INCORPORATING SECURITY INTO THE SOFTWARE DEVELOPMENT LIFECYCLE

Augusta D. Hayward and Young B. Choi

Department of Business, Leadership, and Information Systems

College of Arts & Sciences

Regent University

1000 Regent University Drive

Virginia Beach, VA 23464

USA

e-mail: auguhay@mail.regent.edu, ychoi@regent.edu

Tel: (757) 352-4949

Abstract

To gain the most benefits of information security it cannot be an afterthought. Early integration during system design will enable early detection of system vulnerabilities. Organizations, agencies and businesses can maximize the return of their investments in security programs through implementing risk assessments that will indentify system vulnerabilities, and erroneous system configurations resulting in a reduction in costs due to early detection.

Software Development Lifecycle Process

Incorporating security early will also provide an awareness of potential engineering challenges caused by the expansion of mandatory controls driven by Federal and State mandates. Most importantly, security risk management will aid the decision making processes of executive management who are charged with protecting the organization's logical and physical assets. Risk Management is a core component of Information System Security architecture. NIST states, "Information system security processes enabling information system security processes and activities provide valuable input into managing IT systems and their development, risk identification, planning and mitigation." NIST Special Publication 800-62. 2008).

A definition of Software Development Lifecycle (SDLC) is, "The overall process of developing informant systems through a multi- progression process from requirements analysis through design, development, testing, maintenance and ultimately retirement."(NIST 2008 p.4).

Adhering to an SDLC model increases the likelihood of project success, particularly in the area of fulfilling stakeholder requirements," (Onpoint, n.d, p. 2). There are several different types of SDLC's; for example: Waterfall is one of the most widely used methodologies and is the method from which all others proceed. There is also Fountain, Spiral, Build and Fix, Rapid Prototyping, Incremental and Synchronize and Stabilize. According to Onpoint (n.d.), "The Waterfall has several advantages; it is one of the most widely used and accepted methodologies; nearly all other methodologies derive from the Waterfall; and its linear approach makes it easy to demonstrate where security fits into each phase." The Waterfall methodology is implemented in five stages: Initiation, Development/Acquisition, Implementation/Assessment, Operation/Maintenance and Disposal. The Initiation phase is primarily the phase in which the initial requirements are defined for the system.

This is the phase where a decision has been made that there is a need for the system. Onpointstates, "At the end of this phase, all of the requirements necessary to design or purchase the system should be identified and thoroughly understood. During this phase it is important to also identify security requirements." Identifying risks are important in all phases because they are shared by all. According to NIST, "A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle." (2008, p. 4).

Each phase contains specific security activities that can be incorporated into the Waterfall methodology and these activities are not designed to expand the methodology but to enhance it by incorporating security processes early on in the design of the system. There are three advantages to incorporating security activities into the SDLC; one, the system will benefit from having stronger security architecture which reduce the likelihood and/or lessen the impact of exploited vulnerabilities. Second, integrating security concepts during the system design will be less daunting than implementing security in a system already in production and can be a more costly effort. Integrating security at the design level will help to reduce costs.

Thirdly, integrating security, especially in federal information systems, it is required by the Certification and Accreditation (C&A). Onpoint states, "The SDLC is a process to help ensure the successful development, operation, and retirement of information systems" The security officer of the organization should work closely with the developers and system designers ensuring that the appropriate security requirements have been integrated into the Security architecture and framework of the system and this integration should cover all phases of the SDLC. Although there are several SDLC's to choose from, Waterfall is a process that has been around for a while and is implemented in phases, so each phase will have specific security control activities that will overlay each phase making it a more seamless effort.

The Risk Management Process, a Security Lifecycle Approach.

As previously discussed, implementing security at the system level and is cost effective, implementing a Risk Management Framework ((RMF) is a logical beginning to any software development project. This process generally begins with risk related tasks that are carried out by information security personnel in different roles; such as, a chief information officer, senior information officer, or enterprise architect. These roles can be closely aligned with similar roles in software development. The alignment of these roles will ensure that the security related tasks will be executed concurrently with or as part of the SDLC. One approach to overlaying Risk Management activities is to align the RMF tasks with the primary group who will be responsible for its completion.

