GOT DIACAP?

What is DIACAP?

The Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) is a set of processes by which information systems (ISs) are certified for compliance with the DoD security requirements. All ISs in the DoD require an Authority To Operate (ATO) before they become fully operational. In order to gain an ATO, a DIACAP must be executed by designated Information Assurance (IA) professionals to ensure that risk management is applied and each system is safeguarded.

When Do I Need the DIACAP?

If you have any ISs that will interface with external sources or have users outside your immediate organization, you must have an ATO. A DIACAP is required to obtain an ATO. If you are unsure if your IS requires a DIACAP, contact your nearest Information Assurance (IA) professional or the Defense Human Resources Activity (DHRA) Chief Information Office (CIO) IA contact.

When Should I Start the DIACAP?

Each DIACAP is tailored to the complexity of the system, so some will take longer than others. At a minimum, you should engage your IA professional within one year of the proposed system launch date as DIACAP can take up to one year to execute. It is far easier to incorporate the required IA controls during development rather than afterwards when an ATO is needed. Incorporating IA at the beginning reduces the risk of reworking or delayed deployment schedules.

What Is the Process For Becoming DIACAP Compliant?

The DIACAP considers an agency's mission or business need, the protection of personal privacy, the protection of the information being processed, and the protection of the system's information environment. Key artifacts in the process include identifying IA Roles, preparing the System Identification Profile (SIP), initiating the DIACAP Implementation Plan (DIP), developing a Plan of Action and Milestones (POA&M), and receiving the ATO.

Outline of the Five Main DIACAP Phases