THE SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The most effective way to protect information and information systems is to integrate security into every step of the system development process, from the initiation of a project to develop a system to its disposition. The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system, is called the System Development Life Cycle (SDLC).

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently updated its general guide that helps organizations plan for and implement security throughout the SDLC. The revised guide provides basic information about the comprehensive approach that NIST has developed for managing risks to systems and for providing the appropriate levels of information security based on the levels of risk. Federal agencies are directed to incorporate security controls and services into the SDLC under the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) Circular A-130, Appendix III.

NIST Special Publication (SP) 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*

Revision 2 of NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, was developed by Richard Kissel, Kevin Stine, and Matthew Scholl of NIST, with the expert assistance of Hart Rossman, Jim Fahlsing, and Jessica Gulick, of Science Applications International Corporation (SAIC). In addition, many individuals in the public and private sectors contributed to the revision by reviewing it and providing constructive comments.

The guide focuses on the information security components of the SDLC. One section summarizes the relationships between the SDLC and other information technology (IT) disciplines. Topics discussed include the steps that are prescribed in the SDLC approach, and the key security roles and responsibilities of staff members who carry out information system development projects.

NIST SP 800-64 helps organizations integrate specific security steps into a linear and sequential SDLC process. The five-phase method of development that is described in the guide is also known as the waterfall method, and is one process for system development. Other methodologies can be used as well. Detailed charts and tables in the guide present specific activities for each step of the SDLC, and the security activities associated with each step.

Another section of NIST SP 800-64 provides insight into IT projects and initiatives that are not as clearly defined as SDLC-based developments. Projects such as service-oriented architectures, cross-organization projects, and IT facility developments often require a somewhat different approach to security integration than the traditional system development efforts.

The guide includes detailed supplemental information in seven appendices. Appendix A provides a glossary of terms used in the guide. Appendix B presents a comprehensive list of acronyms. Appendix C lists references cited in the publication. Appendix D matches the security-related steps in each phase of the SDLC to the relevant NIST publications that provide guidance for the security activities. Appendix E gives an overview of other SDLC methodologies. Appendix F discusses additional planning considerations for the development and acquisition phase of the SDLC. Appendix G provides a view of the security considerations in the SDLC in a graph format.

The System Development Life Cycle

The system development life cycle is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. There are many different SDLC models and methodologies, but each generally consists of a series of defined steps or phases. For any SDLC model that is used, information security must be integrated into the SDLC to ensure appropriate protection for the information that the system will transmit, process, and store.

