

DIACAP: COMPLY WITH CONFIDENCE



CONTACT

Prem Iyer, CISSP/PMP
Practice Director
Information Security
infosec@ironbow.com

Depending upon what is being certified, DIACAP (DoD Information Assurance Certification and Accreditation Process) can involve anywhere from 100 – 120 IA controls and can take six months to a year to complete. It is tedious, complex, time-consuming and often outsourced. However, outsourcing could lead to lost time and money if the team you have chosen to do the work doesn't really understand the process.

How can you minimize costs, time delays and ensure a smooth process? Put your trust in the DIACAP experts at Iron Bow Technologies.

MINIMIZE COSTS AND HASSLES

The Iron Bow Information Security Team has been performing DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) and DIACAP assessments since its establishment in 2002. Our dedicated C&A team has completed 432 efforts over eight years, averaging about 72 per year.

Get all the time and cost advantages that experience provides with an Iron Bow team dedicated to your DIACAP project.

Year	Completed Efforts
2010	89
2009	87
2008	79
2007	73
2006	49
2005	55

With this experience comes knowledge of items that can be problematic with DIACAP, including issues that arise with virtualized environments, recertification of DITSCAP certified equipment to DIACAP certification and artifact development.

From initiating and executing the DIACAP Implementation Plan (DIP) to supporting the Program Manager/System Manager in maintaining accreditation, we have proven processes and templates in place that minimize costs, reduce timelines and ensure a smooth experience.

THE IRON BOW ADVANTAGE

- Proven, repeatable processes that ensure effective use of resources
- Tailorable templates provide consistent quality and eliminate the need to generate documents from scratch
- Flexible, team-oriented approach
- Industry-certified, trained, cleared and experienced staff
- Dedicated DIACAP team that works on C&A every day

A DEDICATED, EXPERIENCED TEAM

Assessments are conducted by our Information Assurance Team (Engineer(s) and Analyst) who are DIACAP experienced, certified IAW DoD 8570.01M and have current DoD IA training required for system access. Specific certifications include CISM, CISA, CISSP, ISSEP, CAP, Security +, CCNA, NSA-IAM and CEH. Our team holds appropriate active Secret, TS and TS/SCI clearances.

We take a flexible team approach. Clients can confidently leverage our expertise to complete some or all of the DIACAP tasks in order to get the job done.

WHAT TO EXPECT DURING A DIACAP ASSESSMENT

DIACAP is conducted IAW DoD 8500 series and NIST guidance. It involves defining the security boundary, assessing artifacts (documentation), testing the system (manual and automated) against 8500.2 controls, validation of mitigation activities and a report with recommendation for the Designated Approving Authority (DAA).

Assessments start with a pre-kickoff meeting where a formal activity timeline and responsibilities are identified. At kickoff, everyone is informed of their roles, responsibilities, timeline and deliverables. Status reports are routinely made to the Program Manager or System Manager as activities progress.

System artifact/documentation and system testing will be IAW 8500.2. Based on the architecture, hardware and software, testing will be conducted utilizing Industry, DoD and DISA tools and guidance (i.e. STIGs, SRRs and security checklists). A comprehensive C&A package is generated to include System Identification Profile (SIP), DIP, Supporting Certification Documentation (artifacts), DIACAP Scorecard and IT Security Plan of Actions & Milestones (POA&M).

The resources needed to complete a DIACAP assessment are determined by the scope of the network/system to be assessed. The scope is determined by the number of configuration items, workstations and interfaces, and the number of facilities and their locations.

SERVICES

Whether you need C&A on new technologies being integrated into your enterprise, or DITSCAP on existing technologies with DIACAP certifications about to expire, our team can help with some or all of the tasks.

Services & Activities:	Deliverables:
<ul style="list-style-type: none"> • Project Management • Artifact Review • Test Plan Development • System Testing (Manual and Automated) • Remediation Recommendations • Mitigation Strategy Development • Development of C&A Package 	<ul style="list-style-type: none"> • System Identification Profile (SIP) • DIACAP Implementation Plan (DIP) • Supporting Certification Documentation • DIACAP Scorecard • IT Security Plan of Action & Milestones (POA&M)

Contact our experts today to see how we can streamline and fortify your certification and accreditation processes at infosec@ironbow.com.