Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Certification and Accreditation: A madmans dilemma - Controls

Copyright SANS Institute
Author Retains Full Rights

AD

CERTIFICATION and ACCREDITATION
A madman's dilemma

During the Certification and Accreditation of an Information System an organization defines what supporting documentation is needed in order to accredit the information system in question. But each accreditation process is different in that the requirements needed depends on what you are accrediting either a Major Application or a General Support System. But you still need to remember what exactly you are accrediting.

Title III of the Federal Information Security Management Act (FISMA), P.L. 100-347, December 2002, in section 3544 – Federal Agency Responsibilities, (b) Agency Program (2)(D) which states, "ensure compliance with—

> ''(i) the requirements of this subchapter;
> ''(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;
> ''(iii) minimally acceptable system configuration requirements, as determined by the agency; and
> ''(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

It is item iv above that "in accordance with law and as directed by the President" that basically requires every accredited NSS to add to their Security Requirements Traceability Matrix (SRTM) review of the following documents: (list is not all inclusive)

- Executive Orders
  - E.O.12472 – Assignment of National Security and Emergency Preparedness Telecommunications Functions
  - E.O.12656 – Assignment of Emergency Preparedness Responsibilities
  - E.O.12958 – Classified National Security Information
  - E.O. 13011 – Federal Information Technology
  - E.O.13103 – Computer Software Piracy
  - E.O.13111 – Using Technology to Improve Training Opportunities for Federal Government Employees
  - E.O.13231 - Critical Infrastructure Protection in the Information Age
  - E.O.13292 - Amendment to E.O. 12958 Classified National Security Information
- Presidential Decision Directives (PDD)
  - PDD 63 Protecting America's Critical Infrastructure
  - PDD 67 Enduring Constitutional Government and Continuity of Government
- Presidential Memorandums
  - Action by Federal Agencies to Safeguard Against Internet Attacks
  - Memo from White House Chief of Staff, Security of Federal Information Systems
  - Electronic Government
- Homeland Security Presidential Directive (HSPD)
  - HSPD 7
  - HSPD 8
  - HSPD 12

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- Federal Laws
  http://www.archives.gov/federal_register/public_laws/public_laws.html
  - Clinger Cohen Act (formerly the Information Technology Management Reform Act of 1996)
  - Computer Fraud Act
  - Computer Security Act of 1987
  - Digital Millennium Copyright Act
  - Electronic Communications Privacy Act of 1996
  - Government Performance and Results Act of 1993 (GPRA)
  - Federal Information Security Management Act of 2002 (FISMA) (Title III of the E-Gov Act of 2002)
  - Electronic Government Act of 2002 (E-Gov)
  - Section 639 (A) Prohibition of Federal Agency Monitoring of Personal Information on Use of Internet, Treasury and General Government Appropriations Act of 2002
  - Section 646, Protection of Citizen's Privacy on Federal Web Sites, Treasury and General Government Appropriations Act of 2001
  - Electronic Signatures in Global and National Commerce Act of 2000.
  - Government Paperwork Elimination Act of 1999 (GPEA)
  - Health Insurance Portability and Accountability Act of 1996 (HIPPA)
  - Paperwork Reduction Act of 1995.
  - Patriot Act
  - Public Law 106-398, Defense Authorization Act

Still there are other documents that will need to be reviewed in order to identify additional statements such as the National Archives Records Administration (NARA), NIST, OMB, National Security Agency (NSA), DOD and a host of other regulatory agency requirements.

What is most interesting is the fact that some of these documents are used as references within other documents. However, there are no matrixes available to show the relationship between the referenced documents and the new document. Can a new document provide a matrix of the requirements that were used to create new requirements? "Not available for public viewing". Various agencies are under the belief that if a document is listed as a reference within another document, then that document is in compliance with the referenced document. Yet, how do you reference a classified document or another agencies document that is beyond your organizations realm of responsibility and still meet the requirements. Examples: DODI 8500.2 reference (ai) DOD C-5200.5 (see ECCM-1), DOD S-5200.19 (see ECTC-1).

The hardest part of any CAP is the selection of requirements for the information systems being accredited. This selection process is based entirely on cost.

What single agency in the US has the financial backing to identify, correlate, specify the risk, threat, impact and prepare mitigating procedures for over a several hundred different directives?

The wording in P.L.107-347 section 3544 Federal Agency Responsibilities (a) General (2)(C) "implementing policies and procedures to cost-effectively reduce risks to an acceptable level". So if agency officials follow this statement to cost-effectively implement information systems

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

security, does this statement effectively eliminate P.L. 107-347 Section 3544 paragraph (b) Agency Program. Sub-paragraph (2) sub-sub-paragraph (D) (iv) "any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President."

NOTE: Discussion on what is a National Security Systems will discussed in another article.

What is presented here is the fact that both Presidential directives and federal law create a domino effect in that federal law directs the Office of Management and Budget (OMB) to create guidance for information systems. Which in-turn OMB directs the National Institute of Standards and Technology to create further guidance. The problem that NIST presents is that, it is not authorized to write guidance for National Security Systems, but the domino effect applies NSS follow NIST standards but only if applying cost-effective information systems security policies and procedures.

What is most amazing when considering the number of documents needed to identify the requirements for an IS, is the amount of redundancy involved in the entire process.

The Committee National Security Systems (CNSS) as stated in the NATIONAL INFORMATION SYSTEMS SECURITY (INFOSEC) GLOSSARY, CNSS (Instruction) No. 4009 defines Confidentiality, Integrity and Availability as:

Availability - Timely, reliable access to data and information services for authorized users.

Confidentiality - Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Integrity - Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

The new push in C&A is to relate these requirements and their associated availability, confidentiality, and integrity (CIA) into the new terminology of:

- Management Controls
- Operational Controls
- Technology Controls.

Both the DOD community and NIST have different opinions as to the formulation of various families or controls needed to protect Information System (IS). NIST lists 17 families, while; DOD lists only 7 Information Assurance (IA) Controls. Each organization fails to identify the proper Subject Matter Areas (SMA) needed to properly lists the requirements needed to protect an IS. The NIST Families are listed in Table 1 NIST SP 800-53 and the DOD IA Controls are listed in Table 2 DoDI 8500.2 Subject Areas.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

IDENTIFIER	SECURITY CONTROL FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Certification, Accreditation, and Security Assessments
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity

Table 1 NIST SP 800-53

Abbreviation	Subject Area Name	Number of Controls in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

Table 2 DoDI 8500.2 Subject Areas

The above format shows up as ECCT-2 meaning that EC is "Enclave and Computing Environment", CT is the control Name abbreviation and "2" is the robustness of the system.

Upon examining the NIST documentation it should be noted that the families AC, AU and IA will need to be answered a multitude number of times. This reasoning is based on the need for The solution only unless the agency wishes to print a very large document. The RTM is created by having each Department's input their own policy requirements (see Presidential Directive on sharing information) into the database and the information is hidden from view by all concerned

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

except the originating agency. This process saves everyone the time, expense and loss of materials that would otherwise be expended by a multitude of organizations found within a single agency to generate their own RTM and Certification and Security Test and Evaluation Plans and Procedures (CT&E) (ST&E). The information entered into the master database is linked to a standard Test Identification (TestID) number that links all requirements to a single stated requirement. The requirement in-turn is linked to a threat category (consider the categories as found in DS-2610-142-10) and threat statement, impact statement, risk factor (low, medium, high) and a plan of action for mitigating this requirement should it fail.

All of these requirements will require the linkage to the various controls as identified by either the DOD community include every federal and state agency.

I found in an old DOD regulation DOD 5200.28-STD paragraph 4.3 which stated:

> "The safeguarding of information and AIS resources (against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons) shall be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications security, emanations security, and computer security (i.e., hardware, firmware, and software), as required. The mix of safeguards selected shall achieve the requisite level of security or protection."

These very same safeguards are employed by every federal agency and yet not one federal agency or department can list the Subject Matter Areas (SMA) associated with these safeguards. Table 3 "Safeguards for an Information System provides a glimpse of what SMAs might be associated with each Safeguard. This listing is subject to change as change is the only thing constant in the IT field. After reviewing these safeguards you could place EMSEC under COMSEC and rename COMSEC to Transmission Security (TRANSEC) to include placing ADSEC under the remaining five (5) safeguards.

Consider a process that would identify all requirements and link them to the appropriate Safeguard and the corresponding SMA. Each SMA would contain a questionnaire that would then link these requirements to a single Test ID with a single statement and associated testing criteria. This process would in turn allow a user to reverse engineer the need to select a federal law or organizational policy that in turn would meet, they are linked to a single test identification that has a single stated require extract all Test IDs with the appropriate responses. Otherwise; Can you imagine having to list 30 or more like requirements for single test procedure?

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

CERTIFICATION and ACCREDITATION
A madman's dilemma

Administrative Security (ADSEC)	**Communications Security (COMSEC)**	**Computer Security (COMPUSEC)**	**Personnel Security (PERSEC)**	**Physical Security (PHYSEC)**	**Procedural Security (PROSEC)**	**Emanations Security (EMSEC)**
Subject Matter Areas	Subject Matter Areas	Subject Matter Areas	Subject Matter Areas	Subject Matter Areas	Subject Matter Areas	Subject Matter Areas
Account Management	**Connectivity**	**Configuration Requirements**	**Limited Access Authorizations**	**Facility Description**	**Incident Response Plan (IRP)**	**TEMPEST**
Auditing	NIPRNet	Remote Access	Foreign Nationals	Security Guard	Virus	Red/Black
Create	SIPRNet	Anti-viral	Uncleared Personnel	Parking Areas	Hacking	
Modify	TSABI	OS390	Federal Employees	Force Protection	DataSpill	
Disable	SCI	Unix	Contractors	Fire Evacuation Plans	Security Event / Incident / Violation	
Delete	Wireless	VAX/VMS	Maintenance Personnel	Visitor Logs	**Information Assurance Vulnerability Alerts (IAVA)**	
Electronic Mail (E-Mail)	**Telephone**	**Microsoft O/S**	**Identification**	Escort Duties	**Information Operations Conditions (INFOCON)**	
Password	Cell	Windows 95	Fortezza Cards	Maintenance logs	**Tools**	
Internet Access	STU	Windows 98	Smart Cards	**Inventory**	Penetration Tools	
Monitoring	STE	Windows 2000	Badges	Document Control	Vulnerability Tools	
Privacy	Video Phones	Windows XP	Vendors	Keys	Maintenance	

© SANS Institute 2007, Author retains full rights.

					Logs
Funding	Satellite	Windows 2003	Contractors	Property	Clearing, Sanitizing, Destroying
Identity Management	**Portable Electronic Devices**	Biometrics	New Hires	**Marking and Labeling**	**Internet Service Providers (ISP)**
	Voice Over Internet Protocol	VM	**Security Clearances**	**Information Assurance**	**Security Classification Guide**
	COMSEC	Web Server	Security Clearances	Laptop Security	**Roles and Responsibilities**
	Keying Materials	Firewall	Visit Requests		**System Rules of Behavior (SROB)**
	COMSEC Accounts	Intrusion Detection Systems	Clearance Transfers		**Concept of Operations (CONOPS)**
		Individual Hardware Components	Clearance Upgrades		**Continuity of Operations (COOP)**
		COMSEC Equipment	Periodic Reviews		
		Application Security			
		Database			
		Workstation			
		Servers			

Table 3 Safeguards for an Information System.

© SANS Institute 2008 - Author retains full rights.

The above process would call for a national database with each agency responsible for inputting its own security requirements. The entry of this data would be restricted to each agency less those requirements that would be applied to all agencies regardless of budget restraints. Remember you are only evaluating the effectiveness of the control and preparing a mitigation strategy for your organization. The Plan of Action and Milestones (POAM) are the additional costs needed to protect an IS. It is the Designated Approving Authority (DAA) or Authorizing Official (AO) responsibility to accept the risk. The POAM identifies additional costs that are placed in budget requests that are approved by Congress.

Remember what Roy Clark said "he makes a lot of money, and a lot of his money goes to the parties that he gives, as the one thing that he does not want to hear is about that he should have been at last night". In layman's terms there are a lot of requirements out there, and a lot of those requirements will be applied to your Information System, as the thing you don't want to have happen is to have your CIO explain to Congress Why their organization is not following a specific requirement mandated by federal law or a directive of the President.

Robert Edwards
540.788.3126

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced