



CDC UNIFIED PROCESS PROCESS GUIDE



CERTIFICATION AND ACCREDITATION PROCESS GUIDE

Purpose of the Process Guide

CDC projects are required to comply with various CDC and Federal regulations, mandates, policies, processes, and standards. Information about these requirements is available from various websites and supporting documents. However, this information is often not presented from the perspective of the project team and their roles & responsibilities in complying with these requirements. CDC UP Process Guides provide that perspective.

CDC UP Process Guides help project teams comply with CDC and Federal requirements by:

1. Setting the requirements in the context of their purpose
2. Providing step-by-step instructions for completing the activities required for compliance
3. Illustrating potential integration points between processes
4. Presenting requirements in a concise, easy-to-understand, and consistent format
5. Making that presentation accessible to the CDC community via the CDC Unified Process website

The specific purpose of this Process Guide is to describe the Certification and Accreditation process as it applies to project teams.

Process Overview

The security process includes the following components:

- Certification and Accreditation (C&A)
- E-Authentication
- Business Continuity Planning (BCP)

Incorporating security into all phases of a project's life cycle is less expensive and more effective than waiting until the execution phase to consider security.

Managing security begins with categorizing the information in an information technology (IT) system according to the level of potential impact (low, moderate, or high) of the loss of confidentiality, integrity, and availability on organizations or individuals, in accordance with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

After the system's information has been categorized, the next steps involve selecting, refining, documenting, and implementing appropriate security controls for the IT system, in accordance with FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*. The Office of the Chief Information Security Officer (OCISO) website (<http://intranet.cdc.gov/ociso/CandA/CandA.html>), located on the CDC Intranet, provides links and detailed information to assist in security categorization, security control selection, refinement, and documentation.

Certification and Accreditation

CDC information systems are certified and accredited based on the standards defined in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. NIST SP 800-37 provides guidelines for the security certification and accreditation of information systems supporting the executive agencies of the federal government, and these guidelines are applicable to all federal information systems other than those systems designated as national security systems, as defined in 44 U.S.C., Section 3542.

Certification and Accreditation (C&A) is the process of formal assessment, testing (certification), and acceptance (accreditation) of system security controls that protect IT systems and data stored in and processed by those systems. It is a process that encompasses the system's life cycle and ensures that



CDC UNIFIED PROCESS PROCESS GUIDE



CERTIFICATION AND ACCREDITATION PROCESS GUIDE

the risk of operating a system is recognized, evaluated, and accepted. The C&A process implements the concept of “adequate security,” or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information, which is defined in OMB Circular A-130.

The CDC C&A process ensures that information systems are:

- Operating with appropriate management review
- Performing ongoing security control monitoring
- Submitted for reaccreditations before the end of the accreditation period (at least every three years) or when there is a significant change to an information system or its environment, whichever is sooner.

It also involves recommendations to enhance existing system security controls and to implement additional security controls to mitigate system vulnerabilities discovered while conducting a risk assessment.

Systems Requiring Certification

National requirements clearly define what CDC systems must be C&A'd:

FISMA Extract...§ 3544. Federal agency responsibilities -

“(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source...”

NIST 800-53, Rev 1 definition...Federal Information System: An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [40 U.S.C., Sec. 11331]

All computers, down to the single PC must be provided adequate security, or security equal with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. Personal computers in many cases receive blanket C&A due to common system characteristics. Server based computers hosting applications require more analysis and generally require individual C&A. System environment analysis is often necessary to define system specific C&A requirements.

Must Government contractors abide by FISMA requirements?

Yes and each agency must ensure their contractors are doing so. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including “information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.” Section 3544(b) requires each agency to provide information security for the information and “information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.” This includes services which are either fully or partially provided, including agency hosted, outsourced, and software-as-a-service (SaaS) solutions. (OMB Memorandum 07-19, pp. 14-15)

- **Security Certification** is a comprehensive evaluation of CDC management, operational, and technical security controls for an information system. This evaluation documents the effectiveness of existing security controls in a particular operational environment and includes recommendations to implement additional controls to mitigate outstanding system vulnerabilities. Security certification results are used to assess risks to the system and update the system’s security plan.
- **Security Accreditation** is the official CDC management decision to authorize an information system to operate. By accrediting an information system, a CDC official is explicitly acknowledging his or her responsibility for adverse impacts to CDC resulting from the documented risk levels for the system. The C&A documents provide the factual basis for a CDC authorizing official to render a security accreditation decision. It is essential that CDC officials have the most complete, accurate, and



CDC UNIFIED PROCESS PROCESS GUIDE



CERTIFICATION AND ACCREDITATION PROCESS GUIDE

trustworthy information possible to make credible, risk-based decisions on whether to authorize system operation. An authority to operate can be granted to a system for any period of time up to three years. A system must be recertified by the time its authority to operate expires.

E-Authentication

E-authentication is the process of establishing confidence in a user's identity when it is electronically presented to an information system. E-authentication ensures that the appropriate degree of system access is granted based on the user identity and the sensitivity of the data being accessed. Information related to complying with E-authentication requirements is provided in the C&A templates available on the OCISO website on the CDC Intranet. OMB Memorandum 04-04, *E-Authentication Guidance*, and NIST SP 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, provide more information on Federal E-Authentication requirements.

Business Continuity Planning

A Business continuity plan (BCP) puts procedures in place that minimize the effect of an interruption to an organization's operations as a result of a natural disaster or other disruption to one or more mission-critical services. A BCP is designed to ensure that essential functions can continue during and after a disaster; and that mission-critical services are fully functional as soon as possible following an interruption. Templates for capturing business continuity planning information are available on the OCISO website on the CDC Intranet. NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, provides more information on Federal information system contingency planning requirements. At CDC, information system business continuity planning activities must align with the *CDC Integrated Emergency Management Plan (IEMP)*, coordinated by the Office of Security and Emergency Preparedness (OSEP) Emergency Manager's Office (EMO), and the *CDC Incident Response Plan*, and coordinated by OCISO.

Process Attributes

This section provides a list of process attributes to help project teams better understand the requirements necessary to comply with this process and to determine when and how they may impact their project.

PROCESS ATTRIBUTE	DESCRIPTION
Process Owners	Tom Madden (CDC Chief Information Security Officer) and Cheri Gatland-Lightner, C&A certification agents located in the Office of the Chief Information Security Officer (OCISO)
Process Criteria	All IT projects meeting the following conditions: (A) the project will involve information collected or maintained by or on behalf of the CDC; or (B) information systems that are used or operated by the CDC, by a CDC contractor, or by another organization on behalf of the CDC.
Timing of Process in Project Life Cycle	Security management begins during the planning phase of a project and continues throughout the entire lifecycle.
Estimated Level of Effort	Depending upon the type and size of the project, it requires between 200 and 400 hours to complete the Full C&A process including the BCP templates.
Associated Costs	Full C&A: Costs for the initial Full C&A on CDC's most critical systems have ranged from \$40K to over \$150K per system, and it has usually taken around 50 to 60 business days to achieve ATO. The cost of resulting POA&M items needed to address security weaknesses in systems range from \$40K to over \$1.5M. Moreover, as the C&A process must be repeated every three years, this effort and expense is cyclical and requires advance planning. <u>Enterprise Master System Security Plan (EMSSP) C&A</u> : Systems that meet the EMSSP C&A process criteria will have a shorter time to C&A completion than systems that undergo a Full C&A. Since the four EMSSPs are managed



CDC UNIFIED PROCESS PROCESS GUIDE



CERTIFICATION AND ACCREDITATION PROCESS GUIDE

PROCESS ATTRIBUTE	DESCRIPTION
	<p>by OCISO, there are no direct costs to C//Os for commonly-managed security controls, for systems that complete the EMSSP C&A process. However, C//Os are responsible for costs related to system-specific controls, along with the mitigation of system-specific POA&M items that may result from an EMSSP C&A. CIOs are also responsible for cost of completing C&A packages submitted to OCISO for validation.</p> <p>If the project doesn't have a resource available to assist with completing the necessary documentation; OCISO offers these services for a fee.</p> <p>The project team can also contract with an external resource to assist with completing the required templates; however the resource needs to possess prior experience with the CDC's C&A processes.</p>
Process Prerequisites	<p>Familiarization with FIPS 199; FIPS 200; NIST SP 800-37; NIST SP 800-53, Revision 2; NIST SP 800-64, <i>Security Considerations in the Information System Development Life Cycle</i>; and NIST SP 800-65, <i>Integrating Security into the Capital Planning and Investment Control Process</i>. FIPS and NIST special publications are available at http://csrc.nist.gov/. OMB circulars and memoranda are available at http://www.whitehouse.gov/omb/. Completion of Privacy Impact Assessment (PIA) documents. (See the CDC UP Process Guide for PIA).</p>
Process Dependencies	<p>Capital Planning and Investment Control (CPIC). CDC CPIC requirements are available at http://intranet.cdc.gov/cpic</p>
Related Systems/Tools	<p><i>CDC Integrated Emergency Management Plan</i> and <i>CDC Incident Response Plan</i></p>
Available Training	<p>Upon request, Field Assistance Visits to C//Os</p>
Additional Information	<ul style="list-style-type: none"> • http://intranet.cdc.gov/ociso/CandA/Full_CandA_Process.html • http://intranet.cdc.gov/ociso/CandA/EMSSP/EMSSP_CandA_Process.html • Office of the Chief Information Security Officer (OCISO) http://intranet.cdc.gov/ociso/CandA/EMSSP/FullCandADocuments_EMSSP-beta.html <ul style="list-style-type: none"> ○ Certification and Accreditation Process ○ System Security Plan Template • OMB Circular A-130 http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf • National Institute of Standards and Technology http://www.nist.gov • FISMA http://csrc.nist.gov/groups/SMA/fisma/index.html • NIST SP 800 Series Publications http://csrc.nist.gov/publications/PubsSPs.html <ul style="list-style-type: none"> ○ SP 800-18, <i>Guide for Developing Security Plans for Federal Information Systems</i> ○ SP 800-30, <i>Risk Management Guide for Information Technology Systems</i> ○ SP 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i> ○ SP 800-53, <i>Recommended Security Controls for Federal Information Systems</i> ○ Draft SP 800-53A, <i>Guide for Assessing the Security Controls in Federal Information Systems</i> ○ SP 800-55, <i>Security Metrics Guide for Information Technology Systems</i> ○ SP 800-60, <i>Guide for Mapping Types of Information and Information</i>



CDC UNIFIED PROCESS PROCESS GUIDE



CERTIFICATION AND ACCREDITATION PROCESS GUIDE

PROCESS ATTRIBUTE	DESCRIPTION
	<p><i>Systems to Security Categories</i></p> <ul style="list-style-type: none"> ○ SP 800-70, <i>Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers</i> ○ SP 800-100, <i>Information Security Handbook: A Guide for Managers</i> ○ SP 800-110, <i>Information System Security Reference Data Model</i> ● Federal Information Processing Standard Publications http://csrc.nist.gov/publications/PubsFIPS.html ○ FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i> ○ FIPS 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i> ● CDC UP Practices & Process Guides http://www2.cdc.gov/cdcup/document_library/practices_guides/ <ul style="list-style-type: none"> ○ Certification & Accreditation (Security) Process Guide ○ Risk Management Practices Guide ○ Configuration Management Practices Guide

Contact List

CDC Information Systems Security Officers (ISSOs) are available to assist project teams in answering questions regarding the content of this Process Guide and related topics. For the most up-to-date list of contacts, refer to the OCISO website at <http://intranet.cdc.gov/ociso/ISSOs.html>.

Key Terms

The CDC Unified Process Team maintains a comprehensive list of key terms and acronyms relevant to all Unified Process artifacts maintained on the CDC UP website. Follow the link below for definitions and acronyms related to this, and other, document.

<http://www2.cdc.gov/cdcup/library/other/help.htm>

Activities Checklist

This section provides a list of steps outlining the activities associated with complying with this process. Due to the dynamic nature of the C&A process a website has been established to communicate the most current information regarding C&A requirements. This website also contains a list of the related templates that assist in completing C&A activities. http://intranet.cdc.gov/ociso/CandA/Full_CandA_Process.html and http://intranet.cdc.gov/ociso/CandA/EMSSP/EMSSP_CandA_Process.html