Software Development Lifecycle Policy

Sample Organization

Criteria satisfaction

Standard	Criteria Satisfied
TSC 2017	CC8.1

Document history

Date	Comment
Jun 1 2018	Initial document

Contents

1 Purpose and Scope

a. The purpose of this policy is to define requirements for establishing and maintaining baseline protection standards for company software, network devices, servers, and desktops.

b. This policy applies to all users performing software development, system administration, and management of these activities within the organization. This typically includes employees and contractors, as well as any relevant external parties involved in these activities (hereinafter referred to as "users"). This policy must be made readily available to all users.

c. This policy also applies to enterprise-wide systems and applications developed by the organization or on behalf of the organization for production implementation.

2 Background

a. The intent of this policy is to ensure a well-defined, secure and consistent process for managing the entire lifecycle of software and information systems, from initial requirements analysis until system decommission. The policy defines the procedure, roles, and responsibilities, for each stage of the software development lifecycle.

b. Within this policy, the software development lifecycle consists of requirements analysis, architecture and design, development, testing, deployment/implementation, operations/maintenance, and decommission. These processes may be followed in any form; in a waterfall model, it may be appropriate to follow the process linearly, while in an agile development model, the process can be repeated in an iterative fashion.

3 References

a. Risk Assessment Policy

4 Policy

a. The organization's Software Development Life Cycle (SDLC) includes the following phases:

   i. Requirements Analysis

   ii. Architecture and Design

   iii. Testing

   iv. Deployment/Implementation

   v. Operations/Maintenance

   vi. Decommission

b. During all phases of the SDLC where a system is not in production, the system must not have live data sets that contain information identifying actual people or corporate entities, actual financial data such as account numbers, security codes, routing information, or any other financially identifying data. Information that would be considered sensitive must never be used outside of production environments.

c. The following activities must be completed and/or considered during the requirements analysis phase:

   i. Analyze business requirements.

   ii. Perform a risk assessment. More information on risk assessments is discussed in the Risk Assessment Policy (reference (a)).

iii. Discuss aspects of security (e.g., confidentiality, integrity, availability) and how they might apply to this requirement.

iv. Review regulatory requirements and the organization's policies, standards, procedures and guidelines.

v. Review future business goals.

vi. Review current business and information technology operations.

vii. Incorporate program management items, including:

1. Analysis of current system users/customers.
2. Understand customer-partner interface requirements (e.g., business-level, network).
3. Discuss project timeframe.

viii. Develop and prioritize security solution requirements.

ix. Assess cost and budget constraints for security solutions, including development and operations.

x. Approve security requirements and budget.

xi. Make "buy vs. build" decisions for security services based on the information above.

d. The following must be completed/considered during the architecture and design phase:

i. Educate development teams on how to create a secure system.

ii. Develop and/or refine infrastructure security architecture.

iii. List technical and non-technical security controls.

iv. Perform architecture walkthrough.

v. Create a system-level security design.

vi. Create high-level non-technical and integrated technical security designs.

vii. Perform a cost/benefit analysis for design components.

viii. Document the detailed technical security design.

ix. Perform a design review, which must include, at a minimum, technical reviews of application and infrastructure, as well as a review of high-level processes.

x. Describe detailed security processes and procedures, including: segregation of duties and segregation of development, testing and production environments.

xi. Design initial end-user training and awareness programs.

xii. Design a general security test plan.

xiii. Update the organization's policies, standards, and procedures, if appropriate.

xiv. Assess and document how to mitigate residual application and infrastructure vulnerabilities.

xv. Design and establish separate development and test environments.

e. The following must be completed and/or considered during the development phase:

i. Set up a secure development environment (e.g., servers, storage).

ii. Train infrastructure teams on installation and configuration of applicable software, if required.

iii. Develop code for application-level security components.

iv. Install, configure and integrate the test infrastructure.

v. Set up security-related vulnerability tracking processes.

vi. Develop a detailed security test plan for current and future versions (i.e., regression testing).

vii. Conduct unit testing and integration testing.

f. The following must be completed and/or considered during the testing phase:

i. Perform a code and configuration review through both static and dynamic analysis of code to identify vulnerabilities.

ii. Test configuration procedures.

iii. Perform system tests.

iv. Conduct performance and load tests with security controls enabled.

v. Perform usability testing of application security controls.

vi. Conduct independent vulnerability assessments of the system, including the infrastructure and application.

g. The following must be completed and/or considered during the deployment phase:

i. Conduct pilot deployment of the infrastructure, application and other relevant components.

ii. Conduct transition between pilot and full-scale deployment.

iii. Perform integrity checking on system files to ensure authenticity.

iv. Deploy training and awareness programs to train administrative personnel and users in the system's security functions.

v. Require participation of at least two developers in order to conduct full-scale deployment to the production environment.

h. The following must be completed and/or considered during the operations/maintenance phase:

i. Several security tasks and activities must be routinely performed to operate and administer the system, including but not limited to:

1. Administering users and access.

2. Tuning performance.

3. Performing backups according to requirements defined in the System Availability Policy

4. Performing system maintenance (i.e., testing and applying security updates and patches).

5. Conducting training and awareness.

6. Conducting periodic system vulnerability assessments.

7. Conducting annual risk assessments.

ii. Operational systems must:

1. Be reviewed to ensure that the security controls, both automated and manual, are functioning correctly and effectively.

2. Have logs that are periodically reviewed to evaluate the security of the system and validate audit controls.

3. Implement ongoing monitoring of systems and users to ensure detection of security violations and unauthorized changes.

4. Validate the effectiveness of the implemented security controls through security training as required by the Procedure For Executing Incident Response.
5. Have a software application and/or hardware patching process that is performed regularly in order to eliminate software bug and security problems being introduced into the organization's technology environment. Patches and updates must be applied within ninety (90) days of release to provide for adequate testing and propagation of software updates. Emergency, critical, break-fix, and zero-day vulnerability patch releases must be applied as quickly as possible.

i. The following must be completed and/or considered during the decommission phase:
   i. Conduct unit testing and integration testing on the system after component removal.
   ii. Conduct operational transition for component removal/replacement.
   iii. Determine data retention requirements for application software and systems data.
   iv. Document the detailed technical security design.
   v. Update the organization's policies, standards and procedures, if appropriate.
   vi. Assess and document how to mitigate residual application and infrastructure vulnerabilities.