ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

INFORMATION SECURITY WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE

Annabelle Lee and Tanya Brewer-Joneas
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Many System Development Life Cycle (SDLC) models exist that can be used by an organization to effectively develop an information system. A traditional SDLC is a linear sequential model. This model assumes that the system will be delivered near the end of its life cycle. Another SDLC model uses prototyping, which is often used to develop an understanding of system requirements without developing a final operational system. More complex models have been developed to address the evolving complexity of advanced and large information system designs. The SDLC model is embedded in any of the major system developmental approaches:

- Waterfall - the phases are executed sequentially.
- Spiral - the phases are executed sequentially with feedback loops to previous phases.
- Incremental development - several partial deliverables are constructed and each deliverable has incrementally more functionality. Builds are constructed in parallel, using available information from previous builds. The product is designed, implemented, integrated, and tested as a series of incremental builds.
- Evolutionary - there is re-planning at each phase in the life cycle based on feedback. Each phase is divided into multiple project cycles with deliverable measurable results at the completion of each cycle.

Security should be incorporated into all phases, from initiation to disposition, of an SDLC model. There are several NIST documents that are applicable to every phase of the SDLC, including Special Publications (SPs) 800-27 and 800-64 (see reference list at the end of this bulletin).

The following questions are some high-level starting points that should be addressed in determining the security controls/countermeasures that will be required for a system:

- How critical is the system in meeting the organization's mission?
- What are the security objectives required by the system, e.g., integrity, confidentiality, and availability?
- What regulations and policies are applicable in determining what is to be protected?
- What are the threats that are applicable in the environment where the system will be operational?
- Who selects the protection mechanisms that are to be implemented in the system?

A general SDLC includes five phases. Each of the five phases includes a minimum set of information security tasks needed to effectively incorporate security into a system during its development. The graphic on the following page illustrates the information security tasks applicable to each SDLC phase and the relevant references.

Listed below are the five phases with the information security tasks performed in each phase and the applicable references. At the end of the phase and task descriptions is a complete listing of all the references.

Phase 1: Initiation

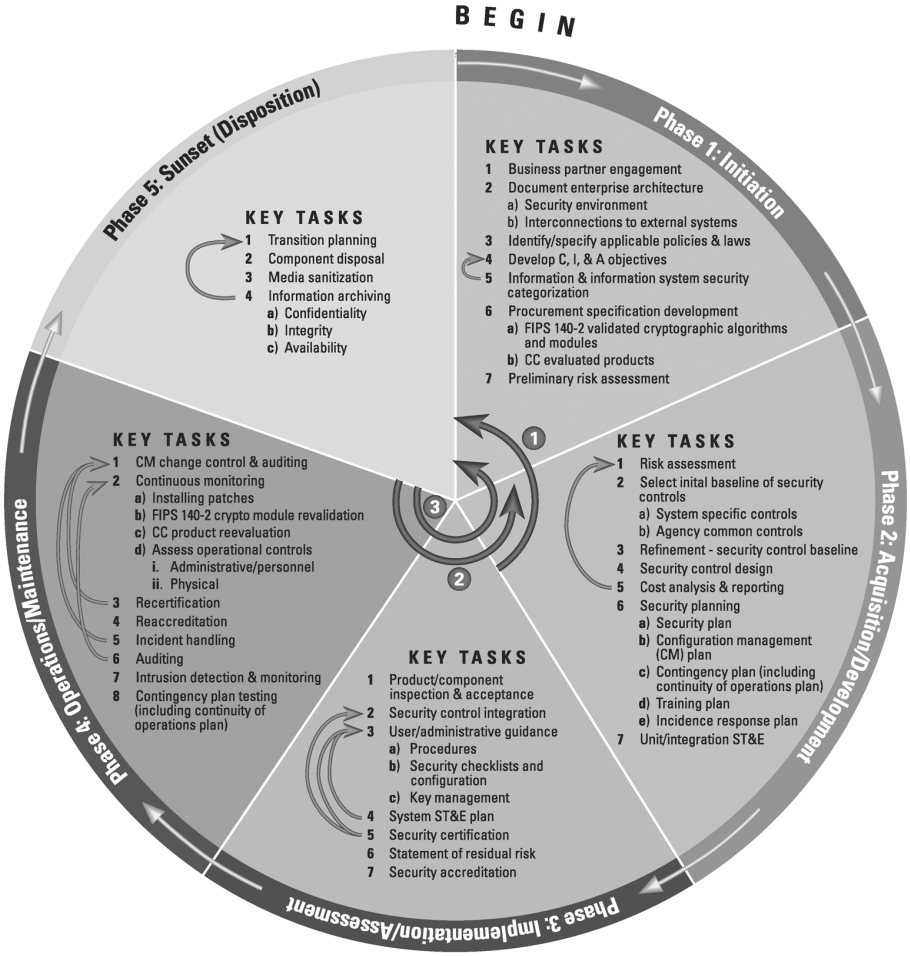
Key Tasks:

1. Business partner engagement (Key Documents: SP 800-35, 800-27; Additional References: Federal Information Processing Standard [FIPS] 191, SP 800-65, SP 800-47, SP 800-33)

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since July 2003



KEY NIST DOCUMENTS

PHASE 1 — 1. SP 800-35 IT Sec Svcs, SP 800-27 Engineering Principles; **2.** SP 800-47 Interconnecting; **3.** SP 800-14 Principles & Practices, SP 800-12 Comp Sec HB; **4. & 5.** FIPS 199 Sec Categorization, SP 800-60 Info. Mapping; **6.** SP 800-36 Selecting Info. Sec Products, SP 800-23 Acquisition of Evaluated Products; **7.** SP 800-30 Risk Management.

PHASE 2 — 1. SP 800-30; **2.** SP 800-53 Security Controls; **3.** SP 800-53; **4.** SP 800-36 Selecting Info. Sec Products, SP 800-23 Acquisition of Evaluated Products; **5.** SP 800-64 Security in SDLC, SP 800-36; **6.** SP 800-55 Security Metrics; **6e.** SP 800-61; **7.** CC, FIPS 140-2 Requirements for Crypto Modules.

PHASE 3 — 1. SP 800-64 Security in SDLC, SP 800-51 CVE; **2.** SP 800-64; 3. SP 800-61 Incident Handling, SP 800-36 Selecting Info. Sec Products, SP 800-35 IT Sec Svcs, SP 800-56 Key Establishment Schemes, SP 800-57 Key Management; **4.** SP 800-55 Security Metrics; **5.** SP 800-37 C&A, SP 800-53A Sec Ctrl Assess; **6.** SP 800-37; **7.** SP 800-37.

PHASE 4 — 1. HB 150 NVLAP Procedures/Requirements; **2.** SP 800-26 Sec Self-Assessment; **3.** SP 800-37 C&A, SP 800-53A Sec Ctrl Assess; **4.** SP 800-37; **5.** SP 800-61 Incident Handling; **6.** HB 150, SP 800-55 Security Metrics; **7.** SP 800-61, SP 800-31 Intrusion Detection; **8.** SP 800-34 Contingency Planning.

PHASE 5 — 1. SP 800-64 Security in SDLC; **2.** SP 800-35 IT Sec Svcs; **3.** SP 800-36 Selecting Info. Sec Products; **4.** SP 800-14 Principles & Practices, SP 800-12 Comp Sec HB.

LEGEND

Phase-to-Phase Iterations

1. Phase 2, Tasks 5 & 6 → Phase 1, Task 1
2. Phase 3, Task 2 → Phase 2, Task 4
3. Phase 4, Tasks 2 & 3 → Phase 1, Task 4

Feedback →

Acronyms

C&A	Certification & Accreditation
C, I, & A	Confidentiality, Integrity, & Availability
CC	Common Criteria
CM	Configuration Management
FIPS	Federal Information Processing Standard
HB	NIST Handbook
SDLC	System Development Life Cycle
SP	Special Publication
ST&E	Security Test & Evaluation

2. Document enterprise architecture (Key Document: SP 800-47; Additional References: SP 800-58, SP 800-48, SP 800-46, SP 800-45, SP 800-44, SP 800-43, SP 800-41, SP 800-40, SP 800-36, SP 800-33, SP 800-31, SP 800-28)
   a. Security environment
   b. Interconnections to external systems
3. Identification/specification of applicable policies and laws (Key Documents: SP 800-14, SP 800-12)
4. Development of Confidentiality, Integrity, and Availability objectives (Key Documents: FIPS 199, SP 800-60)
5. Information and information system security categorization (Key Documents: FIPS 199, SP 800-60; Additional Reference: SP 800-59)
6. Procurement specification development (Key Documents: SP 800-36, SP 800-23; Additional References: SP 800-66, SP 800-49, SP 800-47, SP 800-27)
   a. FIPS 140-2 validated cryptographic algorithms and modules (Additional References: FIPS 140-2; FIPS 46-3, FIPS 81, FIPS 180-2, FIPS 185, FIPS 186-2, FIPS 197, FIPS 198, SP 800-67, SP 800-38A, SP 800-38B, SP 800-38C, 800-22, SP 800-21, SP 800-20, SP 800-17)
   b. Common Criteria (CC) evaluated products (Additional Reference: CC)