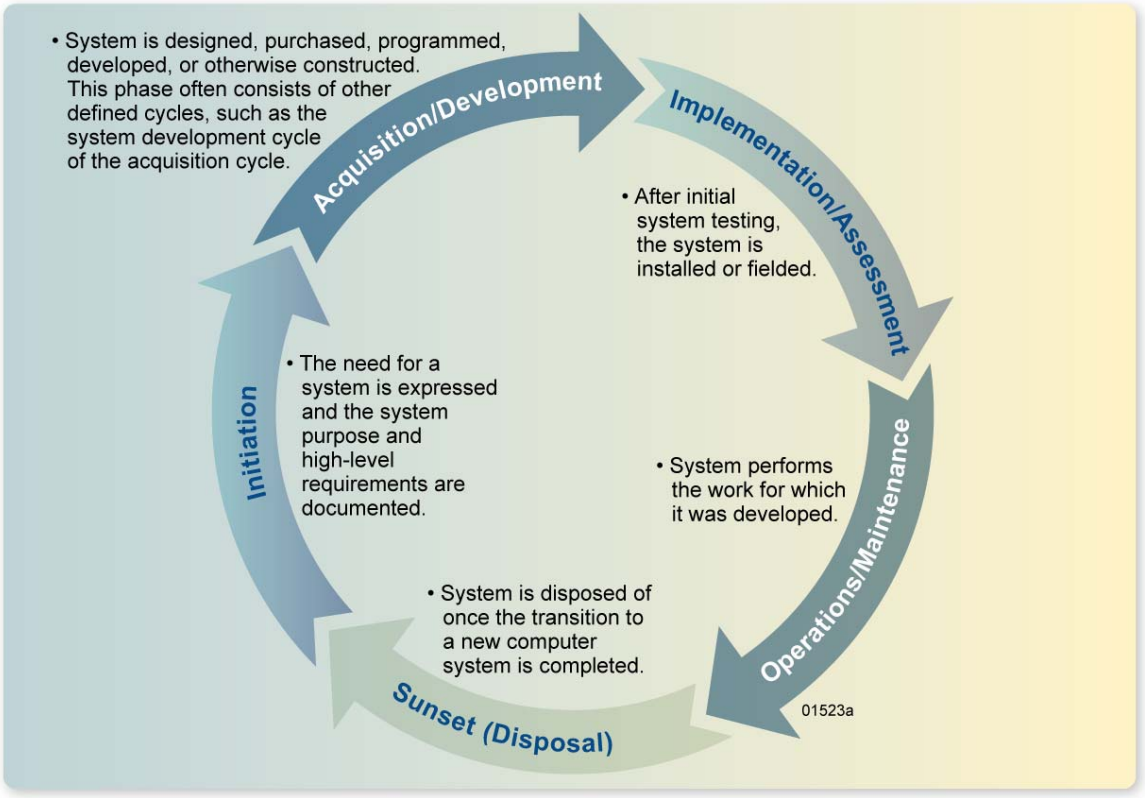
Applying the risk management process to system development enables organizations to balance requirements for the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the SDLC. Risk management processes identify critical assets and operations, as well as systemic vulnerabilities across the organization. Risks are often shared throughout the organization and are not specific to certain system architectures.

Some of the benefits of integrating security into the system development life cycle include:

- Early identification and mitigation of security vulnerabilities and problems with the configuration of systems, resulting in lower costs to implement security controls and mitigation of vulnerabilities;
- Awareness of potential engineering challenges caused by mandatory security controls;
- Identification of shared security services and reuse of security strategies and tools that will reduce development costs and improve the system’s security posture through the application of proven methods and techniques;
- Facilitation of informed executive decision making through the application of a comprehensive risk management process in a timely manner;

- Documentation of important security decisions made during the development process to inform management about security considerations during all phases of development;
- Improved organization and customer confidence to facilitate adoption and use of systems, and improved confidence in the continued investment in government systems; and
- Improved systems interoperability and integration that would be difficult to achieve if security is considered separately at various system levels.

The System Development Life Cycle



Initiation Phase. During the initiation phase, the organization establishes the need for a system and documents its purpose. Security planning should begin in the initiation phase with the identification of key security roles to be carried out in the development of the system. The information to be processed, transmitted, or stored is evaluated for security requirements, and all stakeholders should have a common understanding of the security considerations. The Information System Security Officer (ISSO) should be identified as well.

Security considerations are key to the early integration of security, and to the assurance that threats, requirements, and potential constraints in functionality and integration are

considered. Requirements for the confidentiality, integrity, and availability of information should be assessed at this stage. Federal agencies should apply the provisions of Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.* These standards require agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability and to select appropriate security controls. Any information privacy requirements should be determined as well.

Early planning and awareness will result in savings in costs and staff time through proper risk management planning. In this phase, the organization clearly defines its project goals and high-level information security requirements, as well as the enterprise security system architecture.

Development/Acquisition Phase. During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. A key security activity in this phase is conducting a risk assessment and using the results to supplement the baseline security controls. In addition, the organization should analyze security requirements; perform functional and security testing; prepare initial documents for system certification and accreditation; and design the security architecture.

