

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 Technologies
	Security Management 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 Vulnerability Assessments and Exposures (CVE) Vulnerability Assessments
SP 800-47	Security Controls for Information Technology Systems
SP 800-37	Guide for Managing Information Security Risk of Federal Information Systems
SP 800-36	Guide for Security Controls for Information Technology Systems
SP 800-35	Guide for Security Controls for Information Technology Systems
SP 800-34	Continuity of Operations for Information Technology Systems
SP 800-31	Intrusion Detection and Prevention for Information Technology Systems
SP 800-80	Risk Management for Information Technology Systems
SP 800-27	Engineering Security Controls for Information Technology Systems
SP 800-26	Security Controls for Information Technology Systems
SP 800-23	Guidelines for Assurance of Information Technology Products
SP 800-14	General Security Controls for Information Technology Systems
SP 800-12	An Introduction to the NIST Framework for Improving Critical Infrastructure Cybersecurity
FIPS 199	Standard for Information Security
FIPS 140-2	Security Requirements for Cryptographic Modules
NIST Handbook 150: 2003	Common Criteria for Information Technology Security Evaluation
All References Available	

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:

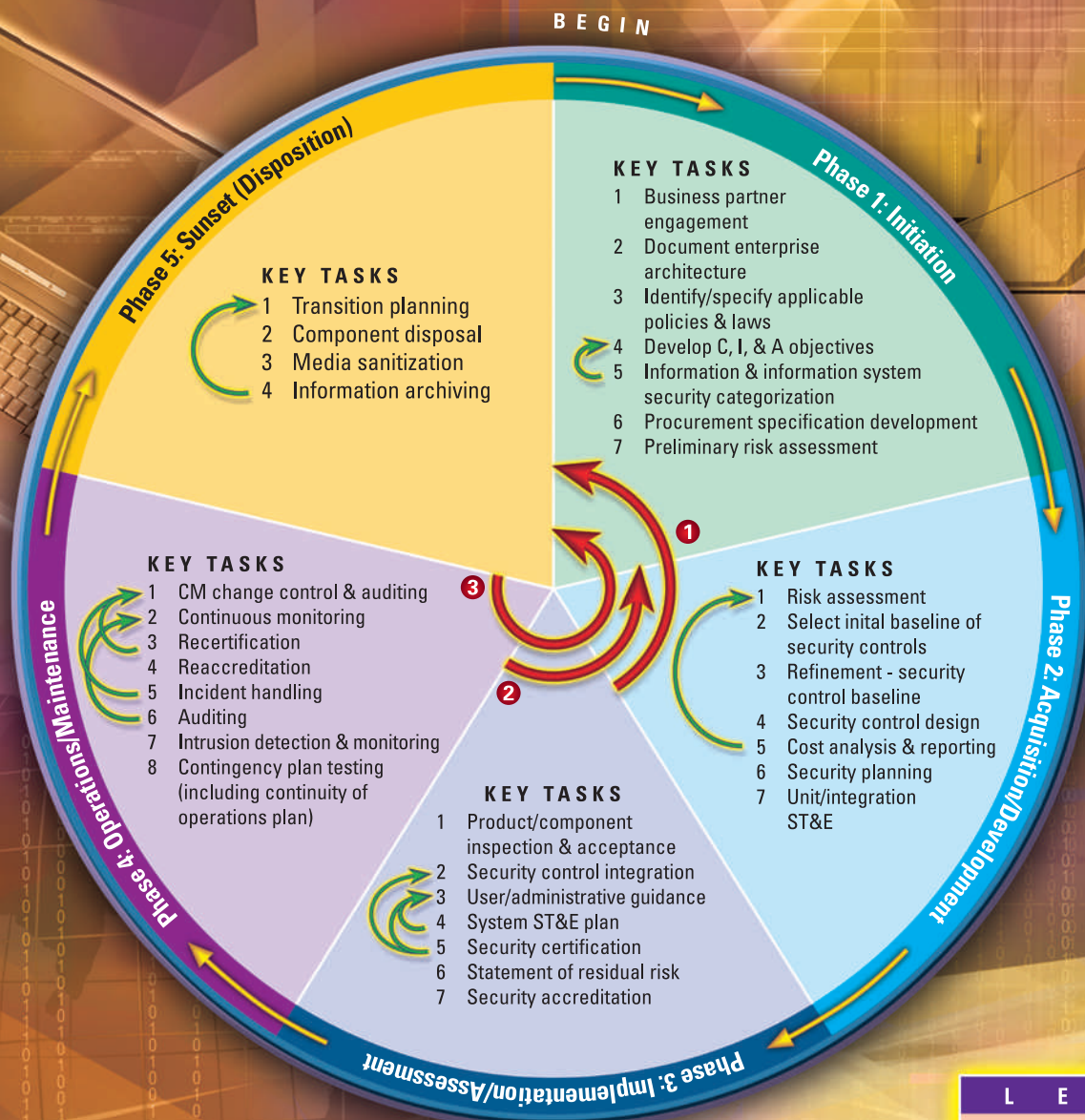
**<http://csrc.nist.gov/SDLCinfosec>
SDLCinfosec@nist.gov**

Information Security

System Development Life Cycle

NIST

Computer Security Division



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