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

7. Preliminary Risk Assessment (Key Document: SP 800-30)

Phase 2: Acquisition/ Development

Key Tasks:

1. Risk assessment (Key Document: SP 800-30; Additional References: SP 800-14, SP 800-12)
2. Selection of initial baseline of security controls (Key Document: SP 800-53)
   a. System specific controls
   b. Agency common controls
3. Refinement - security control baseline (Key Document: SP 800-53; Additional References: SP 800-36, SP 800-35, SP 800-31)
4. Security control design (Key Documents: SP 800-36, SP 800-23; Additional References: FIPS 181, FIPS 190, FIPS 196, SP 800-70, SP 800-66, SP 800-64, SP 800-58, SP 800-49, SP 800-48, SP 800-46, SP 800-45, SP 800-44, SP 800-43, SP 800-41, SP 800-35, SP 800-33, SP 800-31, SP 800-28)
5. Cost analysis and reporting (Key Documents: SP 800-64, SP 800-36; Additional References: SP 800-65, SP 800-35, SP 800-12)
6. Security planning (Key Document: SP 800-55; Additional References: SP 800-65, SP 800-26, SP 800-12)
   a. Security plan (Additional Reference: SP 800-18)
   b. Configuration management (CM) plan (Additional Reference: SP 800-64)
   c. Contingency plan (including continuity of operations plan) (Additional References: FIPS 87, SP 800-34, SP 800-12, SP 800-14)
   d. Training plan (Additional References: SP 800-50, 800-16, SP 800-14, SP 800-12)
   e. Incident response plan (Key Document: SP 800-61; Additional References: SP 800-40, SP 800-14, SP 800-12)
7. Unit/integration security test and evaluation (ST&E) (Key Documents: CC, FIPS 140-2; Additional Reference: SP 800-37)

Phase 3: Implementation/ Assessment

Key Tasks:

1. Product/component inspection and acceptance (Key Documents: SP 800-64, SP 800-51; Additional References: CC, FIPS 140-2)
2. Security control integration (Key Document: SP 800-64)
3. User/administrative guidance (Key Documents: SP 800-61; SP 800-36, SP 800-35; SP 800-56, SP 800-57)
   a. Procedures (Additional Reference: SP 800-14)
   b. Security checklists and configuration (Additional References: FIPS 181, FIPS 190, FIPS 196, SP 800-70, SP 800-68, SP 800-58, SP 800-49, SP 800-48, SP 800-47, SP 800-46, SP 800-45, SP 800-44, SP 800-43, SP 800-41, SP 800-40, SP 800-33, SP 800-31, SP 800-28)
   c. Key management
4. System ST&E plan (Key Document: SP 800-55; Additional References: SP 800-47, SP 800-46, SP 800-45, SP 800-44, SP 800-42, SP 800-41)
5. Security certification (Key Document: SP 800-37, SP 800-53A; Additional References: SP 800-42, SP 800-41, SP 800-26)
6. Statement of residual risk (Key Document: SP 800-37)
7. Security accreditation (Key Document: SP 800-37)

Phase 4: Operations/ Maintenance

Key Tasks:

1. CM change control and auditing (Key Document: Handbook [HB] 150; Additional References: HB 150-17, HB 150-20)
2. Continuous monitoring (Key Document: SP 800-26; Additional References: SP 800-51, SP 800-42, SP 800-41, SP 800-40, SP 800-36, SP 800-35, SP 800-28)
   a. Installation of patches (Additional References: SP 800-40)

b. FIPS 140-2 crypto module revalidation (Additional References: FIPS 140-2, FIPS 46-3, FIPS 81, FIPS 180-2, FIPS 185, FIPS 186-2, FIPS 197, FIPS 198, SP 800-67, SP 800-38A, SP 800-38B, SP 800-38C, SP 800-22, SP 800-21, SP 800-20, SP 800-17)

c. CC product reevaluation (Additional References: CC)

d. Assessment of operational controls

i. Administrative/personnel (Additional Reference: SP 800-35)

ii. Physical (Additional Reference: SP 800-35)

3. Recertification (Key Documents: SP 800-37, SP 800-53A; Additional References: SP 800-42, SP 800-41)
4. Reaccreditation (Key Document: SP 800-37)
5. Incident handling (Key Document: SP 800-61; Additional References: SP 800-40, SP 800-14, SP 800-12)
6. Auditing (Key Documents: HB 150, SP 800-55; Additional References: HB 150-17, HB 150-20)
7. Intrusion detection and monitoring (Key Documents: SP 800-61, SP 800-31)

ITL Bulletins Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

8. Contingency plan testing (including continuity of operations plan) (Key Document: SP 800-34; Additional References: FIPS 87, SP 800-14, SP 800-12)

Phase 5: Disposition (Sunset)

Key Tasks:

1. Transition planning (Key Document: SP 800-64; Additional References: SP 800-47, SP 800-46, SP 800-45, SP 800-44, SP 800-43, SP 800-41, SP 800-35, SP 800-27, SP 800-14, SP 800-12)
2. Component disposal (Key Document: SP 800-35; Additional Reference: SP 800-14)
3. Media sanitization (Key Document: SP 800-36)
4. Information archiving (Key Documents: SP 800-14, SP 800-12)

a. Confidentiality

b. Integrity

References:

Statutes and Regulations

Federal Information Security Management Act of 2002 (FISMA), H.R. 2458, Title III [Public Law 107-347], 107th U.S. Congress, December 17, 2002.

Cyber Security Research and Development Act, H.R. 3394 [Public Law 107-355], 107th U.S. Congress, November 27, 2002.

U. S. Office of Management and Budget, Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, February 1996.

Special Publications

(For current status of NIST publications (draft or final), go to http://csrc.nist.gov.)

SP 800-70, *The NIST Security Configuration Checklists Program*

SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: a NIST Security Configuration Checklist*

SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*

SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*

SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*

SP 800-64, *Security Considerations in the Information System Development Life Cycle*

SP 800-61, *Computer Security Incident Handling Guide*

SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*

SP 800-59, *Guideline for Identifying an Information System as a National Security System*

SP 800-58, *Security Considerations for Voice Over IP Systems*

SP 800-57, *Recommendation on Key Management*

SP 800-56, *Recommendation on Key Establishment*

SP 800-55, *Security Metrics Guide for Information Technology Systems*

SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*

SP 800-53, *Recommended Security Controls for Federal Information Systems*

SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*

SP 800-50, *Building an Information Technology Security Awareness and Training Program*

SP 800-49, *Federal S/MIME V3 Client Profile*

SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*

SP 800-47, *Security Guide for Interconnecting Information Technology Systems*

SP 800-46, *Security for Telecommuting and Broadband Communications*

SP 800-45, *Guidelines on Electronic Mail Security*

SP 800-44, *Guidelines on Securing Public Web Servers*

SP 800-43, *Systems Administration Guidance for Windows 2000 Professional*

SP 800-42, *Guideline on Network Security Testing*

SP 800-41, *Guidelines on Firewalls and Firewall Policy*

SP 800-40, *Procedures for Handling Security Patches*

SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*

SP 800-38B, *Recommendation for Block Cipher Modes of Operation: the CMAC Authentication Mode*

SP 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*

SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*

SP 800-36, *Guide to Selecting Information Security Products*

SP 800-35, *Guide to Information Technology Security Services*

SP 800-34, *Contingency Planning Guide for Information Technology Systems*

SP 800-33, *Underlying Technical Models for Information Technology Security*

SP 800-31, *Intrusion Detection Systems (IDS)*

SP 800-30, *Risk Management Guide for Information Technology Systems*

SP 800-28, *Guidelines on Active Content and Mobile Code*

SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*

SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*

SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*

SP 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*

SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*

SP 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*

SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*

SP 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*

SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*

SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*

SP 800-12, *An Introduction to Computer Security: The NIST Handbook*

FIPS

FIPS 46-3, *Data Encryption Standard (DES)*

FIPS 81, *DES Modes of Operation*

FIPS 87, *Guidelines for ADP Contingency Planning*

FIPS 140-2, *Security requirements for Cryptographic Modules*

FIPS 180-2, *Secure Hash Standard (SHS)*

FIPS 181, *Automated Password Generator*

FIPS 185, *Escrowed Encryption Standard*

FIPS 186-2, *Digital Signature Standard (DSS)*

FIPS 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*

FIPS 191, *Guideline for The Analysis of Local Area Network Security*

FIPS 196, *Entity Authentication Using Public Key Cryptography*

FIPS 197, *Advanced Encryption Standard*

FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*

Handbooks

NIST Handbook 150: 2001, *NVLAP Procedures and General Requirements*

NIST Handbook 150-17, *NVLAP Cryptographic Module Testing*

NIST Handbook 150-20, *NVLAP Information Technology Security Testing - Common Criteria*

Miscellaneous

CC, *Common Criteria for Information Technology Security Evaluation, Version 2.2*

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900