The risk assessment enables the organization to determine the risk to operations, assets, and individuals resulting from the operation of information systems, and the processing, storage, or transmission of information. After categorizing their systems in accordance with FIPS 199 and 200, federal agencies should meet the minimum security requirements by selecting the appropriate security controls and assurance requirements that are described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

Another essential element is the development of security plans, which establish the security requirements for the information system, describe security controls that have been selected, and present the rationale for security categorization, how controls are implemented, and how use of systems can be restricted in high-risk situations. Security plans document the decisions made in the selection of controls, and are approved by authorized officials.

The developmental testing of the technical and security features and functions of the system ensure that they perform as intended, prior to launching the implementation and integration phase.

Implementation Phase. In the implementation phase, the organization configures and enables system security features, tests the functionality of these features, installs or implements the system, and obtains a formal authorization to operate the system. Design reviews and system tests should be performed before placing the system into operation to ensure that it meets all required security specifications. In addition, if new controls are

added to the application or the support system, additional acceptance tests of those new controls must be performed. This approach ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the organization's official records.
.

Operations/Maintenance Phase. In this phase, systems and products are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and software components are added or replaced. The organization should continuously monitor performance of the system to ensure that it is consistent with pre-established user and security requirements, and that needed system modifications are incorporated.

Configuration management (CM) and control activities should be conducted to document any proposed or actual changes in the security plan of the system. Information systems are in a constant state of evolution with upgrades to hardware, software, firmware, and possible modifications in the surrounding environment. Documenting information system changes and assessing the potential impact of these changes on the security of a system are essential activities to assure continuous monitoring, and prevent lapses in the system security accreditation.

Disposal Phase. In this phase, plans are developed for discarding system information, hardware, and software and making the transition to a new system. The information, hardware, and software may be moved to another system, archived, discarded, or destroyed. If performed improperly, the disposal phase can result in the unauthorized disclosure of sensitive data. When archiving information, organizations should consider the need for and the methods for future retrieval.

Usually, there is no definitive end to a system. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information for the original system should still be relevant and useful when the organization develops the security plan for the follow-on system.

The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access. The removal of information from a storage medium, such as a hard disk or tape, should be done in accordance with the organization's security requirements.

Additional Security Considerations

Some IT development projects are service-based and may involve other organizations, such as public-private sector supply chain endeavors. Other projects are facility-oriented, such as the establishment of a data center or a hot site. Organizations developing projects such as these should follow the principles for integrating security into the SDLC, as they examine and address the additional security considerations involved in these projects. See NIST SP 800-64 for more details.

More Information

NIST SP 800-64 is a reference document that should be used in conjunction with other NIST publications throughout the development of the system.

Publications developed by NIST help information management and information security personnel in planning and implementing a comprehensive approach to information security. The general security of information systems depends upon attention to basic issues such as security planning, certification and accreditation, risk management, categorization of systems, and use of security controls. Organizations can draw upon NIST standards and guidelines to carry out their SDLC activities, including the following:

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules.*

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

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Information Technology Systems*.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems.* NIST SP 800-64 complements the Risk Management Framework discussed in NIST SP 800-30 by providing a sample roadmap for integrating security functionality and assurance into the SDLC. NIST SP 800-64 also provides further detail on additional activities that are valuable for consideration in different system and agency settings.

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

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.* This publication is being revised.

NIST SP 800-39, Draft *Managing Risk from Information Systems: An Organizational Perspective*. This publication is being revised.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. This publication is being revised. Security architectures should implement the security control families that are outlined in NIST SP 800-53 and that protect the confidentiality, integrity, and availability of federal information and information systems.

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

NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories.*

NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*. The CPIC process is defined by OMB Circular A-130 as "a management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes." This publication described a seven-step methodology to help organizations integrate security into the CPIC process and to assure that capital planning and information security goals and objectives are met.

NIST SP 800-88, *Guidelines for Media Sanitization.*

NIST SP 800-95, *Guide to Secure Web Services.*

NIST Interagency Report (NISTIR) 7298, *Glossary of Key Information Security Terms.*

For information about NIST standards and guidelines that are listed above, as well as other security-related publications, see NIST's Web page:
http://csrc.nist.gov/publications/index.html

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.