issues, and ensure that problems are corrected early when cost is lower. The team should be formed in the definition phase of the system lifecycle. Forming a team late in a system life cycle may increase project cost as it's more expensive to retrofit security into a system after the fact . The core team could be dissolved when the system moves to production. The following adhoc titles are recommended for core team members:

A. Security Officer

B. System owner's Representative

C. Project Manager

D. Development Team Security Representative

E. Subject Matter Experts as needed

Role of Team Members

The Security Officer is the leader of the core team and is responsible for Chairing team meetings, providing security expertise to the team, writing the certification report.

The System owner's Representative is responsible for resolving administrative project issues such as funding, staffing, contract, privacy and legal issues. This individual can also serve as a communication channel to the system owner. This channel could keep the system owner abreast of potential show stoppers as they occur so that they my be resolved well before the production phase of the system lifecycle.

The Project Manager must ensure that the defined security requirements for the project are included in the system project plan. Each requirement must be tracked and any requirement not being met or implemented must be escalated to the core team members for review and resolution. Prior to each team meeting, the project manager must provide a copy of the updated project plan to the team and be prepared to explain any deviation from the plan.

The Development Team Security Representative role is to brief the project team on security awareness issues, complete the security requirements, ensure that security is embedded into the system, conduct security testing and report security incidents to the core team. The system owner should fund this individual's time.

Phases of the ISA Process with Possible Requirements

Phases		Requirements
Definition	System Overview	Business Needs Statement
		High-level System Description
		System Project Plan
		Definition of Roles and Responsibilities
		Data Classification
Definition	Personnel Security	Security Clearances (if needed)

Phases		Requirements
		Security Awareness and Training
		Separation of Duties
Design	Physical and Environmental Controls	Facility Risk Analysis
		Data and Asset Controls
		Secure Location of Information Resources
		Environmental controls
Design	Risk Management	Risk Management Program
		Risk Assessment
		High Level Architectural Diagram
Development	Software and Hardware	Software licensing & inventory procedures
		Encryption of sensitive data
		Use of Cookies
		Use of Active Content or CGI Code
		Database Security
		Change, Configuration and Version Control
		Data Integrity Controls
		Virus Protection
		Security Code and Application Review
		COTS Vulnerability and Test Plans
		Server Hardening Procedures
Development	Logical Access Controls	System Audit and Logging
		Account Management Procedures
		Identification and Authentication
		Ability to restrict access based on least privilege
Development	System Operations and Management	Detailed System Architectural Diagrams
		Inventory Baselines
Development	Network, Communications And Incident Management	Remote Access Controls
		Secure Network Parameter
		External Connectivity

Phases		Requirements
		Procedures for incident detection, response, containment and recovery
Development	Business Continuity Planning	Contingency Plan
		Data and System Backup and Recovery Procedures
		Disaster Recovery Plan (DRP)
Testing		System Security Controls
		Penetration Testing and Vulnerability Scans
		System Backup and Recovery Procedures
		Disaster Recovery Plan
Production		Monitor laws and organizational Policy changes that may require system changes
		System Recertification
		System Retirement/Data Disposal

Summary

A successful Information Assurance Program must be based on a company's policy that has been approved by senior management. The policy could have administrative sanctions for individuals who avoid the program when building systems. Provisions should be made for reaccreditation of systems based on policy criteria. The ISA program must be adequately funded and one way to achieve this is for each project to budget for security as part of project cost.

References

1. **Information Security Management Hand Book 4th Edition by Harold F. Tipton and Micki Krause.**

2. **FIPS PUB 101, Guidelines for Lifecycle Validation, Verification, and Testing of Computer Software, June 1983.**

3. **FIPS PUB 73, Guidelines for Security of Computer Applications, 1980.**

4. **Generally Accepted Principles and Practices for Securing Information technology Systems, by Marianne Swanson and Barbara Guttman, NIST 1996.**

5. **Web Security & Commerce by Simson Garfinkel with Gene Spafford, June 1997.**

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	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 Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS