COVER SHEET
21st National Information Systems Security Conference Call for Papers and Panels

Type of Submission: Paper

Title: The Benefits of Applying the DoD Information Technology Security Certification and Accreditation Process to Commercial Systems and Applications

Abstract: With the rapid expansion of electronic commerce and other Internet-based services, commercial systems are being exposed to increased threats from electronic intrusion, denial-of-service, and other attacks from outside sources. As a result of this threat, security certification and accreditation of these systems is of paramount importance to ensure that a company's investment and livelihood is protected from all manners of attack.

As a result, commercial systems would benefit from the application of a life-cycle Information Technology (IT) Security (ITSEC) management approach. Unfortunately, many commercial companies do not have the necessary processes in-place to ensure that life-cycle security management is applied to their automated information systems, networks, and applications. However, there is an established life-cycle security certification and accreditation process currently being used to assure the integrity of critical military IT assets. Proper application of the standard procedures currently used by the Department of Defense (DoD) could greatly enhance the overall security and integrity of commercial IT systems.

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is the standard process for security certification and accreditation of IT systems used by DoD and its contractors. This process stresses the importance of a life-cycle management approach to IT Security and focuses on protecting DoD systems through an infrastructure-centric approach for certification and accreditation. Given the similarities between the security needs DoD and commercial IT systems, this paper explores the benefits that commercial companies would derive by applying the approaches and disciplines defined by the DITSCAP to their IT systems.

Authors: Gerald L. Oar and Robert H. Jackson

Organizational Affiliation: SphereCom Enterprises Inc., 7900 Sudley Road, Suite 208, Manassas, Virginia 20109

Phone Numbers: Voice - (703) 361-0808, Fax - (703) 361-0384

E-Mail Address: sphereco@erols.com

Point of Contact: Gerald L. Oar

Previous Publication: None. This paper is an original work, prepared specifically for this conference.

The Benefits of Applying the DoD Information Technology Security Certification and Accreditation Process to Commercial Systems and Applications

Abstract

With the rapid expansion of electronic commerce and other Internet-based services, commercial systems are being exposed to increased threats from electronic intrusion, denial-of-service, and other attacks from outside sources. As a result of this threat, security certification and accreditation of these systems is of paramount importance to ensure that a company's investment and livelihood is protected from all manners of attack.

As a result, commercial systems would benefit from the application of a life-cycle Information Technology (IT) Security (ITSEC) management approach. Unfortunately, many commercial companies do not have the necessary processes in-place to ensure that life-cycle security management is applied to their automated information systems, networks, and applications. However, there is an established life-cycle security certification and accreditation process currently being used to assure the integrity of critical military IT assets. Proper application of the standard procedures currently used by the Department of Defense (DoD) could greatly enhance the overall security and integrity of commercial IT systems.

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is the standard process for security certification and accreditation of IT systems used by DoD and its contractors. This process stresses the importance of a life-cycle management approach to IT Security and focuses on protecting DoD systems through an infrastructure-centric approach for certification and accreditation. Given the similarities between the security needs DoD and commercial IT systems, this paper explores the benefits that commercial companies would derive by applying the approaches and disciplines defined by the DITSCAP to their IT systems.

Keywords

Accreditation, Assurance, Certification, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Information Technology Security (ITSEC)

1. Introduction

With the proliferation of technology into everyday life, much of the general public appears willing to accept whatever commercial off-the-shelf (COTS) technology is available, including security solutions, to perform their daily routines. In many instances, the public's attitude toward security appears to be totally uninformed or indifferent to the use of security procedures to maintain the integrity of private or confidential information.

However, in the corporate environment, this lackadaisical attitude can cost the organization valuable assets and resources, and can result in financial or business losses that can cripple or destroy the ability of a commercial entity to function. From a business and financial perspective, many leaders in industry continue to ask why their company should go to the expense of paying high legal fees, pay high consulting fees, or pay insurance premiums for loss and liability from the use of the Internet.

The answer is simple: interlopers of corporate networks connected to the Internet have caused shutdowns, corrupted data, destroyed irreplaceable files, and caused exorbitant cost due to lost time and work hours to repair ill or afflicted systems. For example, the Senate's Permanent Investigations Subcommittee estimated that major banks and other large corporations lost an estimated $800 million in 1995 to hacker intrusions into their computer systems. In addition, a survey conducted by the Computer Security Institute in April 1996 revealed that 42% of the 428 computer security specialists who responded to the survey had reported an attack within the last year. [1]

Now in 1998, with the proliferation of the Internet use today, increased availability of hacker technology and wide spread home computer use have culminated in a sharp rise in computer crime. A hacker or hacker group could disrupt a corporation's entire network operations, steal sensitive data or alter the system's ability to operate. Recent studies have shown that serious security vulnerabilities exist today on the Internet. Perhaps the most alarming finding of these studies is that over 60 percent of the high-profile, commerce-oriented corporate systems connected to the Internet could be broken into or destroyed. While precise loss figures are not available, some projections estimate that U.S. companies now lose more than $7.5 billion annually. [2, 3]

As a result of these threats, it is apparent that commercial systems would benefit greatly from the application of a life-cycle Information Technology (IT) Security (ITSEC) management approach. Unfortunately, many commercial companies do not have the in-house talent required to ensure that life-cycle security management is applied to their automated information systems, networks, and applications. Fortunately, there is an established life-cycle security certification and accreditation process that corporations could use as a model for their own security programs.

When it comes to the security certification and accreditation of information technology systems, industry can benefit from the experience of one of the guardians of National Security. The Department of Defense (DoD) has an excellent track record of protecting its vital information

processing systems from both internal and external attacks. One key reason for this success is the application of a life-cycle system security certification and accreditation process.

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is the standard process for security certification and accreditation of IT systems used by DoD and its contractors. This process stresses the importance of a life-cycle management approach to IT Security and focuses on protecting DoD systems through an infrastructure-centric approach for certification and accreditation.

The remainder of this paper overviews the DITSCAP and explores specific ways commercial companies could benefit by applying the approaches and disciplines defined by the DITSCAP to their IT systems.

2. DITSCAP Overview

The Department of Defense (DoD) Information (IT) Security Certification and Accreditation Process (DITSCAP) establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit Information Technology (IT) systems that maintain the security posture of the Defense Information Infrastructure. The process defined in the DITSCAP is specifically designed to ensure that an IT system meets the applicable accreditation requirements and that the system will continue to maintain the accredited security posture throughout the system's life-cycle. [4]

As shown in Exhibit 1, the certification and accreditation process defined in the DITSCAP is composed of four phases: Definition, Verification, Validation, and Post Accreditation.

The first phase of the DITSCAP requires the definition of specific certification requirements, determination of the level of effort required to achieve accreditation, and identification of the appropriate individuals who will be responsible for certifying the system. This information is formally documented in a System Security Authorization Agreement (SSAA). The SSAA is the key vehicle in the DITSCAP that guides the implementation of the system's security requirements and describes the mission, environment, target architecture, security requirements and all applicable data access policies, and previously accepted or known security solutions, including process activities, resources, and required documentation for each of the system components. [5]

Phase 1 activities include:

- Documenting the information technology security policy, concept of operations, and requirements;
- Defining a security architecture; and
- Determining the scope, level of effort, and schedule for certification activities.

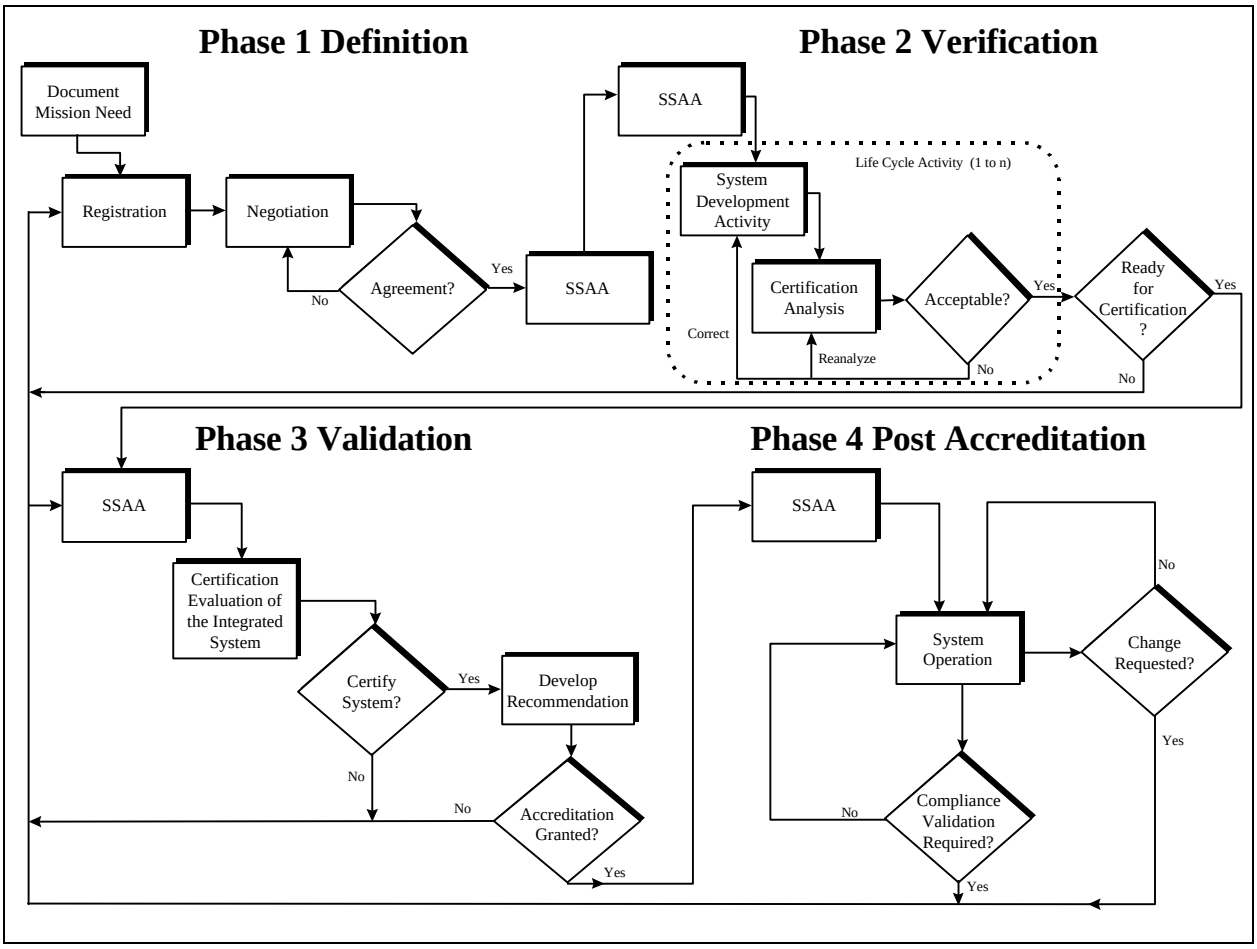


Exhibit 1: The DITSCAP [6]

Once all parties involved in the certification process agree on the requirements and responsibilities defined in the SSAA, the process moves on to Phase 2 for verification.

Phase 2 requires the verification of a system's compliance with the SSAA requirements. For example, at the system architecture phase, verification ensures compliance with the SSAA architecture by determining the effectiveness of implemented policy and requirements. At the software design phase, verification ensures the effectiveness of implementing the SSAA security requirements and architecture, and assesses whether critical components have been implemented correctly and completely. As part of Phase 2, a vulnerability assessment is performed to evaluate the system for any remaining vulnerabilities and, if required, to implement recommended countermeasures. Any uncorrected vulnerabilities constitute the residual risk. If this risk is greater than the acceptable level of risk, the system fails Certification Analysis and Phase 1 is repeated to resolve the problems. If the system is ready for Certification, the process progresses to Phase 3 for validation. [7]

Phase 3 of the security Certification and Accreditation process begins with a review of the SSAA to ensure that the requirements and agreements of the first two phases still apply to the system being validated. Then the process refines and validates the work of the preceding phases to

ensure the system operates in the specified environment at the agreed upon level of risk. Phase 3 requires the evaluation of the integrated system for:

- Certification, including hardware, software, and firmware;
- Inspection of operational sites for physical, and procedural compliance;
- Security-critical component functional testing and penetration testing;
- System management analysis; and
- Risk analysis.

During Phase 3, the system management infrastructure is also examined with respect to the security management organization, security architecture technologies, security posture of the environment, security training and awareness, and the configuration management organization and processes. If accreditation is withheld at this point, specific reasons for the denial, along with suggested solutions, if possible, are provided, and the process returns to Phase 1 to resolve the issues. Otherwise, the system is accredited and the process proceeds to Phase 4, Post Certification and Accreditation support. [8]

Phase 4 includes activities that support the continuing operation of the system and its components after Certification and Accreditation. The objective of this phase is to ensure that security management, operation, and maintenance activities of the system and its components maintain the acceptable level of risk established in the SSAA. Phase 4 activities include security management, change management, and periodic SSAA compliance validation. Proposed changes that can significantly affect the security posture of a system component reinitiates the Certification and Accreditation process at Phase 1. [9]

3. Benefits of Applying DITSCAP Activities To Commercial IT Systems and Applications

The DITSCAP applies discipline to the security process by formally requiring certification and accreditation of DoD systems throughout the entire life-cycle of any system. This disciplined life-cycle approach would prove beneficial to many commercial entities as well. The following paragraphs highlight some of the key features of the DITSCAP that are directly beneficial to any commercial IT system.

3.1 Life Cycle Process

The DITSCAP is designed to be applicable throughout the life-cycle of any system requiring security certification and accreditation. In addition, it is designed to be adaptable to any type of Information Technology system and any computing environment and mission. The DITSCAP may also be adapted to include existing system certifications, evaluated products, new security technology or programs, and be adjusted to the applicable corporate standards. [10]
Given this flexibility inherent in the process, the DITSCAP can be effectively simplified and/or tailored to meet the specific information security requirements of a commercial application. Section 4 of this paper presents one example of how the phases and activities defined in the

DITSCAP could be tailored to provide a simplified framework for the management of the security life-cycle of a commercial information technology system.

3.2 Management Approach

The DITSCAP management approach focuses on management at the applicable system levels to execute the DITSCAP for a given system. The DITSCAP concept includes active participation by system program or operations management, senior operational staff, users, and working level security managers. The DITSCAP provides visibility into the security certification process to all managers responsible for system development, operation, maintenance, and to system users. [11]

Within the corporate environment, management involvement in the security process across all levels of the organization is critical to the success of any implementation activity. Any security program is doomed to failure without complete support from development, operations, maintenance, and user personnel. For this reason, the involvement of all levels of the organization in the security process, as specified by the DITSCAP, is the only true way to ensure a successful implementation of system security features.

3.3 System Security Authorization Agreement

One key feature of the DITSCAP is the concept of documenting the conditions for security certification and accreditation for an IT system. Within the DITSCAP, this documentation is maintained in a single document, the System Security Authorization Agreement (SSAA). The SSAA is intended to reduce the need for extensive documentation by consolidating all security related documentation into one document. The SSAA documents how the security requirements and features of a system's requirements specification are incorporated into the configuration, implementation, and operation of the IT system. This SSAA is a living document. As new requirements or service features emerge, or if the nature of the threats to the system significantly change, the SSAA is updated to reflect the nature and impacts of the changes to the IT system's operating environment. In addition, the SSAA identifies all costs relevant to the security certification and accreditation process, thereby allowing program managers to ensure that the funds needed for security related activities are included in the program budget. [12]

In addition to the obvious benefits associated with completely documenting all security related activities, the SSAA offers one major advantage to commercial entities; the SSAA provides continuity during periods of staff turnover. In this era of job mobility and corporate reorganization, corporations can no longer count on individuals to be the "corporate history" for specific system implementation activities. By way of example, the authors of this paper recently were involved in a program in which virtually all of the key members of the security implementation team left the program during Phase 2 of the DITSCAP process. However, since the initial SSAA was completed, the security features and certification plans of the system were completely documented in a single source. This allowed the replacement staff to become fully knowledgeable in all facets of the system in a matter of days, thereby allowing certification activities to move forward without the slightest disruption in the program's schedule or budget. Without the SSAA, this smooth transition would have been impossible.

3.5 Personnel Security Controls and Awareness Training

In addition to the role that the DITSCAP plays in security certification of an IT system, it also recognizes that other security disciplines, such as personnel controls and security awareness training are critical to the successful operation of a system. To be effective, the SSAA is to include the appropriate Appendices which document the plans for ensuring that adequate personnel controls and security awareness training are provided to all personnel who have direct responsibilities in the management, operation and maintenance of the system. [13]

An old proverb states that "a chain is only as strong as its weakest link". Within the security environment, the weak link exploited by potential electronic intruders to a system is often created by inadequate personnel security controls or lack of proper security training. For example, there has been much information written about the more basic methods electronic intruders employ to gather information about various systems. These methods, such as "Trashing" (i.e. gathering information about a company or system by sorting through a victim's trash) and "Social Engineering" (i.e. assuming a false identity to gather valuable data, such as passwords), are commonly used by all classes of electronic intruders. [14]

Corporations must ensure that employees recognize that their actions are vital to protecting the security and integrity of all of the company's assets from attacks by hackers and other electronic intruders. By adopting personnel security controls and security awareness training, as required by the DITSCAP, commercial companies can close one of the major vulnerabilities to their systems that are commonly exploited by electronic intruders.

4. Sample Application of the DITSCAP to a Commercial Environment

Section 3 of this paper discussed some of the specific benefits that a commercial company could derive by applying the precepts of the DITSCAP to their systems and applications. Given the substantial investment corporations make in information, application of the life-cycle security precepts of the DITSCAP will benefit any commercial entity.

However, many organizations may view the DITSCAP as being too complex or expensive to implement within their corporate environment. Fortunately, as previously discussed, the activities within the DITSCAP have been designed to allow adaptation to various processing environments and systems. While each commercial organization may have unique security requirements, applying a "simplified" DITSCAP to their systems and applications could dramatically improve the overall security and integrity of their operations.

By way of example, Exhibit 2 illustrates how the key DITSCAP phases and activities could be organized to form the foundation of a commercial certification and accreditation process. While the process shown in the exhibit is not intended to be all-inclusive, it does illustrate how the basic activities of the DITSCAP could be simplified for application in the commercial environment.

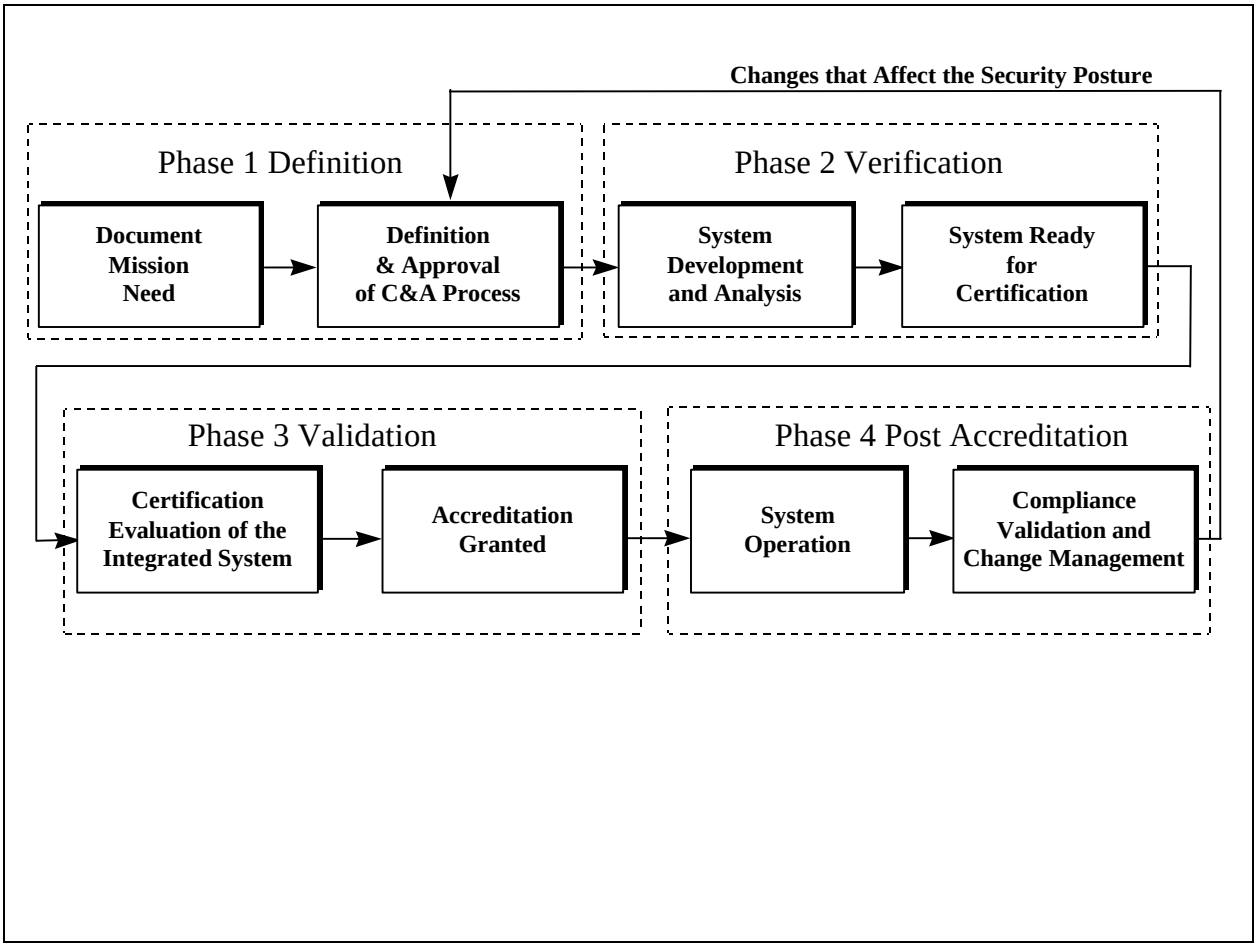


Exhibit 2: Simplified DITSCAP Process for Commercial Applications

While the application of a DITSCAP-based security certification process would benefit all corporate entities, specific industry environments and functions that are particularly good candidates include:

- Companies migrating from the centralized security of a mainframe to a distributed network environment;
- Companies actively performing business over the Internet;
- Organizations with centralized networked databases that contain proprietary information, financial information, copyrights and trademarks, marketing information, personal health records, or other sensitive data that must be protected; and

- Corporations whose livelihood is dependent on computer-aided manufacturing or embedded microprocessor systems that could be crippled by a malicious attack by an electronic intruder.

In addition to the risk to a corporation's resources, the application of a DITSCAP-like process will also benefit the company's managers and employees. Even if the network and information systems are available 100 percent of the time, one hacker's intrusion for a few moments can destroy the system and irreplaceable information and data, as well as the careers and reputations of the Chief Information Officer and IT Manager. If for no other reason, these key corporate managers should embrace the benefits of using a life-cycle security process to protect their professional reputations.

5. Conclusion

Corporations and computer criminals will continue to do battle over the security and integrity of information processing systems. Corporations that do not proactively develop adequate life-cycle security measures for their systems are highly likely to pay the price in terms of lost productivity and revenue. To ensure adequate security assurance measures, commercial entities should have an established process to manage the certification and accreditation process throughout the entire life-cycle of an IT system or application.

However, many companies do not have the necessary in-house talent to develop a life-cycle security process from scratch. Fortunately, there is an established life-cycle security certification and accreditation process that corporations could use as a model for their own security programs.

Proper application of the standard procedures currently used by the Department of Defense (DoD) could greatly enhance the overall security and integrity of commercial IT systems. By applying the approaches presented in the DITSCAP, a corporation can establish the framework necessary to ensure that system security is an integral part of their operations, instead of an afterthought.

6. References

1. *The Wall Street Journal*, "Computer Hackers Cost Big Business $800 Million in '95", Thursday, June 6, 1996.

2. Linda McCarthy, *Intranet Security - Stories from the Trenches*, Sun Microsystems Press, 1998, pp. 22.

3. Lars Klander, *Hacker Proof*, Jamsa Press, 1997, pp. 6.

4. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Enclosure 3, Section E3.1, DITSCAP OVERVIEW", December 30, 1997, pp. 16.

5. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Enclosure 3, Section E3.3, Phase 1, Definition", December 30, 1997, pp. 18 through 25.

6. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Figure E3-1, THE DITSCAP", December 30, 1997, pp. 17.

7. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Enclosure 3, Section E3.4, Phase 2, Verification", December 30, 1997, pp. 26 through 31.

8. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Enclosure 3, Section E3.5, Phase 3, Validation", December 30, 1997, pp. 32 through 37.

9. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Enclosure 3, Section E3.6, Phase 4, Post Accreditation", December 30, 1997, pp. 37 through 40.

10. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Section 6.4, Life-Cycle and Tailoring", December 30, 1997, pp. 5.

11. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Enclosure 4, Management Approach", December 30, 1997, pp. 41.

12. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Enclosure 3, Section E3.3.5, SSAA", December 30, 1997, pp. 24 through 25.

13. Department of Defense Instruction 5200.40, *DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)*, "Enclosure 6, SSAA Outline", December 30, 1997, pp. 51 through 55.

14. National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications - An Awareness Document*, Second Edition, December 5, 1994, pp. 2-2 through 2-4.

The Benefits of Applying the DoD Information Technology Security Certification and Accreditation Process to Commercial Systems and Applications

Authors: Gerald Oar/Robert Jackson

SphereCom Enterprises Inc.

Overview

- Increasing Threat to Commercial Systems
- Certification and Accreditation of Commercial Systems
- The DITSCAP and Its Phases
- System Security Authorization Agreement (SSAA)
- Benefits of Applying DITSCAP to Commercial Systems
- Application of The DITSCAP to Commercial Systems
- Conclusions
- On-Line Information Sources
- Questions and Answers

Increasing Threat to Commercial Systems

- 1995 - U.S. Senate Estimates U.S. Corporations Lost $800 Million to Hacker Attacks
- 1996 - CSI/FBI Survey Reports 42% of Security Practitioners Responding Experienced Security Breaches Within the Last 12 Months
- 1998 - CSI/FBI Survey Reports 64% of Security Practitioners Responding Experienced Security Breaches Within the Last 12 Months
- 1998 - FBI Estimates U.S. Companies Lose $7.5 Billion Annually to Computer-Related Crimes

