Reference Document List

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 800-57	Recommendation on Key Management
SP 800-56	Recommendation on Key Establishment Schemes
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	Security Controls for Federal Information Systems
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-31	Intrusion Detection Systems (IDS)
SP 800-30	Risk Management Guide for Information Technology Systems
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 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 140-2	Security Requirements for Cryptographic Modules

NIST Handbook 150: 2001, NVLAP Procedures and General Requirements

Common Criteria for Information Technology Security Evaluation, Version 2.2

All References Available at http://csrc.nist.gov

Many System Development Life Cycle (SDLC) models exist that can be used by an organization in developing 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. More complex models have been developed to address the evolving complexity of advanced and large information system designs.

A general SDLC includes the following phases: *initiation, acquisition/development, implementation/assessment, operations/maintenance, and sunset (disposition).* Each of these five phases includes a minimum set of tasks to incorporate security in the system development process. Including security early in the information SDLC will usually result in less expensive and more effective security than adding it to an operational system.

The following questions should be addressed in determining the security controls 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?

For more information:

http://csrc.nist.gov/SDLCinfosec

SDLCinfosec@nist.gov

NIST

National Institute of Standards and Technology

Technology Administration, U.S. Department of Commerce

Computer Security Division

Information Technology Laboratory

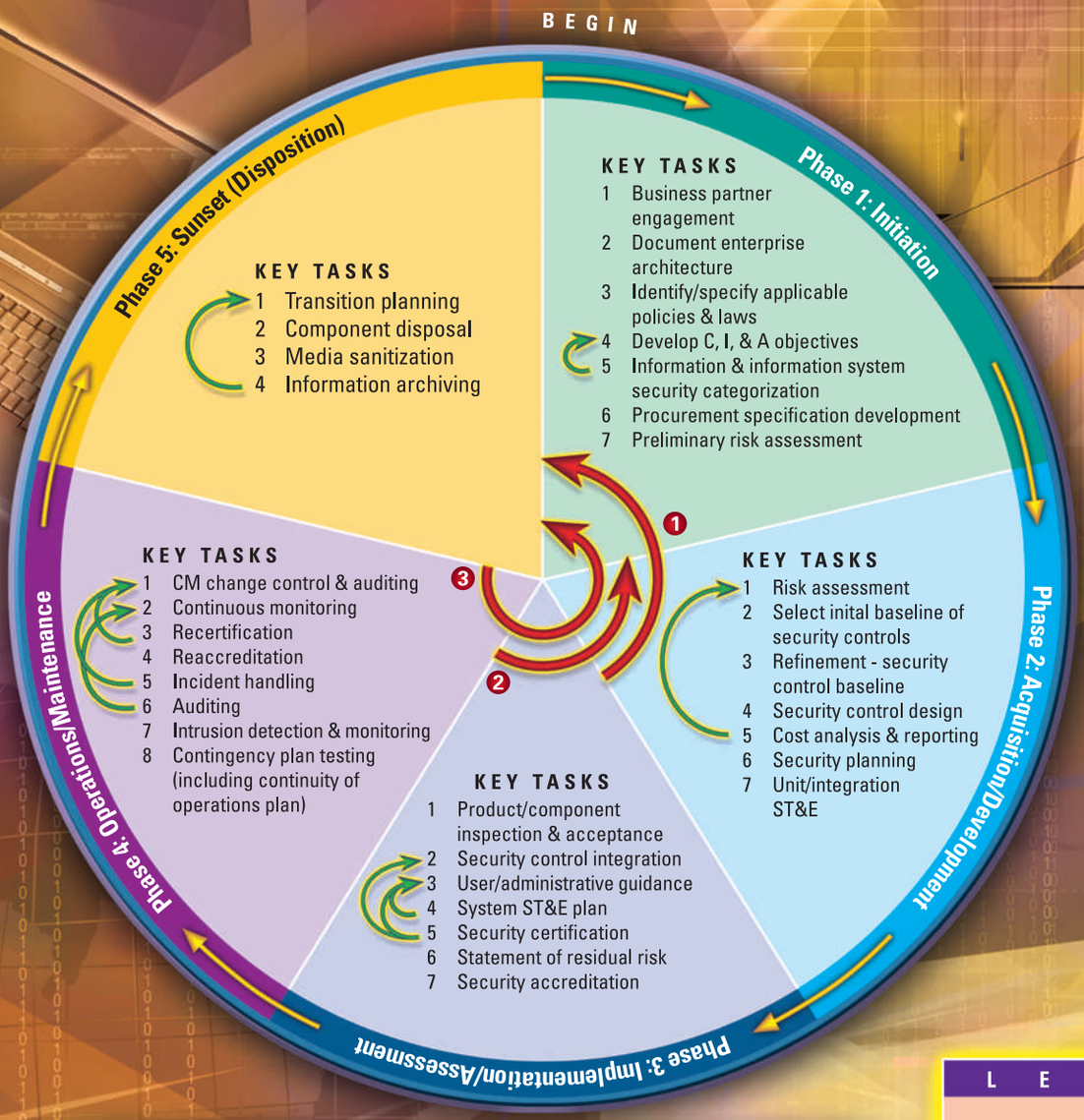
Information Security

System Development Life Cycle

NIST

Computer Security Division

INFORMATION SECURITY IN THE SDLC



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; 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

NIST
Computer Security Division