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 - Costs

Copyright SANS Institute
Author Retains Full Rights

AD

CERTIFICATION and ACCREDITATION
A madman's dilemma

When associating the various documents needed to conduct a CAP, it is most confusing in trying to actually place a dollar value to this process. Remember there are a multitude number of ways of conducting a CAP. Table 6 provides an example of how to estimated the cost of conducting a CAP. For simplicity we use the DOD 8510.1-M Appendix 1 format for System Security Authorization Agreement (SSAA) each corresponding Appendix will have the title only and not the Appendix Letter (you see the similarity between your process and this process). Remember the federal government does not share information with other federal agencies let alone within its boundary as well. "We don't share our information with anyone that includes our own subordinate organizations".

For the sake of clarity, I am using the format of the DITSCAP Application Manual Appendix A.

Note: if you follow the process listed in the Application Manual your SSAA will contain 7 parts (See Task 1-8 Output Statement) not the 6 parts as shown in Appendix A.

Still DOD has initiated a new process titled the DOD Information Assurance Certification and Accreditation Process (DIACAP). Although this is process is considered new, it is not really, they have just gotten a bit wiser in understanding the overall process. You don't need to submit everything for a "Connection Approval", you just supply the basics.

The DIACAP has two packages the Executive and the Comprehensive. The Executive has the SIP, the Scorecard and the Plan of Action and Milestone (POAM). The Comprehensive contains the Executive and supporting documentation. The supporting documentation is undefined at this time. It is to be noted in the E3.3.1 that a Computer Network Defense Service Provider (CNDSP) rating should be acquired for an Approval to Operate (ATO). The CNDSP rating is based on the evaluation of the Evaluators Scoring Matrix (ESM) that contains 120 questions in two parts for the System Provider (General Support Systems (GSS) and the System User (Major Applications (MA)). These two parts contain over 600 bullets relating to the various references listed at the bottom of each question. What is not evident is the matrix that links each bullet to the stated reference that is needed in order to cross-reference the replies to from the ESM into the perspective C&A packet for each MA or GSS that the CNDSP was written to support. (see Table 1 DITSCAP to DIACAP Comparison).

In order to determine the cost of preparing a C&A packet the following scenario is provided as shown in Table 2 Cost Estimate.

Process
1. Formulate a table into an excel spreadsheet.

2. The cost per man-hour shall be computed at $41.57. This cost is estimated on the 2003 average hourly earnings of 5 federal employees (11, 12, 13, 14 and SES 1) for a single federal agency. (Estimate only use your own figures)

3. Cost is computed as Man-hours multiplied by Time multiplied by Regulations (Regs).

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

DITSCAP	a	Status
System Security Authorization Agreement (SSAA) (SSP)	System Identification Profile (SIP)	Change from a 6/7 part to 34 questions
Acronyms		Not really needed
Definitions		Not really needed
References		Not really needed
Concept of Operations (CONOPS)		Still needed, although if the requirement is listed in the ST&E, why restate the answer in another document
ISSP		Never really defined by DOD or NIST
SRTM		Optional, ST&E contains same information.
CT&E		Formal output of scanning applications.
ST&E		Still required
ASDA/SD		Historical Document, out with old, in with the new
SROB		Still required
IRP		Still required
COOP		Still required
PC/TSC		Still needed, although if the requirement is listed in the ST&E, why restate the answer in another document
MOA/MOU/ISA		Still required
SETAP		Still required
TER	Scorecard	Still required
RRAR/POAM	POAM	Still required
CAL		Still required

Table 1 DITSCAP to DIACAP Comparison

Cost estimate

a. The SSAA consists of 6.4 parts and it is estimated at an average of 80 hours to generate just the SSAA. This estimate is based on the preparation, review, modification and signature approval from at least 5 individuals involved in the process.

b. Acronyms, references and definitions are a simple cut and paste from various documents with little or no change from the master document, with 1 hour per document.

c. The Concept of Operations (CONOPS) is estimated at 100 hours as a format needs to be identified as neither NIST or the DOD community has an established format or regulation that covers this particular area. You may wish to examine the IEEE 1362-1998 IEEE Guide for Information Technology - System Definition - Concept of Operations (CONOPS) Document as a possible suggestion for a format process.

d. The Information System Security Policy (ISSP) is estimated at 100 hours, as a format will need to be identified as neither NIST nor does the DOD community have an established format or regulation that covers this particular area. The ISSP is supposed to identify how security is to be applied to the system as well as to define what is the reporting process for security

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

events/incidents and violations. Some people refer to this document as the Security Features Users Guide (SFUG)

e. The Security Requirements Traceability Matrix (SRTM) is estimated at 200 hours, as this document will list all of the requirements that the system that is to be accredited and adhere to. The problem with this document is that most C&A will not list the configuration requirements of the system, but will reference the document as part of the SRTM.

a) Here is a decision for all managers to face. Do we break up the SRTM and organize the document into sections (by safeguard area like a checklist) or do we leave everything into a single document?
b) Do we separate the hardware/software and firmware requirement into the CT&E or do we combine everything into the ST&E?
c) Still do we really need a SRTM, as the information provided here will be provided again in the ST&E and CT&E?

You will need to determine whether or not the requirement is related to your system or not. I.e. In the Clinger Cohen act it mentions that a Chief Information Officer (CIO) is to be identified, obviously the CIO is positioned well above your system and should therefore not appear in your requirements section or should it. Considering that the CIO is part of Information System Security Personnel chain of Command. Also configuration requirements are handled through the scanners used to verify fictitious configurations as identified by the scanner database. Each requirement will need to be linked to a test procedure and related requirements. This process is necessary to reduce the possibility of repeating the same test more than once

f. The CT&E or the ST&E will list the necessary test plan and procedures for each requirement or related requirements.

g. The ASDA/SD calculation will depend on whether this is a new system or old system. If old system the cost has already been spent on the development of old documentation. If new as you move through the Life Cycle Management Process and develop various document and or support contracts for this new system this cost will need to be computed. This section would contain such items as the:

a) Configuration Management Plan (CMP),
    i. Configuration Review Board (CRB) Charter,
    ii. Configuration Control Board (CCB) Charter,
b) Security Features Users Guide (SFUG)
c) Trusted Facility Manual (TFM)
d) Previous accreditation documentation and,
e) Any previous white papers, checklists or inspections surveys.

h. The SROB is an explanation on rights of the users and the responsibilities of the system to the user.

i. The Incident Response Plan (IRP) has no established format as a formal document has not been identified by any federal publishing agency.

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

j. The Contingency Plan or Disaster/Recovery Plan (DRP) should follow the NIST SP 800-34 Still DOD does reference a continuity planning in their DODD 3020 series documents.

k. The PC/TSC has no established format as a formal document has not been identified by federal publishing agency. Still the brief title leads a person to believe that what is being requested here are actually two documents better known as the Security Features Users Guide (SFUG) and the Trusted Facility Manual (TFM). The choice is open for discussion.

l. The MOA/MOU/ISA are agreements between different DAAs both agreeing on the security aspects that will allow the two systems to operate together and not become a security risk to the other. These two systems may be connected via a guard that allows communications between high-to-low or low-to-high communications channels.

m. The SETAP is the training plan for the entire system and covers three distinct areas:

1. All users are to receive training pertaining to their rights and responsibilities.
2. The information Systems Security Personnel (those who run the system from the Designated Approving Authority to the System Administrator). This section explains how these individuals are to be trained, what requirements are to be met and provide career mobility. This training will be conducted in conjunction with user training as well.
3. Specialized Training is for those individuals with special needs such as database administrators or special applications on the system.

