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 for Dummies

Copyright SANS Institute
Author Retains Full Rights

AD

Certification and Accreditation
For
Dummies

Since the issuance of the Computer Security Act of 1987 commonly known as Public Law 100-235 every national and international Information Technology (IT) community have been under fire to Certify and Accredited information systems.

This rabid animal known as Certification and Accreditation (C&A) has been allowed to run amok throughout every organization there is that embraces IT. In the United States we see various hybrids such as the DOD community following the DOD Information Technology Security Certification Accreditation Process (DITSCAP) over the past 7 years with a new process now labeled as the DOD Information Assurance Certification Accreditation Process (DIACAP) and this is just the tip of the iceberg as there remains the two variations of the DCID 6/3 or DCID 6/3 Annotated, National Institute of Standards and Technology (NIST) Special Publications (SP) 800-18 or the NIST SP 800-37 or the Federal Information Processing Systems (FIPS) 102[1], and the DOD Intelligence Information Systems (DODIIS) Security Certification and Accreditation Guide, the Joint DODIIS/Cryptologic SCI Information Systems Security Standards. It seems that for every US Federal Department, Agency, Service or Component there is some sort of variation of how to conduct and what documentation is required for an Accreditation Package (AP).

So what is really needed for an accreditation of an Information System? The following paragraphs will offer some insight on how to prepare, combine and enhance your overall C&A process or rather the formal of the documentation for an AP.

The accreditation of any major application or system or network will involve the approval of a multitude Designated Approving Authorities (DAA).

In the past all processes have dealt with identifying the starting documentation and working their way through to the end. Perhaps we should look at the process from a Reverse Engineering perspective and start at the end and work our way towards the beginning of the process.

The accreditation of an IT component is conducted in three parts:

1) Interim Approval to Operate or Approval to Operate (IATO/ATO) - Accreditation for the privilege to process and store information.
2) Interim Approval to Connect or Approval to Connect (IATC/ATC) - Accreditation for the privilege to transmit and receive information.
3) Denial of Service (DOS) – Failure of an IT component to meet any of the first two conditions i.e. IATO/ATO or IATC/ATC. DOS status places the component in a re-evaluation process that requires the mitigation of outstanding requirements or the dismissal of the component due to non-compliance with security mandates.

[1] FIPS 102 was replaced with the NIST SP 800-37 publication.

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

The accreditation of any IT component ends with a system[2] being connected to a network[2].

- System - "The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information."
- Network - IS implemented with a collection of interconnected nodes.

An ATO is not necessarily the final approval factor in connecting a system to a network, rather it is the evaluation of the accreditation packet by the network IT professional and the corresponding DAA as to whether or not the system or other network meet their established parameters. A connection may be granted based on the issuance of an IATO. Remember that an ATO is valid for three years whereas the IATO is valid for a maximum of 1 year or any subsequent combination of months or weeks up to a maximum time period of 1 year. It is the corresponding DAA's responsibility to determine the acceptable level of risk for the system or network to operate at.

The ATC is a formal acknowledgement between two DAAs that the security posture of one network and/or the other network/system has no impact on the security posture of the other DAAs' area of responsibility. An ATC is much like the issuance of the ATO, in that it is also valid for a three year time period. The main difference between the two is that the ATC may not be granted until a complete evaluation of the IATO/ATO has been completed and when signed the ATC is back dated to the day that the IATO/ATO was originally signed. Thus if the evaluation of the ATO lasted one year the ATC approval would only be valid for 2 more years.

When accrediting two networks it is best to list only the essential elements much like what the US DOD community has done with the implementation of the new DOD Information Assurance Certification Accreditation Process (DIACAP)[3]. This process has both an Executive and a Comprehensive accreditation package.

- Executive Package
  - System Identification Profile (SIP)
  - Scorecard
  - Plan of Action and Milestone (POAM)
- Comprehensive Package
  - Executive Package
  - Supporting Documentation – dictated by the DODI 8500.2.

The SIP presents problems in that nearly two thirds of the document should be covered in the System Test and Evaluation Plans and Procedures (ST&E) document not to mention it suggests violation of the Federal Paperwork Reduction/Elimination Acts. Those questions pertaining to the Contingency Plan (CP), Incident Response Plan (IRP) and the previous accreditation information can be covered in the ST&E that is organized by

[2] Committee on National Security Systems No. 4009 National Information Security (INFOSEC) Glossary

[3] DOD Information Assurance Certification Accreditation Process (DIACAP) July 2006

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

Subject Matter Area (SMA) organized by the seven safeguards that are natural to all IT communities.

The SIP is the new identification name for the old expressions of the System Security Plan or the System Security Authorization Agreement. In order to properly align a network or system it would be more beneficial to follow the Business Impact Analysis (BIA) format found in the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-34 Contingency Planning Appendix B. This formatted document limits you to the System Identification, System Description and Prioritization for Restoration Identification[4].

The incorporation of the Scorecard and the POAM will also be needed, in that the scorecard shows what requirements the network or the system is following. The POAM illustrates what requirements that is not in compliance and the mitigation procedures that are planned to bring the requirement into compliance.

What you will need to add are copies of any internal/external agreements with other systems/networks so that the other IT professional may determine if a hidden back door exists.

The IATC is only a formality in that it is a formal request from one DAA to connect their system or network to another system or network. The issuance of the IATC is an acknowledgement that an IATO/ATO package is under review and awaiting approval for an ATC. The IATC functions much like the IATO in that it is only valid for a single year or until such a time as both parties agrees on the security posture and mitigation procedures for both systems/networks. When submitting an IATC request and only supplying an Executive package remember that the other party may request any supporting materials needed to complete their own analysis.

In order to receive an IATO or an ATO the following documentation will need to be provided in order for the IAM personnel to be able to review all necessary compliance factors in order to ascertain the proper risk of the system or network for the DAAs accreditation approval or disapproval.

For the accreditation of any IT component the following documentation will be required.

Enterprise or Network documentation
Configuration Management Plan (CMP) - Management of security features and assurances through control of changes made to hardware, software, firmware, and documentation, test, test fixtures, and test documentation throughout the life cycle of an IS.

The CMP should be written at the highest level such as the Departmental level as this process only need to be listed once within an organization and all subsequent components

[4] Process shows compliance with Homeland Security Presidential Directive -7 Critical Infrastructure Identification, Prioritization, and Protection

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

should follow this process. This process represents a cost-effective means of controlling changes made to any component in that:

1. All problems are reported to the Help Desk; which in turn creates a Trouble Ticket (TT) and passes the problem laterally to the technicians for solutions. (Tier 1)
2. If a Change Request (CR) is made it is also made through the Help Desk TT Process and at the same time if the technician have a problem that they cannot solve the problem is as with the CR. The problem is passed to the System Owner (SO) for resolution. (Tier 2)
3. The SO represents the chair for their own Configuration Control Board (CCB); the DAA only needs to be notified of the problem and may attend at their own discretion. The SO will create a Configuration Review Board (CRB) if they fell such action is warranted. The CRB will conduct the feasibility study to determine a viable solution and will submit their findings to the CCB. The SO will forward the recommendation to the DAA for approval. (Tier 3)
4. If the solution calls for a modification to the network the recommendation will be passed to the system DAA for their concurrence and subsequent submission to the network DAA for mitigation. (Tier 4)
5. If the network DAA feels that the solution may affect the enterprise, then the recommendation is forwarded to the enterprise DAA for mitigation. (Tier 5).

Training Plan (TP)

This plan is created and maintained at the departmental level and covers such areas as:

1. User Training – Initial and Refresher training is conducted for all classification levels at the same time. This process presents a cost effective approach and reduces overhead cost and increases productivity. Each user should sign a standardized Rules of Behavior (ROB) for access to any classified or unclassified information system in this department or component. The ROB is to be updated on an annual basis. Initial training should be conducted in a formal classroom with refresher training conducted on-line with a printable output showing completion and should be signed by the user and returned to the training coordinator.
2. IT Professional Development – This training identifies all IT professionals that need to be trained in the performance of their duties to include their legal obligations to the organization. Training needs to be provided to all positions not just IT, but also to such areas Incident Response, Contingency to include (but not limited) to DAA, Program Manager, Information Systems Security Manager/Officer, Database Administrators, System Administrators, Firewall Technicians, Intrusion Detection Technicians, Communication Security Custodians, Fire Teams, Physical and personnel Security Specialists, etc.

Incident Response Plan (IRP)

This plan contains three parts, it is divided this way in that the first part present the basic information as to the formulation of teams and flow chart type diagram that identifies if a certain action is performed then go to this section for resolution. The second part and not in a particular order should deal with Physical incidents in regards to bomb, fire, Nuclear Biological or Chemical attacks, building damage, or physical intrusion (armed or

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

unarmed). The third part should cover the IT realm in regards to (but not limited to) hacking, virus, unauthorized software/hardware, etc.

Requirements Traceability Matrix (RTM)
This process needs to be located in a database. The database is configured in such a way as to divide international documentation, nations' laws and various organizational policies and procedures into the six (6) safeguards (administration, communications, and configurations, personnel, physical and procedural). Each safeguard is lists various Subject Matter Areas (SMA) that reflect specific protection requirements. This RTM provides a SO the ability to weed out unnecessary requirements through the use of a questionnaire that is used to describe your system i.e. do you have firewalls, what is your electronic authentication level, what is FIPS 199 categorization, List your hardware and software for verification for use IAW CNSSS No. 11[5]. This document lists the test procedures, risk factor, threat impact, name of person conducting the test, dated and is linked to the POAM for compliant requirements. This process allows the creation of a subsequent database report for the ST&E, Scorecard, POAM and a Residual Risk Assessment Report (RRAR)[6]. This RTM should also list the various vulnerabilities/weaknesses for all hardware and software. These weaknesses and their associated testing procedures will be created for the Certification Test and Evaluation Plans and Procedures (CT&E).

Roles and Responsibilities
This document should list all possible position descriptions associated with an information system. These following provides and example of possible descriptions:

1.1.1 SENIOR DATA BASE MANAGER.

a) DUTIES.

- Manages the development of data base projects.
- Plans and budgets staff and data base resources.
- As necessary, reallocates resources to maximize benefits.
- Prepares and delivers presentations on Data Base Management Systems (DBMS) concepts, data warehousing, and data mining capabilities.
- Provides daily supervision and direction to support staff.
- Evaluates and designs existing or proposed systems to structure and access databases.
- Analyzes data base requirements of the user department, applications programming and operations for IA requirements.
- Submits recommendations for solutions, which require definition of the physical structure and functional capabilities of databases and require data security and data backup/recovery specifications.
- Proposes detailed specifications and flowcharts and coordinates installation of revised or new systems when incorporating IA.

---

[5] CNSS No. 11 NATIONAL POLICY ON CERTIFICATION AND ACCREDITATION OF NATIONAL SECURITY TELECOMMUN1CATIONS AND INFORMATION SYSTEMS is the requirement for all COTS/GOTS hardware/software to be certified through the NIAP, FIPS or Common Criteria selection process.

[6] The RRAR may be combined with the Scorecard as an added column or included in the POAM.

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

b) QUALIFICATIONS:

- A Bachelor's degree in Computer Science, Business, Information Systems, Engineering, or other related scientific or technical discipline is required.
- Six (6) years general experience and two (2) years of IA specialized experience.

c) EXPERIENCE:

- General Experience:
  - Six (6) years of data base management experience with information systems.

- IA Specialized Experience:
  - Two (2) years experience in an IA discipline (e.g., Information Systems Security (IA), Computer Security (COMPUSEC); Communications Security (COMSEC); TEMPEST; or Operations Security (OPSEC).
  - Demonstrated ability in evaluation of databases as related to IA requirements, and experiences with data base management systems design and system analysis, current operating systems software internals and data manipulation languages.
  - Experience with securing distributed databases, data locking, multi-level access within the database, user accountability with respect to accessing remote data repositories, and database transaction logging and auditing.
  - Experience with data warehousing and data mining.

d) EDUCATION/WORK EXPERIENCE SUBSTITUTION:

- A Master's Degree in Computer Science, Engineering, Business, or other related scientific or technical discipline may be considered equivalent to two (2) years general experience, and one (1) year IA specialized experience.

Duty Appointment Orders

Every IT position has someone being responsible for the actions of the position and in turn needs to have that person listed on duty appointment orders or additional duties descriptions. These orders should be created in format only by the department and made available to all SO. The information contained on these forms should list the following:

- ✓Name of Positions
- ✓Duration of Order
- ✓Expiration of previously issued order
- ✓Name of person filling the role
- ✓Date
- ✓Location of all responsibilities for the position i.e. ISSO locate in Roles and Responsibilities section 2.5 covering the following duties: (Example)
  - Day to day operations
  - Contingency Operation (CP)
  - Incident Response Operations (IR)
  - Continuity of Operations (COOP)

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

System Documentation
SIP already explained earlier

Security Test and Evaluation Plans and Procedures (ST&E)
The ST&E is created after answering the questionnaire associated with the RTM. The ST&E will need to have the ability to inherit controls in both directions i.e. Firewall/IDS requirements will be inherited to lower level applications as well as the ISA between applications and points outside the system will need to be listed in the system ISA section in order to show a proper flow of data. This process should allow an auditor the ability to trace the flow from start to finish. Example an application located within a system has an ISA with a bank. The flow should show the application, the system connected, the network connected, the phone company or satellite connection to another network to the next system down to the application used at the bank. This inheritance process can be employed with the implementation of the HSPD-12 process in regards to the levels of implementation for the installation, structure, floor, bay, room, system, application or database and other hardware or software components. Where else might this inheritance process be used is up to your discretion.

Certification Test and Evaluation Plans and Procedures (CT&E)
The CT&E should be created by listing all hardware and software through the RTM. However, current operations today rely to heavily on scanning tools to only identify what they consider to be a weakness in your system or application based on their own search criteria. These tools do not list any known weaknesses with the associated tested material. They only list what the tool has determined to be a weakness, often producing a false positive.

Scorecard and POAM is created as the ST&E is completed.

Training Plan
This plan is directed by Office of Management and Budget (OMB) Memorandum A-130 Transmittal Letter No. 4 Appendix III as Specialized Training. This training is required for those personnel learning how to operate/manipulate a new software package.

Memorandum of Agreement/Memorandum of Understanding/Interconnected Service Agreement (MOA/MOU/ISA)
These agreements are integral part of accreditation for the purpose of sharing information between two parties. In essence the MOA/MOU/ISA is the ATC document between systems or networks or systems and networks.

Certification Statement
A formal acknowledge by the Certifier that the system is in compliance with stated requirements with the associated Risk of the system, application or network.

Accreditation Statement

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

Formal statement by the DAA or a DOS/IATO/ATO/IATC/ATC that also identifies the risk and any mitigation procedures that is to be executed. The IATC/ATC approval will result in formal MOU/MOA/ISA between DAAs.

Conclusion

The above listed documentation is a single persons opinion on how various documentation should be created in order reduce costs, consolidate documentation and less the impact for conducting a Certification and Accreditation. When answering the various SMA questions within the ST&E and associating these weaknesses with the weaknesses found through the CT&E for the creation of the Scorecard, POAM, RRAR and subsequent Certifiers Letter. Automation is a wonderful tool to have for the C&A process if it is used to the utmost capability.

A C&A packet is a consolidation of smaller C&A packets for the various components of a system or network. In essence you should be conducting a mini-C&A for any software or hardware component that requires a userid and password pertaining to the six safeguards and SMAs. Each mini-C&A package should be inherited into a larger C&A packet to properly identify the risk to a system or network. Even systems and network need to inherit SMAs from such areas as the HSPD-12 implementation of installations, structures, floors, bays, and rooms or any combination thereof to properly identify the risk associated with each area.

© SANS Institute 2007, Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced