



# CDC UNIFIED PROCESS PRACTICES GUIDE



## AUTHORIZATION TO OPERATE

### Purpose

The purpose of this document is to provide guidance on the practice of an **Authorization to Operate (ATO)** and to describe the practice overview, example common metrics, best practices, activities, and attributes related to this requirement. In addition, templates relevant to this practice are provided at the end of this guide.

### Practice Overview

An Authorization to Operate (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to agency operations. The ATO is signed after a Certification Agent (CA) certifies that the system has met and passed all requirements to become operational.

All CDC IT systems are required to obtain a signed ATO prior to full start up. The ATO represents the formal management approval to place a system into operation at CDC. An ATO is granted after an IT system fully complies with the Certification and Accreditation (C&A) process. A system must be compliant with the following regulations specified in the C&A process:

- Security Certification
- Security Accreditation
- E-Authentication
- Business Continuity Planning

For IT systems that complete the full C&A Process, the DAA is typically a senior management official, at the division level or above, within a center, institute or office. There are two different ATO forms, the Non-Reportable System/Application ATO and the Reportable System/Application ATO. The Certifying Authority (CA) must sign within the C&A Process pending on level of the [Federal Information Processing Standard Publication \(FIPS PUB\) 199](#), Standards for Security Categorization of Federal Information and Information Systems. The CAs are typically the application sponsors, business steward, system owner, chief information security officer and/or designated approving authority.

FIPS PUB 199 is an important component of a suite of standards and guidelines that National Institute of Technology (NIST) is developing to improve the security in federal information systems, including those systems that are part of the nation's critical infrastructure. FIPS PUB 199 enables agencies to meet the requirements of the Federal Information Security Management ACT (FISMA) and improves the security of federal information systems.

- The CA must use the Reportable ATO form if the system has a high FIPS PUB 199 impact level and/or are critical inventory systems.
- The CA must use the Non-reportable ATO form if the system has a low or moderate FIPS PUB 199 impact level.

The ATO forms can be found in the following link

[http://intranet.cdc.gov/ociso/CandA/Full\\_CandA\\_Process\\_Documentation.html](http://intranet.cdc.gov/ociso/CandA/Full_CandA_Process_Documentation.html)

Note: The Office of the Chief Information Security Officer (OCISO) will not grant an ATO to a web-based system with an application scan containing high vulnerabilities. The CA must collaborate with OCISO to lower the system's vulnerabilities to an acceptable level prior to receiving an ATO. The project officer must submit a self-signed ATO, in PDF format, as part of the C&A package. The Certification Agent (CA) will sign the ATO upon approval of the accepted package.



# CDC UNIFIED PROCESS PRACTICES GUIDE



## AUTHORIZATION TO OPERATE

For additional information, refer to the C&A process guide in the CDC UP website for full compliance details. The link to the C&A process guide can be found in the following link [http://www2.cdc.gov/cdcup/document\\_library/process\\_guides/default.asp](http://www2.cdc.gov/cdcup/document_library/process_guides/default.asp)

### Best Practices

The following best practices are recommended for the practice of **obtaining an ATO**:

- **C&A** – ATO is dependent on a successful completion of the C&A process. It is vital for the CA to understand the C&A process and collaborate with the DAA to effectively facilitate the ATO process.
- **Review** – The CA must review the vulnerabilities (if high) of the system in the ATO process.
- **Manage & Follow up** – The C&A process can be a long process. It is the CA's responsibility to start the C&A process early in order to receive an ATO on a timely fashion.

### Practice Activities

- It is important for the project officer to be familiar with the C&A process. However, CA, application owners, and sponsors should also be familiar with the C&A process. Please refer to C&A process guide for detailed information and guidance.

### Practice Attributes

This section provides a list of practice attributes to help project teams determine when and how applying for **an ATO** impacts a project.

<b>Practice Owner</b>	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)
<b>Criteria</b>	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.
<b>Estimated Level of Effort</b>	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.
<b>Prerequisites</b>	Successful completion of a C&A
<b>Practice Dependencies</b>	Successful completion of a C&A
<b>Practice Timing in Project Life Cycle</b>	ATO is an activity that is performed with the C&A process. Security management begins during the planning phase of a project and continues throughout the entire lifecycle.
<b>Templates/Tools</b>	<ul style="list-style-type: none"> <li>• C&amp;A process guide <a href="http://www2.cdc.gov/cdcup/document_library/process_guides/default.asp">http://www2.cdc.gov/cdcup/document_library/process_guides/default.asp</a></li> <li>• Reportable and Non Reportable ATO forms <a href="http://intranet.cdc.gov/ociso/CandA/Full_CandA_Process_Documentation.html">http://intranet.cdc.gov/ociso/CandA/Full_CandA_Process_Documentation.html</a></li> </ul>
<b>Additional Information</b>	<a href="http://intranet.cdc.gov/ociso/CandA/Full_CandA_Process.html">http://intranet.cdc.gov/ociso/CandA/Full_CandA_Process.html</a> <a href="http://intranet.cdc.gov/ociso/CandA/EMSSP/EMSSP_CandA_Process.html">http://intranet.cdc.gov/ociso/CandA/EMSSP/EMSSP_CandA_Process.html</a>

### Related Templates/Tools

Below is a list of template(s) related to this practice. Follow the link below to download the document(s).