NIST also states, "Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes."(NIST Special Publication 800-64, 2010). Risk management tasks are to begin early enough in the SDLC because they will provide the security building blocks upon which the system will rely upon.

Risk decisions made at the executive and organizational level will be addressed at the information system level in the form of security controls, or countermeasures and needed safeguards. During the initiation phase of the project, the system requirements are established by the organization and these are typically mapped to the Security Controls so that they are addressed during the design, development and during the implementation of the system.

Coordinating Security Requirements in the SDLC Initiation Phase

The Initiation phase is the beginning of the development phase. Security considerations are identified here. According to NIST, "During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. At this point, security is looked at more in terms of business risks with input from the information security office, "(2008, p. 13). Important security activities here will define the terms of the confidentiality, integrity and availability as identified in the business requirements.

The information that the system will be expected to process will need to be categorized with any known specific requirements in transmission, storing or personally identifiable information and most importantly, identifying any privacy requirements. Security cannot be defined in a box; it must be a collaborated effort amongst all key project and security personnel to ensure that there are solid understandings about the business decisions that are taking place and their implications for each department and the overall impact to the project.

Basically the Initiation phase will take into account laws; directives, policy guidance, strategic goals and objectives, priorities and resource availability even supply chain considerations. Nist says, "Finally, organizations maximize the use of security-relevant information (e.g., assessment results, information system documentation, and other artifacts) generated during the system development life cycle to satisfy requirements for similar information needed for information security-related purposes. Similar security-relevantinformation concerning common controls, including security controls provided by external providers, is factored into the organization's risk management process, "NIST 2010, p. 7).

Selecting Security Controls in the SDLC Initiation Phase.

Another important step for the organization is to select and document the security controls. This is generally carried out by the Chief Information Officer and other security personnel. NIST states that, "There are three types of security controls for information systems that can be employed by an organization: (I) *system-specific controls* (i.e., controls that provide a security capability for a particular information system only); (ii) *common controls* (i.e., controls that provide a security capability for multiple information systems); or (iii) *hybrid controls* (i.e., controls that have both system-specific and common characteristics,"(NIST Special Publication 800-37, 2010).

The organization will allocate controls based on the information security architecture within the organization. The organization will implement controls that will support multiple information systems efficiently as a common base amongst all system (i.e., common controls). The common controls will simply the implementation of risk activities across the organization and will promote cost savings because they will be used to support specific information system needs thereby making them "inherited" controls. It is good to note, "When the common controls provided by the organization are not sufficient for information systems inheriting the controls, the system owners supplement the common controls with system-specific or hybrid controls to achieve the required protection for the system and/or accept greater risk,"(NIST 2010 p. 24).

Implementing Security in SDLC Development

It is in this phase that the system is designed, purchased, programmed, and constructed. There are key security activities for this phase such as conducting the risk and using the results to support baseline controls. The security requirements must also be analyzed for functional and security testing. After all development and testing is completed, documents for certification and accreditation are prepared.

To ensure that system development is successful, NIST states, "System development should occur with standard processes that consider secure practices and are documented and repeatable. To accomplish this, appropriate security processes for the assurance level required by the system should be determined and documented. Thus, systems with a high assurance requirement may need additional security controls built into the development process," NIST, 2008, p. 21). There are also quality gates that will be positioned to determine the readiness of system development. The Architecture/Design review will evaluate the system design to determine its ability to be integrated with other systems and to incorporate shared services, common security controls, for example; authentication, disaster recovery, intrusion detection, or incident reporting.

To ensure that the system is capable of delivering according to the expectation of the owner, a system performance review will performed to validate if the

system behaves in a predictable manner when it is used in a proper and improper manner.A functional system review will verify that the functional requirements identified are sufficiently documented in detail and are testable. If the requirements are not testable, then functional testing results will be skewed. If the security controls or requirements change, then a follow up risk review may also be necessary.

Implementation/Assessment Phase

This is the third phase of the SDLC and the system will be installed and evaluated in the production environment.According to Radack, "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."(Radack, n.d.)

There are security activities that are relevant to this phase as well. For example, using the best practices chosen for the development technologies and these should included by default. The Security plan should also be finalized and this would be in accordance to NIST SP 800-18. Onpoint states, "If the system was properly documented during the previous SDLC phases, the finalization of the SSP will be a small task. If major changes are required, it probably means that the design plans could not be followed," (Onpoint, n.d.).

As design moves closer to completion, the Security plan should reflect its production state. All the security controls listed in the previous phase should also be tested. NIST SP 800-53 A suggests the development of a Security Control Testing Plan (SSP). "The Test plan that is created should reflect the information that has been provided in the SSP. Test Plans should not include the testing of controls that are not applicable, deemed unnecessary, or already known to be ineffective,"(Onpoint, n.d.pg 5). Before releasing the system, it must be determined that all the security controls documented in the SSP are implemented and working accordingly. A security control assessmentwillbe the best way to make that determination and all testing results should be documented accordingly including all the test cases that did not pass. Once all the deficiencies have been identified through analysis and documentation, including the tests that failed, a contingency plan or a plan of action should detail how all deficiencies will be fixed and what resources will be required for the effort. The final step will be to authorize the system for release. This is the last phase of the SDLC.

The authorizing official will present a package that contains all system artifacts such as assessments, documentation and the plan of action. According to Onpoint, "If the residual risks are acceptable, the system will be authorized to enter production. To expedite system deployment, it is important to have completed all of the previous security activities in the correct Waterfall phase. All too often, security enters the SDLC for the first time at this point. The result is of this is delayed deployments," (Onpoint, n.d. p .5).

The Operations and Maintenance Phase of SDLC

"Operations and Maintenance encompasses all of the activities required to keep the system working as intended. It can include preventative maintenance on hardware, patch management, as well as application fault remediation. It does not include user functionality enhancement."(Onpointn.d. p. 6). Adding new functions at this point will more than likely cause a revisit to the Requirements analysis phase. However, most organizations have adopted a change management service that allows changes when necessary.

Unfortunately gaps are found in operations due to missed requirements, or critical defects that may require a change. The business will then create what is called a change service request. Managing change is the most important activity during the operations phase. "During the operations/maintenance phase, the security weaknesses are corrected in concert with the schedule and prioritization out lined in the point of action plan," (Onpoint, n.d. p. 7). When the configuration changes, the organization must track all modification and evaluate for effective continual security. If there is a plan to remediate the deficiencies it will be implemented here in this phase. Even though a system has flaws, it can still operate as long as there is a plan to remediate the issues. Testing will also continue in this phase too.

It is recommended that to ensure that all security controls in place remain effective; a plan for retesting all controls throughout the year and uses the results to fulfill the security control assessment requirement of the security authorization process. The security controls in this phase are to preserve the information and sanitize media. There are laws that govern how to maintain data when systems have retired and those laws must be observed and based on the level of information that must be protected, the system should still maintain that level of sensitivity. To keep data from leakage threats, it is important that media is sanitized or destroyed to protect date from dumpster divers and the like.

Conclusion

SDLC is a process designed to assist businesses in implementing systems in a sequential fashion that will lead to a successful deployment, operations, and retirement of the information system. In times past, organizations lacked the involvement of security professionals who where intimately involved in the development of the system and this caused great security deficiencies and additional costs to the organizations. If security is implemented during the development of system by overlaying security risk activities early on in its development, the organization will build a system that is less likely to be vulnerable to security threats to the physical system and the data that it processes and protects improving the overall security of the system and reducing significant risk to the organization. This approach will also save time and money.

References

Onpoint (n.d.) Incorporating Security into the System Development Life Cycle

www.onpointcorp.com

NIST Special Publication 800-37. (2010). Guide for Applying the Risk Management Framework to Federal Information Systems: *A Security Lifecycle Approach.*

NIST Special Publication 800-39. (2010). Integrated Enterprise-Wide Risk Management: *Organization, Mission and Information System View.*

NIST Special Publication 800-62. (2008). Security Considerations in the System Development Life Cycle

Radack, S. (n.d). National Institute of Standards and Technology: They System Development Life Cycle