Personnel and Readiness Information Management

Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)

What is DIACAP?

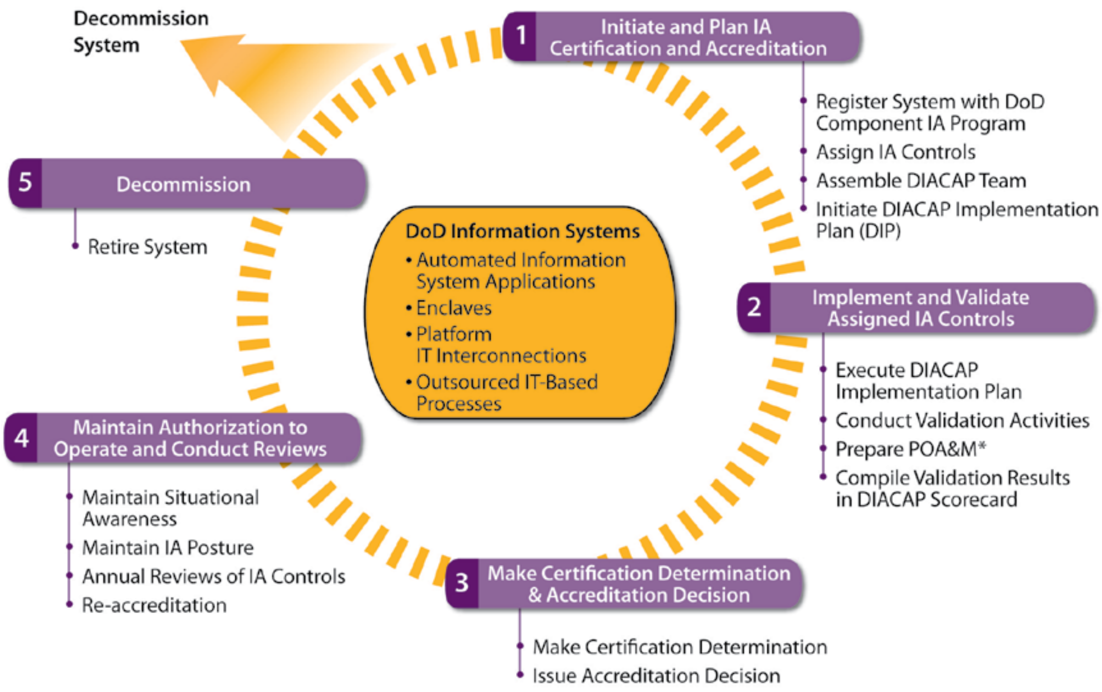
The Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) is a process by which information systems are certified for compliance with DoD security requirements and accredited for operation by a designated official. DIACAP provides visibility and control for the secure operation of DoD information systems.

The DIACAP considers:

- Mission or business need
- Protection of personally identifiable information
- Protection of the information being processed
- Protection of the system's information environment

What Is The Process For Becoming DIACAP Compliant?

The DIACAP includes five main activities necessary for compliance, as outlined in the diagram below.



Decommission System

1 Initiate and Plan IA Certification and Accreditation

- Register System with DoD Component IA Program
- Assign IA Controls
- Assemble DIACAP Team
- Initiate DIACAP Implementation Plan (DIP)

2 Implement and Validate Assigned IA Controls

- Execute DIACAP Implementation Plan
- Conduct Validation Activities
- Prepare POA&M*
- Compile Validation Results in DIACAP Scorecard

3 Make Certification Determination & Accreditation Decision

- Make Certification Determination
- Issue Accreditation Decision

4 Maintain Authorization to Operate and Conduct Reviews

- Maintain Situational Awareness
- Maintain IA Posture
- Annual Reviews of IA Controls
- Re-accreditation

5 Decommission

- Retire System

DoD Information Systems

- Automated Information System Applications
- Enclaves
- Platform IT Interconnections
- Outsourced IT-Based Processes

* See the reverse side for more information

Who Should Be Informed About DIACAP?

The DIACAP is important in continually managing the Information Assurance (IA) posture of an organization. It ensures that risk management is applied to information systems within the DoD in order to protect personal privacy, the information environment, and other missions reliant upon shared information.

System Owners, Program Managers, and IA staff should be aware of and understand the DIACAP. This is to establish and/or confirm that IA controls are implemented correctly and effectively within the organization. Individuals with responsibilities over the following tasks should be informed about DIACAP:

- Information system security management and oversight;
- Information system and IA control assessment and monitoring; and
- IA implementation and operation.

For more information, please visit the P&R IM DIACAP webpage online at **http://www.prim.osd.mil/cap/dhra-diacap.html?p=1.1.1.1**.

Personnel and Readiness
Information Management

How Do I Maintain My System's ATO?

The Department of Defense Instruction (DoDI) 8500.2 implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under reference. Validation of the DoDI 8500.2 controls must be performed prior to the Accreditation Decision and annually thereafter. A system must draft exception memoranda for IA controls where risk will be assumed and perform quarterly scans. Upon completion of these scans, the system administrator must patch, fix, mitigate, and document open findings.

When Do I Need To Acquire A New ATO For My System?

If the system requires a new ATO before the re-authorization date, it must go through the DIACAP for recertification. There are two reasons why a system would require a new ATO:

- The system is brand new
- Major changes were made to the system such as:
  - Changing the system location
  - Major alterations to the system code

Please refer to DoDI 8501.01 "DoD Information Assurance Certification and Accreditation Process (DIACAP)" to determine whether "major changes" to your system qualifies for a new ATO. DoDI 8501.01 is located online at http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf.

If you have any questions regarding HRM Systems and DIACAP, contact P&R IM at **HRMCIOSupport@osd.pentagon.mil**.

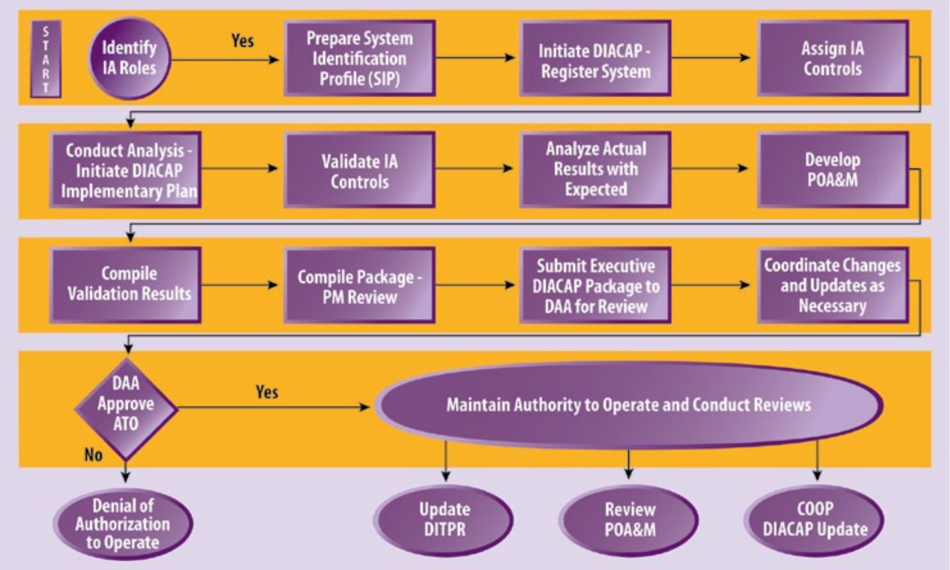
The DIACAP package is comprised of five major artifacts:

1) System Identification Profile (SIP) – the set of information gathered during system registration;
2) DIACAP Implementation Plan (DIP) – the plan that contains the strategy for system implementation and the current implementation status of assigned IA Controls for a system;
3) Supporting Documentation for Certification – documents that include actual validation results and artifacts associated with implementation of IA Controls;
4) DIACAP Scorecard – a tool intended to convey information about the IA posture of a DoD information system; and
5) Plan of Action & Milestones (POA&M) – a tool identifying tasks that need to be accomplished to remediate any identified vulnerabilities in a program or system.

What Are The Certification and Accreditation Decisions and How Are They Made?

A Certification Determination is made by a Certification Authority (CA), an active member of the DIACAP Team. The CA assigns a Severity Code – an assessment of the likelihood of system wide IA consequences – to specific findings or deficiencies identified during certification. The Severity Codes are expressed as CAT I, CAT II, and CAT III. CAT I is an indicator of the greatest risk and urgency, and will prevent the system from acquiring an ATO.

The formulation of an Accreditation Decision is made after a certification recommendation has been made, which is supported by the DIACAP Package. The Accreditation Decision applies to an operationally ready instance of a DoD information system and is a balance of the DIACAP considerations.


START
Identify IA Roles
Yes
Prepare System Identification Profile (SIP)
Initiate DIACAP - Register System
Assign IA Controls
Conduct Analysis - Initiate DIACAP Implementary Plan
Validate IA Controls
Analyze Actual Results with Expected
Develop POA&M
Compile Validation Results
Compile Package - PM Review
Submit Executive DIACAP Package to DAA for Review
Coordinate Changes and Updates as Necessary
DAA Approve ATO
Yes
Maintain Authority to Operate and Conduct Reviews
No
Denial of Authorization to Operate
Update DITPR
Review POA&M
COOP DIACAP Update

The diagram above shows a process chart for the DIACAP.

What Are The Differences Between The Accreditation Decisions?

Once the Designated Approval Authority (DAA) has reviewed the system information and recommendation, there are four possible DAA accreditation decisions that can be made:

- Authorization to Operate (ATO) – full operation approval with a duration of three years;
- Interim Authorization to Operate (IATO) – allows operation to manage IA security weaknesses for a maximum of six months ;
- Interim Authorization to Test (IATT) – a special case for authorizing testing allowing operation for a limited time; or
- Denial of Authorization to Operate (DATO) – issued if a DoD information system has inadequate IA design. If you receive a DATO, please contact your organization's IA professional.

NOTE: If an Accreditation Decision has not been issued, a system is considered "unaccredited" and is not allowed to operate.