



Preparing for the Certification & Accreditation Process

- Making Security a Fundamental Part of the SDLC -

*Timothy Watt
Technical Director
Tenacity Solutions, Inc.*

6th Annual OWL Cross-Domain Solutions Forum - April 21, 2010

The SDLC & Security Processes

The SDLC & Security Processes

Security in the SDLC - Guidance

“Consideration of security in the System Development Life Cycle is essential to implementing and integrating a comprehensive strategy for managing risk...”

- NIST SP 800-64 rev2

Security in the SDLC – Formal Requirement

■ SA-3 Life Cycle Support

– The organization:

- a. Manages the information system using a system development life cycle methodology that includes information security considerations;
- b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
- c. Identifies individuals having information system security roles and responsibilities.

NOTE: SA-3 part of Low, Moderate, and High “baselines”

SDLC Phases

- **Phases in the SDLC**

- Initiation
- Development/Acquisition
- Implementation
- Operation/Maintenance
- Disposal

SDLC Phases	Initiation	Development & Acquisition	Implementation		Operation & Maintenance	Disposal
Security Authorization Process (C&A)	Initiation		Certification	Accreditation	Continuous Monitoring	

SDLC - Initiation Phase

- **During the Initiation Phase, the need for a system is expressed and the purpose of the system is documented - key security activities include:**
 - Document business requirements - - - > C – I – A
 - Define information categorization and any “special requirements”
 - Determination of any privacy requirements

SDLC – Development & Acquisition

- **During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed - key security activities include:**
 - Conduct the risk assessment and use the results to supplement the baseline security controls;
 - Analyze security requirements;
 - Perform functional and security testing;
 - Prepare initial documents for system certification and accreditation; and
 - Design security architecture.

SDLC – Implementation

- **During this phase and after system acceptance testing, the system is certified , authorized to operate and installed or fielded - key security activities include:**
 - Integrate the information system into its environment;
 - Plan and conduct system certification activities in synchronization with testing of security controls; and
 - Complete system accreditation activities.

SDLC – Operation & Maintenance

- **During this phase, the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events - key security activities include:**
 - Conduct an operational readiness review;
 - Manage the configuration of the system;
 - Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and
 - Perform reauthorization as required.

SDLC – Disposal

- **Activities conducted during this phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies - key security activities include:**
 - Build and Execute a Disposal/Transition Plan;
 - Archive of critical information;
 - Sanitization of media; and
 - Disposal of hardware and software.

SDLC – The Benefits to Integration

- **Integration of security in the SDLC enables maximization of return on investment in their security programs, through:**
 - Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;
 - Awareness of potential engineering challenges caused by mandatory security controls;
 - Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques; and

SDLC – The Benefits to Integration (cont.)

- Facilitation of informed executive decision making through comprehensive risk management in a timely manner.
- Documentation of important security decisions made during development, ensuring management that security was fully considered during all phases;
- Improved organization and customer confidence to facilitate adoption and usage as well as governmental confidence to promote continued investment; and
- Improved systems interoperability and integration that would otherwise be hampered by securing systems at various system levels.

Pitfalls in the C&A Process

Pitfalls in the C&A Process

Common Pitfalls in the C&A Process

- **Poor understanding of security requirements**
- **Inaccurate documentation**
- **System misconfiguration (development artifacts)**
- **Poor implementation of Least Privilege**
- **Poor implementation of Role Separation**
- **!!! Poor configuration & patch management !!!**
- **LACK of involvement throughout the SDLC (on the part of the security element(s))**

From the “Front Lines”

- ✓ CTPs not executed prior to test date
- ✓ Any SOPs require use of 'root'
- ✓ SysAdmin can create and utilize a SecAdmin (or vice versa)
- ✓ Role separation properly configured, but there is one user with all roles
- ✓ MAC enforcement disabled but system still runs with full connectivity
- ✓ GAMES
- ✓ Default label encodings file in use
- ✓ Not using official classifications
- ✓ System Development is not complete
- ✓ Your password list is “securely” stored in a Windows network share on JWICS
- ✓ Documentation states you're running Solaris, but you're actually running Windows.
- ✓ Ostentatiously dropping the DCID in the trash in front of an evaluator
- ✓ “How did that get there?”
- ✓ Giving half the root password to the SysAdmin and the other half to the SecAdmin
- ✓ Development environment is the same one your wife and kids use to surf the Internet
- ✓ If you've got hacking tools on the system

Questions?

- ? Questions ? -

Contact Information

- **Timothy Watt**
 - Technical Director
 - Tenacity Solutions, Inc.
 - Email: tlwatt@tenacitysolutions.net
 - Cell: 571-235-3997
 - Website: <http://www.tenacitysolutions.net/>