

Security Certification & Accreditation (C&A)

International Field Directors & Technologies Conference

Charles Armstrong, NORC

What is C & A

- Risk management framework to ensure security of Federal Information Systems
 - Based on NIST 800-53 Security Controls for Federal Information Systems
 - All federal information systems must complete the C&A program before system can be put into operation
 - C&A process is performed on a per agency basis
-

Impact of C&A

- More federal contracts require that C&A be achieved for any systems that handle federal information
 - The C&A process can be a long process depending on the size and complexity
 - Additional tools may be needed
 - The C&A process is ongoing. Requires continuous auditing and reporting
-

Major Components of C&A

- System Security Plan
 - Risk Assessment
 - Configuration Management
 - Incident Response Plan
 - Contingency Plan
 - Security Awareness Program
-

Steps to Success

- Need to have senior management support
 - The C&A process is not only an IT issue
 - Identify teams from across the company including HR, facilities, and users
 - Do not under estimate effort to complete the C&A process and maintain it. Proper planning and ownership must be defined.
-

Scope

- Define data classification (FIPS 199) to determine appropriate security controls
 - Low, moderate, high
 - Define the scope (boundaries) of the information system
 - Data flow diagram of system
 - Do not over complicate a simple system
 - External vendors
-

Policies and Procedures

- C&A process requires many policies
 - Do not under estimate the time and effort to define and approve policies
 - C&A procedures
 - Generates a lot of documentation. If you say you do something, you should have a procedure for it.
 - Organize policies and procedures for easy access and management
-

Auditing & Reporting

- Verifies security plan is being executed properly
 - System security scans, logging, event log reports
 - Alerts to security issues
 - Plan of Action and Milestones (POAM)
-

Conclusion

- C&A uses the NIST 800-53 framework for security
 - Company initiative not just an IT initiative
 - Do not under estimate the effort required
 - Ensure procedures can be audited
-

Helpful Web Sites

- General NIST Security Documents
<http://csrc.nist.gov/publications>
 - NIST Guide for the Security Certification and Accreditation
<http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>
 - NIST 800-53
<http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf>
-

Thank You

Contact Information:

Charles Armstrong

Armstrong-charles@norc.org

CISSP
