



CERTIFICATION AND ACCREDITATION FUNDAMENTALS

**CERTIFICATION
AND
ACCREDITATION
TRAINING
COURSE
OFFERINGS**

Course:
C_A101

Title:
**C&A
Fundamentals**

Duration:
3 days

Size:
25 Max

Prerequisites:
None

DESCRIPTION:

The Federal Information Security Management Act (FISMA) directed the National Institute of Standards and Technology (NIST) to develop a comprehensive security certification and accreditation (C&A) process for information systems that support the federal government. The guidelines for implementing this process are contained in NIST Special Publication (SP) 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems". SeNet has designed this introductory course to train Government personnel and their contractors on the fundamentals of this process.

INTENDED AUDIENCE:

Government personnel and their contractors who are:

- Authorizing Officials, Authorizing Official Designated Representative, Chief Information Officers, Senior Agency Information Security Officers, Risk Executives, Information System Owners, Common Control Providers, Information Owners, Information System Security Officers, Information System Security Engineers, Security Control Assessors, and User Representatives.
- Tasked with performing or maintaining their organizations system/network C&A process.
- Responsible for any portion of a C&A effort but have less than one year of active participation in the process.
- Interested in learning how to build the team necessary to conduct a successful, efficient C&A effort.

COURSE TOPICS:

C&A Process Background

Introduction to the FISMA, OMB and NIST statutory requirements of the C&A process.

Purpose and Applicability

A presentation of the role of NIST SP 800-37 in providing guidelines for the risk-based security process of federal information systems with the purpose of enhancing the security of Federal IT systems.

C&A Roles and Responsibilities

A discussion of the statutory C&A responsibilities entrusted to Government personnel.

C&A Fundamentals

The new security authorization process described in NIST SP 800-37 creates a common process to authorize federal information systems for operation as related to the topic areas below:

- | | |
|----------------------------|---|
| ➤ Accreditation Boundaries | ➤ Authorizing Decisions |
| ➤ Authorization Package | ➤ C&A & the SDLC |
| ➤ Continuous Monitoring | ➤ Control Inheritance and Common Controls |
| ➤ Risk Assessment | ➤ Roles and Responsibilities |
| ➤ System Testing | |

The C&A Process (Current and Future)

An overview of the 4 phase process (Initiation, Security Certification, Security Accreditation and Continuous Monitoring) and how it will be enhanced in the future (NIST SP 800-37, Rev-1).

The Security Authorization Process

The soon-to-be implemented 3 phase security authorization process is compared and contrasted to the current certification and accreditation process throughout this course of instruction.



PHASE I - INITIATION

**CERTIFICATION
AND
ACCREDITATION
TRAINING
COURSE
OFFERINGS**

Course:
C_A102-1

Title:
**Phase I -
Initiation**

Duration:
3 days

Size:
25 Max

Prerequisites:
C_A101

DESCRIPTION:

This session covers the basic documents and tasks involved in the initial documentation phase of the C&A process. Attendees will learn what goes into each of the documents that are required for certification and accreditation of information systems under FISMA and NIST SP 800-37.

INTENDED AUDIENCE:

Government personnel and their contractors who are:

- Responsible for performing, reviewing and/or maintaining their organizations system/network certification and accreditation.
- Authorizing Officials, Authorizing Official Designated Representative, Chief Information Officers, Senior Agency Information Security Officers, Risk Executives, Information System Owners, Common Control Providers, Information Owners, Information System Security Officers, Information System Security Engineers, Security Control Assessors, and User Representatives.

COURSE TOPICS:

Activities Overview

An overview of C&A initiation activities. This course addresses all components of the C&A package.

Developing System C&A Plan

This segment details developing a C&A plan for your organization.

Developing System Certification Boundary

This segment explains how to identify the components to be included within a system boundary and how to develop and sustain an information system boundary.

System Security Categorization

This segment explains how to assess and categorize an information system in accordance with FIPS-199 and NIST SP 800-60 recommendations as related to the organization's mission.

Privacy Impact Statement Review

How to create, review and incorporate Personal Identifiable Information (PII) into the security package.

Developing the Initial System Security Plan (SSP)

This segment details the components of an SSP and how to develop an initial SSP. It also provides a basis for security control definition, selection and implementation. The different families of controls are discussed in this segment in detail.

Initial Risk Assessment Report

This segment details how develop an initial Risk Assessment Report.

ISA/SLA/MOU Agreements

This segment details how to develop interconnection support agreements that help define your system boundary and security responsibilities.



PHASE II = SECURITY CERTIFICATION

**Certification
and
Accreditation**

**Training
Course
Offerings**

**Course:
C_A102-2**

**Title:
Phase II -
Security
Certification**

**Duration:
3 days**

**Size:
25 Max**

**Prerequisites:
C_A101
C_A102-1**

DESCRIPTION:

This session covers the basic tasks involved in the certification phase of the C&A process. This phase of the C&A process is about execution of security control assessments for components of an information system. This session covers how to develop the plans for testing those components and then executing those tests and analyzing the results.

INTENDED AUDIENCE:

Government personnel and their contractors who are:

- Responsible for performing or maintaining their organizations system/network certification and accreditation and testing.
- Authorizing Officials, Authorizing Official Designated Representative, Chief Information Officers, Senior Agency Information Security Officers, Risk Executives, Information System Owners, Common Control Providers, Information Owners, Information System Security Officers, Information System Security Engineers, Security Control Assessors, and User Representatives.

COURSE TOPICS:

Activities Overview

An overview of C&A security certification activities.

Scheduling C&A Activities

How to schedule your C&A activities with all stakeholders and successfully coordinate and execute certification activities.

Preliminary Documentation Review

Performing an preliminary document review can be tedious and painstaking. This segment presents how to do it efficiently and avoid the common pitfalls associated with poor initial C&A package documentation that might result in failing external audits.

Developing ST&E (Security Control Assessment) Plans

This segment details how to develop ST&E plans. A detailed discussion of security control assessment guidelines and configuration lists is given as part of this segment.

Executing ST&E (Certification Testing)

Certification testing and reporting techniques (ST&E report and SAR) are presented in detail in this segment. Hands-on testing labs are addressed in course C_A102-2L.

Risk Assessment Update

This segment teaches how to update your Risk Assessment Reports based upon certification testing results. In addition, this segment teaches how to assess the threat, likelihood, and impact analysis of vulnerabilities identified during the certification testing in accordance with NIST SP 800-30 recommendations.

System Security Plan (SSP) Update

This segment teaches how to update your SSP based upon the results of the certification testing. Additionally, this segment identifies the linkage between the results of the certification testing and the final statuses of control implementations for the information system.

C&A Package Preparation and Delivery

This segment teaches how to verify that the final C&A package is complete, consistent, accurate and satisfies NIST, Departmental and Agency requirements.



PHASE II = SECURITY CERTIFICATION + LAB

**CERTIFICATION
 AND
 ACCREDITATION
 TRAINING
 COURSE
 OFFERINGS**

**Course:
 C_A102-2L**

**Title:
 Phase II –
 Security
 Certification +
 LAB**

**Duration:
 5 days**

**Size:
 15 Max**

**Prerequisites:
 C_A101
 C_A102-1**

DESCRIPTION:

The Federal Information Security Management Act (FISMA) directed the National Institute of Standards and Technology (NIST) to develop a comprehensive security certification and accreditation (C&A) process for information systems that support the federal government. The guidelines for implementing this process are contained in NIST Special Publication (SP) 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems". SeNet has designed this introductory course to train Government personnel and their contractors on the fundamentals of this process.

INTENDED AUDIENCE:

Government personnel and their contractors who are:

- Responsible for performing or maintaining their organizations system/network certification and accreditation and testing.
- Information System Owners, Common Control Providers, Information Owners, Information System Security Officers, Information System Security Engineers, and Security Control Assessors.

COURSE TOPICS:

Activities Overview

An overview of C&A security certification activities.

Scheduling C&A Activities

How to schedule your C&A activities with all stakeholders and successfully coordinate and execute certification activities.

Preliminary Documentation Review

Performing an preliminary document review can be tedious and painstaking. This segment presents how to do it efficiently and avoid the common pitfalls associated with poor initial C&A package documentation that might result in failing external audits.

Developing ST&E (Security Control Assessment) Plans

This segment details how to develop ST&E plans. A detailed discussion of security control assessment guidelines and configuration lists is given as part of this segment.

Executing ST&E (Certification Testing)

Certification testing and reporting techniques (ST&E report and SAR) are the subjects addressed in this segment. The testing tasks are presented in detail and hands on lab experience is gained in this segment. Labs include:

- | | |
|---|--------------------------------------|
| Lab 1 – Network Scans | Lab 4 – Application Testing |
| Lab 2 – Host-Based Testing | Lab 5 – Database, Web Server Testing |
| Lab 3 – Penetration/Vulnerability Testing | Lab 6 – Analyzing Test Results |

Risk Assessment Update

This segment teaches how to update your Risk Assessment Reports based upon certification testing results. In addition, this segment teaches how to assess the threat, likelihood, and impact analysis of vulnerabilities identified during the certification testing in accordance with NIST SP 800-30 recommendations.

System Security Plan (SSP) Update

This segment teaches how to update your SSP based upon the results of the certification testing. Additionally, this segment identifies the linkage between the results of the certification testing and the final statuses of control implementations for the information system.

C&A Package Preparation and Delivery

This segment teaches how to verify that the final C&A package is complete, consistent, accurate and satisfies NIST, Departmental and Agency requirements.



SECURE APPLICATION ENGINEERING FUNDAMENTALS

**CERTIFICATION
 AND
 ACCREDITATION
 TRAINING
 COURSE
 OFFERINGS**

**Course:
 CAE101-1**

**Title:
 Secure
 Application
 Engineering
 Fundamentals**

**Duration:
 1 day**

**Size:
 15 Max**

**Prerequisites:
 None**

DESCRIPTION:

This session covers the fundamentals of SeNet’s secure application engineering methodology which based on the NIST 800-37 Revision 1 “Guide for Security Authorization of Federal Information Systems: A Security Life Cycle Approach”. The new NIST 800-37 drastically changes how information system security is address by applying a revised Risk Management Framework approach. This session will introduce the attendees to the concepts of the Risk Management Framework as they apply to the Systems Development Lifecycle for the engineering and security of an information system.

INTENDED AUDIENCE:

Government personnel and their contractors who are:

- Responsible for engineering or maintaining their organizations applications.
- Information System and Application Engineers, Information Owners, Information System Security Officers, Information System Security Engineers, and Executive Management interested in the concepts of SAE.

COURSE TOPICS:

Activities Overview

An overview SAE course activities.

Secure Application Engineering

What is Secure Application Engineering?
 Why Do It?
 How To Do It?

Security Authorization Process and Risk Management

This segment covers the basics of the new Security Authorization Process formerly known as C&A (Certification and Accreditation). It covers the concepts associated with a holistic approach in addressing the risks from an aggregate view of an agency’s system security perspective.

NIST 800-37 Rev1 Fundamentals

This segment details the revised Risk Management Process for the Security Authorization of an Information System as presented in the NIST guidance. It covers the following:

- | | |
|---|---|
| <ul style="list-style-type: none"> • Security Authorization Process Details • Security Control Assessments • Preparation, Execution and Maintenance • Maintenance Phase (Continuous Monitoring) | <ul style="list-style-type: none"> • Security Authorizations • Security Authorization Package • RMF Six Steps • Risk Executive Role |
|---|---|

SAE Security Tasks

This segment covers the SAE Security Tasks Overview as well as delving into the details associated with each task.

SAE Benefits

This segment covers the programmatic and budgetary benefits of the SAE.

System Security Plan (SSP) Update

This segment teaches how to update your SSP based upon the results of the certification testing. Additionally, this segment identifies the linkage between the results of the certification testing and the final statuses of control implementations for the information system.

C&A Package Preparation and Delivery

This segment teaches how to verify that the final C&A package is complete, consistent, accurate and satisfies NIST, Departmental and Agency requirements.