Global Information Assurance Certification Paper

Roopangi Kadakia, Assignment Version 2.0

Collaborative Security Strategies in an Outsourced, Cross-Agency Web System

Introductions

As more and more system management is outsourced in government, new challenges are faced in creating a security management framework that meets the rules and regulations of government and policy controls. Creating collaborative, cross-agency, cross-government systems that rely on innovative ways of managing a security program further complicates this type of system. This analysis will look at the Certification and Accreditation models, Risk assessment frameworks, and risk management strategies, which can be used in combating new challenges in existing processes and standards.

This discussion will bring together different frameworks and discuss how to integrate different methodologies to create a comprehensive and complete security management system that meet each systems unique needs. I will bring together standard and commonly used functionalities and discuss how in a collaborative, outsourced, cross-agency web system, unique and integrated solutions are providing protection strategies for comprehensive security management.

Certification and Accreditation

Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources[1] requires Accreditation for an information system to operate based on an assessment of management, operational, and technical controls. The security plan documents the security controls that are in place and are planned for future implementation.

One must first determine which certification and accreditation process to follow. The major methodologies include NIACAP (National Information Assurance Certification and Accreditation Process), DITSCAP (DOD Information Technology Security Certification and Accreditation Process), NSTISSI (National Security Telecommunications and Information Systems Security Instructions, FIPS 102 (Guideline for Computer Security Certification and Accreditation), DODI (Department of Defense Instruction) and the D/CID (Director of Central Intelligence Directive). For the purposes of this discussion, the focus will be on the FIPS 102 and the NIACAP, which are standard methodologies for unclassified, civilian agency systems.

Each of the Certification and Accreditation (C&A) methodologies have common activities to establish standard processes and each have a different level of stringency in evaluation criteria dependant upon the sensitivity of the domain in which the system resides Some of the other differences include what documentation is required, what steps are performed to authorize the operation of the system and what resources need to be allocated to achieve accreditation.

The FIPS 102[2] was published on September 27th, 1983. This is a comprehensive guide that not only shows how to establish a C&A program but also how to perform a full C&A. This is a 6-step approach that includes Planning, Data Collection, Basic Evaluation, Detailed Evaluation, Report of Findings and Accreditation.

The NIACAP[3] was published in April 2000. It consists of a 4-phase approach: Phase 1 is Definition, which includes agreement on the security requirements, boundaries, schedule, level of effort and resources required. This phase includes the formulation of the SSAA (System Security Authorization Agreement) document. The 2nd phase is Verification and it verifies the evolving or modified systems' compliance with the information in the SSAA. Phase 3 validates the compliance of the fully integrated system with the security policy and requirements stated in the SSAA. This phase produces the required evidence to support accreditation by the DAA (Designated Accreditation Authority). Finally, phase 4 ensures secure system management, operation and maintenance to preserve an acceptable level of residual risk.

Both C&A process models establish standards for technically evaluating a system for security and the management of security posture of the system throughout its life cycle. They both also establish similar participation roles for key stakeholders. The NIACAP is based around the agreement between the accreditor, the program manager, the certifier, and the user. In FIPS 102, the roles are the accreditor, the program manager, the certification manager and the evaluator. The roles are defined and the documentation required is an evaluation report that contains the technical security recommendations and is used to decide on the accreditation. In both models the accreditor has basically the same responsibilities. This individual(s) accepts the security responsibilities for the system, and has the ability to allocate resources. The NIACAP Program manager is responsible for system acquisition and development. While the FIPS Program manager is responsible for the defining and managing the security program within an agency. The NIACAP certifier is a combination of the FIIPS 102 certifier and evaluator. They provide the independent security technical evaluation. The NIACAP also includes a user representative for the operational interest of the system.

I believe streamlining the C&A process, performing independent evaluations, and creating a formalized, ongoing advisory function can add better security management practices to the C&A methodology. I propose that C&A should consist of thoroughly documented Security Plan as specified in NIST Special Publication 800-18 that incorporates everything from operational, management and technical controls to a comprehensive contingency plan, an independent security risk evaluation to formulate the foundation for risk management, a fully independent security audit and accreditation by the senior executive of the system.

One unique feature is the creation of a security advisory board. This consists of policy makers and security experts that can advise on accreditation. This is key, since buy-in at multiple levels is necessary to facilitate full functionality of the system. The security

advisory board consists of members of the agencies that are most effected by the system or representatives that can have the greatest impact on security policy and the allocation of resources.

The security plan is the foundation of the comprehensive system. A good starting point is the NIST Special Publication 800-18[4]. The first step is defining the boundaries of each system. This can be especially complicated when there are numerous outsourcing partners and contractors. Once the boundary is defined, it becomes clear which Memorandums of Understandings need to be formulated and where inter-agency agreements must be defined. This discussion will not fully analysis the security plan since the guidance in SP800-18 is comprehensive.

Risk Assessment Frameworks

Next, the risk assessment framework has to be identified. We will examine three different frameworks. Each of the three discussed below have different methodologies and can provide a technological vulnerability assessment. The differences between the three methodologies are cost, assessment scope, and third-party validation needs.

INFOSEC assessment methodology (IAM)[5] is a detailed and systematic way of examining system vulnerabilities. Experienced National Security Agency (NSA) Information Security (INFOSEC) assessors developed this framework. The IAM examines the mission, organization, security policies and programs, information systems, and the threat to these systems. The goal is to determine the vulnerabilities of information systems and recommend effective low cost countermeasures. This entails providing an exit briefing on the assessment process findings and recommendations to senior leaders in the organizations with the follow-up of a written report. The methodology is carried out by a team that is required to maintain a high-level of proficiency within the INFOSEC field, remaining state-of-the-art with technological advances, and be prepared to participate in joint support calls for crisis and/or contingency situations. The teams may be required to develop and provide training/assistance to those organizations that continually update data resulting from assessments.

Carnegie Mellon University's Software Engineering Institute (SEI) has created the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)[6]. It is a self-guided assessment that is conducted in three phases, each of which has outputs that are immediately applicable. This methodology takes advantage of knowledge from multiple levels of the organization and is implemented in a series of short workshops focusing on key organizational areas to: Identify critical assets and the threats to those assets; Identify the vulnerabilities that expose those threats; Develop an appropriate protection strategy for the organization's mission and priorities. The activities are supported by catalogs of practices, surveys, and templates designed to elicit and capture information during focused discussions and problem-solving sessions.

The National Institute of Standards and Technology (NIST) has published the Information Technology Security Assessment Framework[7]. This framework provides a

methodology for agencies to determine the security status of their assets, programs, as well as the entire agency. The framework will also assist agencies in prioritizing efforts for improvement. It gives the Federal government a standard by which to measure and to improve security programs across government. The framework does not create new security requirements but provides a vehicle to consistently and effectively apply existing policy and guidance.

Each framework is based on the SEI's Capability Maturity Model (CMM). The CMM is based on quality processes and methods used to develop software systems. Choosing the appropriate assessment framework requires decisions in how much to spend, who will perform the assessment and what other information is needed to create strategic protection of the systems. The IAM framework may cost two to three times the cost of OCTAVE or the NIST Assessment Framework. If independent validation is an important outcome, then options may be limited.

Let us look at a brief case study of how to determine what framework to implement. After conducting a thorough analysis of these three frameworks, we proposed a unique framework that was a hybrid OCTAVE with some consulting services from SEI. The IAM framework is too rigid and too focused on the technical vulnerability assessment. The NIST framework is a self-directed methodology that cam only work if the government organization has the required security skill set. Also, a self-directed assessment may not give the objective, independent validation of your security practices. In this case, the OCTAVE had a very balanced technical and management methodology that was conducted by SEI for the independent validation. One of the most interesting parts of the OCTAVE is the protection strategies that are formulated for all the systems. These can help guide how to mitigate risk and also will help in creating future enhancements to those systems. More about protection strategies will be discussed in the next section.
It is important to note that this was the framework selected for this system because it fit well with the technical and management needs; however, another system may have used another framework that fit its needs better.

Risk Management
Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. NIST Special Publication 800-12, An Introduction to Computer Security and NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems are two documents that discuss risk management.

Using the five principles of risk management identified by the General Accounting Office (GAO), we can analyze a collaborative risk management program[8]. The first principle is to assess risk and determine needs. This can include classifying resources by criticality and sensitivity, identifying authorization, establishing physical and logical controls, monitoring access, investigating violations, and taking actions. This process will identify protection strategies that can significantly help in managing the risks. Protection strategies are developed from the assessment of identified risks, current

vulnerabilities, and existing security practices. Some of the areas that these can be in are institutional knowledge, security management, security strategy, security policies and regulations, collaborative security management, physical security, contingency planning & disaster recovery, incident management, monitoring and auditing, system and network management, authentication and authorization, encryption, and security architecture and design.

The second principle is to establish a central management focus. This is especially true in an outsourced environment. The responsibility for security can never be outsourced and this creates a very important role for central management and the creating of a trust baseline. As more and more contractors and partners gain security responsibilities, the need to establish a specific trust baseline becomes important. This trust baseline gives all players standards and a foundation to start their security management programs.

The third principle is to implement appropriate policies and related controls. A current and comprehensive set of policies is mandatory for an effective security management program. Key staff and also the security advisory group supports these policies.

The fourth principle is promoting awareness. Involvement through defining, developing, implementing and evaluating phases by key management and security people is crucial. These phases are the phases described in many of the C&A methodologies. During the initiation phase, a sensitivity assessment should be conducted that is based on the high level of integrity and availability required of the system. In the development/ acquisition phase, the security requirements should be identified and the appropriate security controls and associated testing procedures should be developed based on industry best practices. During the implementation phase, completion of the certification and accreditation activities is performed including an independent security audit. Authorized processing allows Certification and Accreditation (C&A) activities and documentation ensures and demonstrates that the appropriate security controls are in place and performing as expected. This is a key role that the security advisory group can play when inter-agency collaboration is crucial in maintaining effective secure systems.

The fifth principle is to monitor and evaluate policy and control effectiveness. A dedicated fulltime position with full management support can evaluate:

a) Assessment process and frameworks
b) Audit protocols
c) Security and partnership agreement
d) Technology integration and security implications
e) New enhancements and security implications
f) Certification and Accreditation
g) Cross agency (cross government, etc.) collaboration and implications on security

We believe that a comprehensive security management program must be an ongoing

process. We have developed a quarterly evaluation model where assessment activities are performed every quarter. This is especially important for web systems. Since, these systems are continuously changing, the management and assessment process must happen simultaneously.

Conclusion

Information security depends on the ability to implement a security policy that provides Availability, Integrity, Authentication, Authorization, Privacy, and Non-repudiation. Since time to deployment is becoming shorter and shorter, the security management system must be thought out completely and standards must be determined as completely as possible prior to development. So, that when a new application or functionality must be deployed, the development cycle and security requirements cycle can be synchronized. This is complicated by cross-agency direction that needs to be taken into account in the development and integration process. An integrated and hybrid risk assessment and management approach can give a comprehensive framework to securing systems. In government, the rules, regulations and guidelines issued by OMB, NIST and GAO can help define sound methodologies in creating an effective certification and accreditation methodology that takes into account the unique challenges of government, outsourcing, cross-agency collaboration and a short deployment environment.

References

1. **Appendix III to OMB Circular No. A-130: Security of Federal Automated Information Resources (28 Nov 2000).** ***Office of Management and Budget at the White House*****.** http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html **(07 Aug 2001).**

2. Federal Information Processing Standards 102 (Sep 1983). Guidelines for Computer Security Certification and Accreditation. *National Institute of Standards and Technology*. http://csrc.nist.gov/publications/fips/index.html (07 Aug 2001).

3. National Security Telecommunication and Information Systems Security Committee No. 1000. (2000). National Information Assurance Certification and Accreditation Process. http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf (Apr 2000).

4. Swanson, M. (Dec 1998). Special Publication 800-18: Guide for Developing Security Plans for Information Technology Systems. *National Institute of Standards and Technology: Computer Security Special Publications*. http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.doc (07 Aug 2001).

5. National Security Agency: Information Security Assessment Methodology. *National Security Agency: Information Assurance Directorate*. http://www.nsa.gov/isso/iam/index.htm (07 Aug 2001).

6. Alberts, C. and Dorofee, A. (Jan 2001). An Introduction to the OCTAVE Method. *Carnegie Mellon University, Software Engineering Institute, CERT Coordination Center.* http://www.cert.org/octave/methodintro.html (07 Aug 2001).

7. Swanson, M. (2000). Self-assessment Guide for Information Technology Systems Draft. *National Institute of Standards and Technology.* http://csrc.nist.gov/publications/drafts/SelfAssessmentGuideITSystems-Review.doc (9 Mar 2001).

8. Information Technology Laboratory Bulletin. (March 1998). Management of Risks in Information Systems: Practices of Successful Organizations. *National Institute of Standards and Technology: Information Technology Laboratory*. http://www.itl.nist.gov/lab/bulletns/archives/mar98.htm (07 Aug 2001).