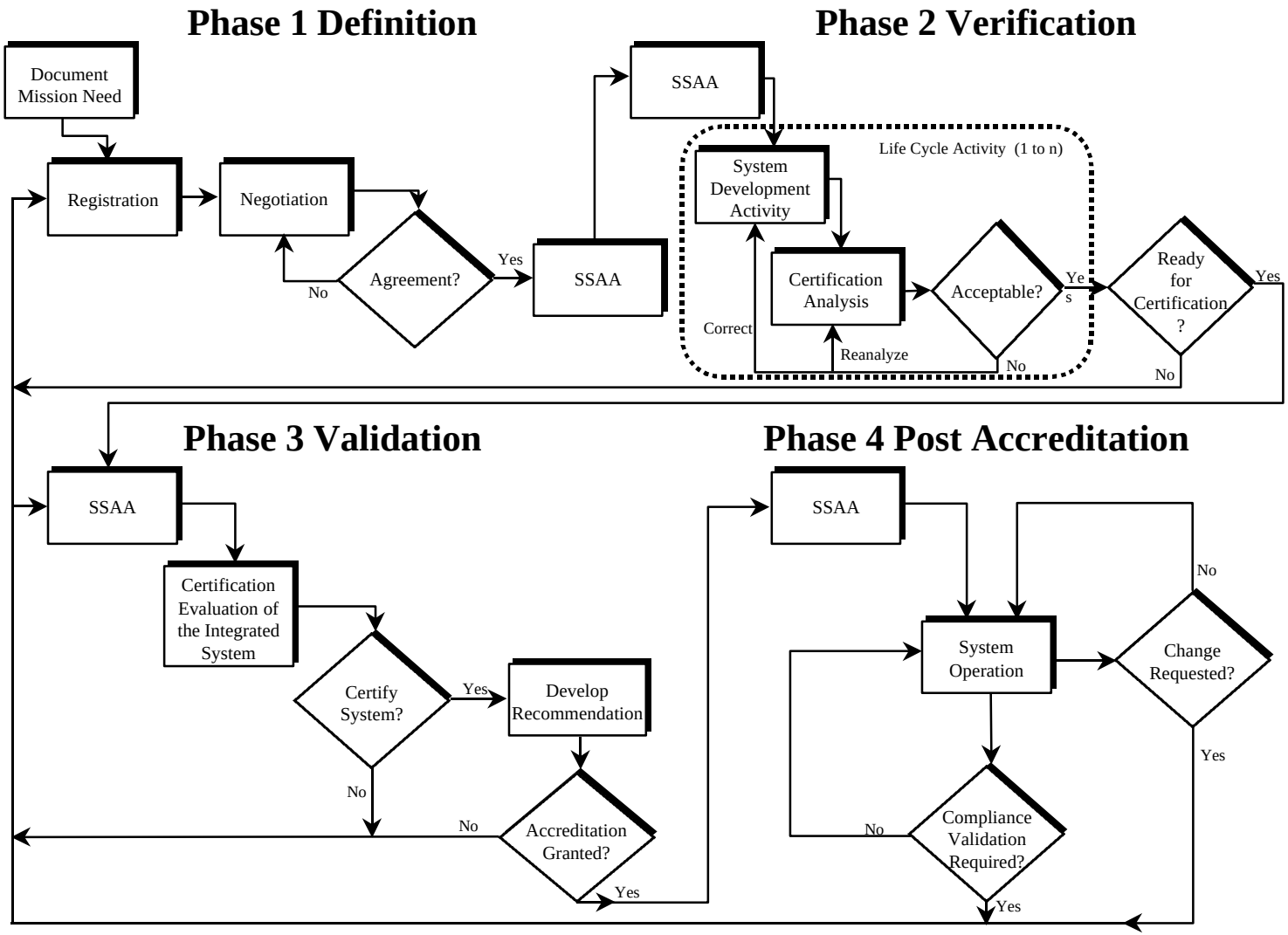
Certification and Accreditation of Commercial Systems

- A Sound Business Practice to Protect Against Potential Losses That Requires:
  - A Disciplined Life-Cycle Process
  - Active Participation From All Levels of Management
  - Thorough Documentation
  - Implementation of “Non-Technical” Security Disciplines
- Many Companies Do Not Have In-House Talent Required To Develop Custom C&A Process

The DITSCAP and Its Phases

- Disciplined Process for Information System Security Certification and Accreditation (C&A)
- Infrastructure-Centric Approach that Focuses on All Phases of a System's Life
- Stresses Life-Cycle Management of the Security Process
- Requires Formal Documentation of System Environment and Conditions for C&A
- Formally Adopted as DoD Instruction 5200.40, December 30, 1997

The DITSCAP and Its Phases (Cont'd)



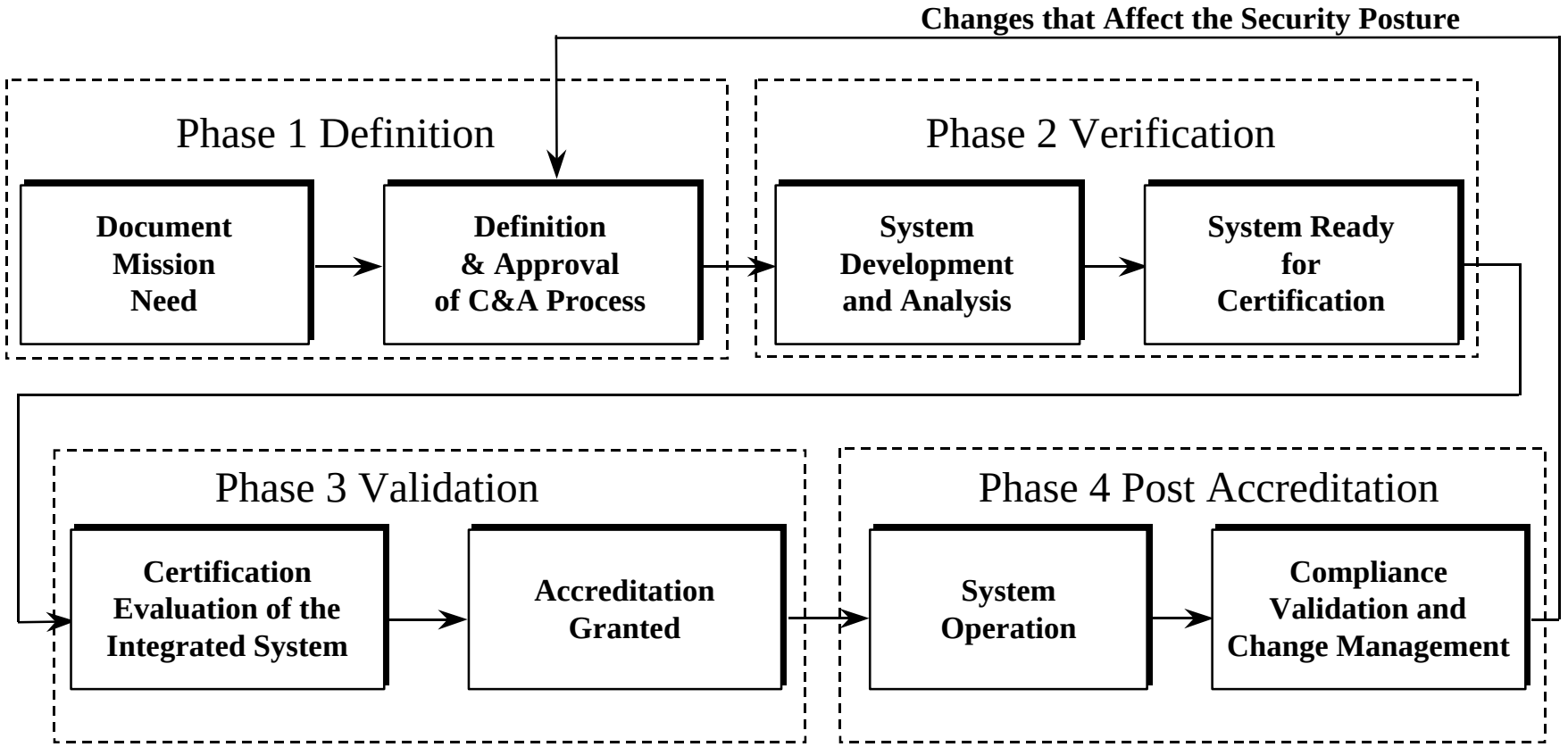
System Security Authorization Agreement (SSAA)

- Single Document Containing All Relevant Security-Related Information
  - System Operating Environment
  - System Architecture
  - Security Requirements Traceability
  - Implementation of Non-Technical Security Programs
  - C&A Costs and Schedule
- “Living Document”
- Provides Continuity During Staff Turnover

Benefits of Applying The DITSCAP to Commercial Systems

- Provides Proven Life Cycle Process
- Provides Comprehensive Management Approach
- Supplies Consolidated Documentation
- Stresses Importance of “Non-Technical” Security Disciplines
- Benefits IT Managers Careers
- Builds Customer Confidence

Sample Application of DITSCAP to Commercial Systems



Conclusions

- Security Threats to Commercial Systems are a Reality and Are Increasing
- Successful Security Programs Must Look at All Facets of the Infrastructure, Not Just Technical Solutions
- Corporation Need An Established Process To Manage System Certification and Accreditation
- Incorporation of DITSCAP Principles Makes Security an Integral Part of a Company’s Operations, Not an Afterthought

On-Line Information Sources*

- DOD Instructions, including DODI 5200.40 http://web7.whs.osd.mil/dodiss/instructions/instruc2.htm
- Computer Security Institute
  - http://www.gocsi.com
- International Computer Security Association
  - http://www.icsa.net
- SphereCom Enterprises Inc.
  - http://www.spherecomenterprises.com

*Sources Cited Are for Reference Purposes Only, and Do Not Necessarily Endorse This Paper's Conclusions. URLs Are Accurate As of Publication Date, But Are Subject to Change Without Notice.

Questions and Answers