n. TER is the after action report or in plane terms, these are the results of the tests required by the requirements listed in the SRTM and linked to the test plans found in either the CT&E and or the ST&E.

o. RRAR is the breakdown of those requirements that did not pass or were identified as being deferred due to the lack of requirements, equipment or duly trained personnel. This section will also contain corrective action statements detailing how a deficiency is to be corrected. These corrective actions are commonly called the Plan of Action and Milestones (POA&M).

p. The Certification statement acknowledges the fact that the system in question is operating at defined level of risk and that the Certifying Official (CO) or Certifying Authority (CA) is merely identifying that risk

q. The Accreditation statement is the formal approval by the DAA that the system can operate at the risk as identified by the CO or CA as the case may be.

If this example is to be used for the creation of a new system, don't forget to add in the cost for the CMP, CCB, CRB, SFUG, TFM, and any other supporting documentation, meetings, third party involvement and travel if needed.

NOTE: This cost does not include any meetings or travel involved in gathering information.

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

	Regs	Man-Hour	Time	Cost
		$41.57		
SSAA		$41.57	80	$3,325.76
Acronyms	2	$41.57	0.15	$12.47
Definitions	2	$41.57	0.15	$12.47
References	2	$41.57	1.0	$41.57
Concept of Operations (CONOPS)	1	$41.57	80	$3,325.76
Information Systems Security Plan (ISSP)	1	$41.57	100	$4,157.20
Security Requirements Traceability Matrix (SRTM)	2	$41.57	120	$9,977.28
Certification Test and Evaluation Plans and Procedures (CT&E)	2	$41.57	120	$9,977.28
Security Test and Evaluation Plans and Procedures (ST&E)	2	$41.57	120	$9,977.28
Applicable System Development Artifacts / System Documentation (ASDA/SD)	1	$41.57	187	$7,773.96
System Rules of Behavior (SROB)	1	$41.57	10	$415.72
Incident Response Plan (IRP)	1	$41.57	100	$4,157.20
Continuity of Operations Plan (COOP)	1	$41.57	100	$4,157.20
Personnel Controls and Technical Security Controls (PC/TSC)	1	$41.57	200	$8,314.40
Memorandum of Agreement / Interconnected Service Agreements (MOA/ISA)	1	$41.57	10	$415.72
Security Education Training and Awareness Plan (SETAP)	1	$41.57	200	$8,314.40
Test and Evaluation Report (TER)	1	$41.57	100	$4,157.20
Residual Risk Assessment Report (RRAR)	1	$41.57	120	$4,988.64
Certification and Accreditation Letters (CAL)	1	$41.57	1	$41.57
		Total	**Cost**	$83,543.09

Table 2. Cost Estimate

The above cost is estimated at $83,543.09 for a single system based on 2 documents. Consider the cost (we do not share) for 100,000 like C&A in the Federal Government $8,400,000,000. This estimate is not difficult to imagine when you consider 50 plus federal agencies, coupled with the DOD's OSD, Navy, Army and Air Force and don't forget the various security classification levels of Unclassified, Secret, Top Secret and Special Compartmented Information (SCI). Also consider the different methods or processes when performing a Certification and Accreditation. This cost of a mere $8,400,000,000 is considered to be low at best as you can also compute in what can be accredited as mentioned earlier. Lets see how that estimate comes to roughly an additional 10 categories with multiple locations and let us not forget that IAW CNSS No. 11 any commercial off the shelf (COTS) or government off the shelf (GOTS) products that is to be placed, connected or affixed to a federal government IS, these products are to certified by NSA, Common Criteria or the National Information Assurance Process (NIAP). So don't forget to add in the cost of all the hardware and software that needs to meet certification standards as well.

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

CERTIFICATION and ACCREDITATION
A madman's dilemma

Experience has shown that Certification and Accreditation is a confusing process that grows exponentially as time progresses due to untrained and inexperienced personnel. The cost associated with conducting a C&A effort in determining the level of effort to be employed. Without a standardized process and shared information in preparing C&A documentation no single organization will be able to PROPERLY accredit their information system today or tomorrow.

Based on the number of requirements currently available today, we can see the overlapping and redundant information that needs to be eliminated in order to make this process flow more evenly. Still federal agencies will do what they want, when they want, if they do anything at all to properly protect an information system.

Don't believe the last statement, how many agencies have listed HSPD-12 into your C&A requirements matrix. Have you considered the implications of HSPD-12? HSPD-12 will be required for:

a) Installation access – areas that require security guard access control points such as Fort Meade, MD.
b) Building Access – areas that require security guard access control points.
c) Floor Access - areas that require security guard access control points or combination card, or CAC entry points.
d) System Access – basis for HSPD-12
e) Application/Database access
f) Maintenance
    a. Firewalls
    b. Intrusion Detection Systems
    c. Workstations
    d. Servers
    e. Routers, Switches, etc.

HSPD-12 is the forerunner of the Real ID Card Act and the need to put a microchip into passwords. What other requirements are lurking in the shadows?

Robert Edwards
540.788.3126

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

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

Last Updated: April 25th, 2015

Upcoming SANS Training

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

SANS ICS London 2015	London, GB	Apr 27, 2015 - May 02, 2015	Live Event
SANS Bahrain 2015	Manama, BH	May 02, 2015 - May 07, 2015	Live Event
SANS Security West 2015	San Diego, CAUS	May 03, 2015 - May 12, 2015	Live Event
SANS Secure India 2015	Bangalore, IN	May 04, 2015 - May 23, 2015	Live Event
SANS Secure Europe 2015	Amsterdam, NL	May 05, 2015 - May 23, 2015	Live Event
SANS/NH-ISAC Healthcare Cybersecurity Summit	Atlanta, GAUS	May 12, 2015 - May 19, 2015	Live Event
SANS Melbourne 2015	Melbourne, AU	May 18, 2015 - May 23, 2015	Live Event
SANS Pen Test Austin 2015	Austin, TXUS	May 18, 2015 - May 23, 2015	Live Event
SANS Secure Thailand 2015	Bangkok, TH	May 25, 2015 - May 30, 2015	Live Event
SANS ICS Security Training - Houston	Houston, TXUS	Jun 01, 2015 - Jun 05, 2015	Live Event
SANS ICS410 Vienna in Association with IAEA	Vienna, AT	Jun 06, 2015 - Jun 10, 2015	Live Event
SANS Dublin 2015	Dublin, IE	Jun 08, 2015 - Jun 13, 2015	Live Event
SANSFIRE 2015	Baltimore, MDUS	Jun 13, 2015 - Jun 20, 2015	Live Event
SANS Rocky Mountain 2015	Denver, COUS	Jun 22, 2015 - Jun 27, 2015	Live Event
SANS Pen Test Berlin 2015	Berlin, DE	Jun 22, 2015 - Jun 27, 2015	Live Event
Cyber Defence Canberra 2015	Canberra, AU	Jun 29, 2015 - Jul 11, 2015	Live Event
SANS Capital City 2015	Washington, DCUS	Jul 06, 2015 - Jul 11, 2015	Live Event
Digital Forensics & Incident Response Summit	Austin, TXUS	Jul 07, 2015 - Jul 14, 2015	Live Event
European Security Awareness Summit	London, GB	Jul 08, 2015 - Jul 10, 2015	Live Event
SANS London in the Summer	London, GB	Jul 13, 2015 - Jul 18, 2015	Live Event
SANS Minneapolis 2015	Minneapolis, MNUS	Jul 20, 2015 - Jul 25, 2015	Live Event
SANS San Jose 2015	San Jose, CAUS	Jul 20, 2015 - Jul 25, 2015	Live Event
SANS SEC401 London	OnlineGB	Apr 27, 2015 - May 02, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced