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 (C&A) Vs System Development Life Cycle Management (SDLC)

Copyright SANS Institute
Author Retains Full Rights

AD
ONLY ONE INDEPENDENT TEST
MEASURES REAL-WORLD,
ENDPOINT MALWARE PROTECTION.
TREND MICRO SMART PROTECTION NETWORK

Certification and Accreditation (C&A)
Vs
System Development Life Cycle Management (SDLC)

In 1987 the US Congress passed the Computer Security of 1987 Public Law (PL) 100-235. This particular law launched one of the first technological control mandates that has exploded over the years in identifying the need to control technology in the protection of the information that is processed, stored, transmitted and received in electronic form.

These protective measures have been encapsulated into various procedures such as the Certification and Accreditation of Information Systems based on various Life Cycle Management descriptions. Both expressions have the basic results with plus or minus an accurate description based on the various steps that are the same with different titles. The following paragraphs describe the relationship between Certification and Accreditation to System Development Life Cycle Management and Planned Parenthood. This comparison offers a relational description so that although a person may not understand the terminology associated with C&A, they will be able to relate the process to their every day lives.

SDLC will be utilize a 5 cycle phased approach using:

- Phase 1 Concept
- Phase 2 Acquisitions and Development
- Phase 3 Testing
- Phase 4 Operations and Maintenance
- Phase 5 Disposal.

There is an article titled as the Systems Development Life Cycle for IT Auditors[1] that will be used a cross matrix for auditors to understand the relationship between what the persons doing a C&A and what the functions of an auditor.

Before proceeding we must understand what the definition of the words Certification and Accreditation. The NSTISSI[2] NATIONAL INFORMATION SYSTEMS SECURITY (INFOSEC) GLOSSARY No. 4009 September 2000 will be used to provide these definitions.

Certification - "Comprehensive evaluation of the technical and non-technical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements."

Accreditation - "Formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode at an acceptable level of risk,

[1] Information Systems Control Journal dated as Volume 1, 2007 on pages 24 through 26

[2] National Security Technology Information Systems Security Instruction (NSTISSI) has been re-designated as the Committee for National Security Systems (CNSS), NATIONAL INFORMATION SYSTEMS SECURITY (INFOSEC) GLOSSARY No. 4009

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

based on the implementation of an approved set of technical, managerial, and procedural safeguards."

It should be understood that under ideal conditions a C&A should be executed in 6 to 18 months depending upon the complexity of the system being accredited. However, due to managerial decisions a C&A on an information system is to be accredited by yesterday.

The differences between a Certifier (C&A) and an Auditor is that they compliment each other as the Certifier will Certifier will confirm that the information system meets the stated requirements as identified by law or presidential decisions. The auditor will verify that results provided by the Certifier due in fact meet the requirements. It should be noted that an auditor can be a person under the Certifier or a person that is not part of the same organization as the Certifier.

Auditor[2] – a person that conducts an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Certifier - Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages. This person is usually associated with the Information System Security Manager (ISSM).

Reviewer – a person positioned internally within an organization; that is under the Certifier. (See Auditor)

Information System Security Officer (ISSO) – prepares the C&A documentation for the Certifier.

Phase 1 Concept

The process of planning for a child is related to the process of planning for a new information system in that you have the following steps to follow:

Parents discuss the desire to add a child to the family. They consider the cost and the selection of the sex of the child. They prepare such lists (configuration) as how the child will dress, what languages the child will learn (Training Plan), will they be a musician or an athlete. They will also update their current notification procedures (Incident Response) in regards to relatives, fire, police, medical and employers.

<u>Systems Planning (Phase 1 for Auditors)</u>

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

Organizational developments require the meeting of management to discuss the need for a new system based on the mission and objectives of the new system. Topics for discussion are for the budget, and system selection

System Analysis (Phase 2 for Auditors)
Organizations begin by analyzing user requirements'; conduct a system analysis, feasibility studies, and a preliminary systems design or architectural design document.

Conceptual Design (Phase 3 for Auditors)
Using the architectural design document as a base this document is updated to include data flow and user description. This process is not limited to single design, but provides different configurations for the same system.

System Evaluation and Selection (Phase 4 for Auditors)
Using the designs prepared in the Conceptual Design additional analysis are conducted to determine the best or most cost effective solution for the new information system. A formal requirements Traceability Matrix needs to be developed in order to determine compliance with stated federal laws, presidential directives and departmental polices and procedures.

During this entire phase we see the adjustment to the Departmental Configuration Management Plan (CMP), Incident Response Plan (IRP), User Training Plan (Initial and Refresher), IT Professional Training Plan (ITPTP), Continuity of Operations Plan (COOP) and the development of the system Business Impact Assessment (BIA), Specialized Training Plan (STP), Contingency Plan (CP), Certification Test and Evaluation Plans and Procedures (CT&E), Security Test and Evaluation Plans and Procedures (ST&E), Threat Analysis Report (TAR), Memorandums of Agreement/Memorandums of Understanding/Interconnected Service Agreements (MOA/MOU/ISA) and other supporting documents.

Phase 2 Acquisitions and Development
Parenthood is a trying and confusing time for both parents as the expected mother has various Trimesters to progress through. There are the visits to the Doctor's office for examinations such as the Sonograms that now allow the determination of the sex of the child. This early determination of the sex allows parents to center their purchases on pink for girls and blue for boys. This period is also devoted to updating their configuration, training, and incident plans for the child.

Systems Evaluation and Selection (Phase 4 for Auditors)
Although this process is included Phase 1 of the SDLC process it needs to be mentioned here as well as applying Murphy's Law that if something can go wrong it will needs to be mentioned here. If during this phase new legislation is passed or technology developments dictate that the design selected is no longer feasible then the system will need to be re-evaluated to determine if it is still feasible to establish. The system may be scrubbed or cancelled at any point during its life cycle.

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

Detailed Designed (Phase 5 for Auditors)
As the system is reviewed for a functionality fit, it needs to be noted that hardware and software to include software or hardware conflicts need to be analyzed to determine the compatibility of components for the system.

Programming and Testing Systems (Phase 6 for Auditors)
Detailed Designed and the Programming and Testing of the System is conducted in a parallel process as they each compliment each other in building the system. This process will have technicians testing each sub-component part for its compatability with other sub-components or components of the overall system. It will also see to the updating of documentation in regards to the SSP, TP, CMP, CP, IRP and COOP.

As the system is acquired, all supporting documentation is to be updated in order to properly certify and accredit the system in a timely manner.

Phase 3 Testing
The testing of a child begins with the delivery of the child during birth. The birth of a child is an ominous occasion for both parents as they rush together to the hospital. Technicians are called for, the doctor, the nurses, the anesthesiologist, cardiologist and others. Then there are the calls to the grand parents, aunts, uncles and cousin to advise all concerned that a new addition to the family has arrived. Both the mother and child are given a battery of tests to ensure their well-being and heath.

Programming and Testing Systems (Phase 6 for Auditors)
Detailed Designed and the Programming and Testing of the System is conducted in a parallel process as they each compliment each other in building the system. This part of the life cycle bears witness to the fact that is entailed in both Phase 2 and 3. Phase 2 is the testing each individual component and testing of all components into a single system. Phase 3 testing is conducted prior to the authorization of the system for live operations under stress conditions.

As the system is acquired, all supporting documentation is to be updated in order to properly certify and accredit the system in a timely manner.

System Implementation (Phase 7 for Auditors)
Once the system has received the approval from the Certifier stating that all operational requirements are in compliance or mitigated to allow full operation of the system. The Designated Approving Authority makes a determination to allow the system to function under the following approvals:

- Interim Approval to Operate (IATO) – approval to operate with restrictions for a maximum period of 1 year, the DAA may stipulate that the IATO be valid for any combination of time periods up to a maximum of 1 year, with the fact that certain corrective actions are to be accomplished during these time periods.
- Approval to Operate (ATO) – approval for the system to operate for a maximum period of three (3) years or less. This approval is usually associated with the fact

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

the DAA is accepting the risk for this system, and may stipulate specific actions that are to be accomplished during this period.

- Denial of Service (DOS) – the DAA has determined that the system has too many outstanding issues in regards to security, operations or requirements that do not offer a safe environment for operations. The issuance of this approval puts the system in a non-operational status and returns the system back to Phase 1 or 2 for re-evaluation and corrective actions.

Phase 4 Operations and Maintenance

During this phase of the life cycle process, we see our children learning to walk, talk, go to school, attend dances, their first date, their skinned knees, how to ride a bicycle, getting married and having their own children.

The issuance of an IATO or ATO puts the system into operations with corrective actions and follow-up reports.

Programming and Testing Systems (Phase 6 for Auditors)

Detailed Designed and the Programming and Testing of the System is conducted in a parallel process as they each compliment each other in building the system.

This process is an on-going process once the system has received an IATO or ATO as the system is now place in a constant state of flux due to changes in hardware/software or technology requirements.

System Implementation (Phase 7 for Auditors)

The system is monitored for compliance, changes in security and costs of operations.

System Maintenance (Phase 8 for Auditors)

See the above comments for this section.

Phase 5 Disposal

During the life of a person, we all prepare and dream for the day that we can retire. We plan of traveling, golfing, fishing, hunting, sleeping in late, and best of all spoiling our own grandchildren. We plan on pumping our grand children full of sugar and sending them home to their parents, for payback for the wild animals that they were, when they were are our own children.

Although there is no mention of this section for an auditor, it is obvious that when a system is disposed of certain actions must be taken such as:

- Sanitization of storage devices – information may still be classified or useful to persons of unknown origins.
- Disposition of hardware components – hardware maybe reused by other organizations or sold as scrap materials.
- Hardcopy materials – architectural diagrams, printed outputs and systems documentation will need to be disposed of in accordance with departmental policies and procedures.

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

The relationship between C&A, Auditing and SDLC is a matter of different wording and interpretation, but for the most part SDLC is the process by which C&A implements management decision for security with auditing being the investigator that verifies the compliance of the SDLC process. Although the auditor verifies the implementation, there is no enforcer that forces any department or agency to completely adherent to established procedures as there is a different C&A process for nearly every federal agency to follow.

The best depiction of a Life Cycle Management Process is the 2004 version of a Wall Chart listed as The Integrated Defense Acquisition Management Framework Chart. This chart is a training aid for Defense Acquisition University (DAU) courses, designed to serve as a pictorial roadmap of key activities in the capabilities development and systems acquisition processes. The Chart illustrates the interaction of the three key major decision support systems – Capabilities Development (Joint Capabilities Integration & Development System (JCIDS)), Acquisition Management (Defense Acquisition System), and the Planning, Programming, Budgeting, and Execution (PPBE) process. This chart is based primarily on policies from the following Department of Defense (DoD) documents:

- DoD Directive (DoDD) 5000.1, *The Defense Acquisition System*
- DoD Instruction (DoDI) 5000.2, *Operation of the Defense Acquisition System*
- CJCS Instruction (CJCSI) 3170.01D, *Joint Capabilities Integration and Development System*
- CJCS Manual (CJCSM) 3170.01A, *Operation of the Joint Capabilities and Integration System*
- CJCS Instruction 6212.01C, *Interoperability of Information Technology and National Security Systems*

How to Obtain Copies[3]

Download from the Defense Acquisition University (DAU) Press web site at: http://www.dau.mil.

Military and government employees can obtain a **single** copy from:

DAU Publications Distribution Center,
Room 7, Bldg 231
Defense Acquisition University Campus,
Fort Belvoir, VA.

A copy can also be obtained by sending a written request for DAU Chart Number _____ to the DAU Publications Distribution Center.

Defense Acquisition University
Attention: OP-CL Publication/Distribution
9820 Belvoir Road, Suite G-3
Fort Belvoir, VA 22060-5565
E-mail: jeff.turner@dau.mil
Phone: (703) 805-2743
DSN 655-2743

[3] This contact information is 3 years old and may no longer be valid.

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

FAX: (703) 805-3726

Copies can be purchased from the U.S. Government bookstore at

http://bookstore.gpo.gov.

Orders can also be placed with credit card at (202) 512-1800 or FAX (202) 512-2250.

© SANS Institute 2007, Author retains full rights.

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

Last Updated: May 25th, 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