



Integrating Risk Management in System Development Life Cycle

¹M. F. Unuakhalu, ²D. Sigdel, ³M. Garikapati,
Kentucky State University, U.S.A

Abstract: While impossible to eliminate all risk from organizational operations, one of the most effective ways to protect organization assets is through the incorporation of risk management and security into the System Development Life Cycle (SDLC). The paper goes through each phase of the SDLC and provides a minimum set of security steps that needs to be effectively incorporated into a system during its development. Adhering to an SDLC model increases the likelihood of project success, particularly in the area of fulfilling stakeholder requirements. By identifying security requirements early in the development process and incorporating them throughout the SDLC, security objectives will be easily met in all systems released from development. The intent is not to disturb or add more phases to the SDLC, but rather to incorporate security activities into an existing SDLC methodology.

Keywords: SDLC, risk management, IT initiation, development, acquisition, implementation, operation, security, management program.

I. INTRODUCTION

Organizations depend on information technology and the information systems that are developed from that technology to successfully carry out their missions and business functions. Information systems can include as constituent components, a range of diverse computing platforms from high-end supercomputers to personal digital assistants and cellular telephones. Information systems can also include very specialized systems and devices (e.g., telecommunications systems, industrial/process control systems, testing and calibration devices, weapons systems, command and control systems, and environmental control systems). Information and information systems are subject to serious threats that can have adverse impacts on organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. Threats to information and information systems include environmental disruptions, human or machine errors, and purposeful attacks. Cyber attacks on information systems today are often aggressive, disciplined, well organized, well funded, and in a growing number of documented cases, very sophisticated [5].

Given the significant and growing danger of these threats, it is imperative that leaders at all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks [1]. 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. 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 [2]. Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. It encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. 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.

II. IMPORTANCE TO SDLC IN AN ORGANIZATION

A systems development lifecycle (SDLC) has three primary objectives: ensure that high quality systems are delivered, provide strong management controls over the projects, and maximize the productivity of the systems staff. In order to meet these objectives, the SDLC has many specific requirements it must meet, including: being able to support projects and systems of various scopes and types, supporting all of the technical activities, supporting all of the management activities, being highly usable, and providing guidance on how to install it [4]. The technical of SDLC activities include system definition (analysis, design, coding), testing, system installation (e.g., training, data conversion), production support (e.g., problem management), defining releases, evaluating alternatives, reconciling information across phases and to a global view, and defining the project's technical strategy. The management activities of SDLC include setting priorities, defining objectives, project tracking and status reporting, change control, risk assessment, step wise commitment, cost/benefit analysis, user interaction, managing vendors, post implementation reviews, and quality assurance reviews.

SDLC system is use to build and maintain software systems. When you pay your telephone bill your payment is processed by a system. That system has evolved over many years and continues to evolve in order to meet the changing needs of the business. When the phone company cashes your check that check is also processed by a system which itself is evolving. These two systems are composed of manual activities and automated components. They also exist in the context of many other systems with which they must interface. Each system works so well individually because it is composed of a rigorous set of tasks, which result in well-defined outputs. Regardless of who is doing the task, the result is essentially the same. As staff turnover occurs, the system provides continuity to the way of doing business. Thus, no matter which bank the check is drawn on, the process is the same; no matter which Phone Company sends in the check, the process is the same. If there is no SDLC, each team must reinvent it based on their own experiences and judgments. In addition to this, SDLC systems also have a long life. The billing system and check processing system will probably never be de-automated. These systems will outlive their development teams. As staff turnover occurs, continuity is required in how the systems are supported. This is provided by the SDLC [8].

Another issue is systems integration. Can you imagine if the architects designing a skyscraper each had their own ways of creating and documenting the building's plans? The plumbing, wiring, heating systems, floors, walls, etc., would never come together. Most computer systems interface with other computer systems. The degree of system integration is rapidly increasing. The descriptions of functions and data at the interfaces must be produced and documented in a consistent manner; in much the same way as architects must have a standard way of documenting plans. This is provided by the SDLC.

III. IMPORTANCE OF RISK MANAGEMENT & SECURITY IN ORGANIZATION

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. 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 [3]. Some of the benefits of integrating security into the system development life cycle include [11]:

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;
- 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.

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 encompasses three processes: risk assessment, which includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures; risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process; and evaluation and assessment that evaluates process and keys for implementing a successful risk management program. The DAA or system authorizing official is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing (or accrediting) the IT system for operation.

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real-world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission essential security capabilities [11].

IV. INTEGRATING RISK MANAGEMENT AND SECURITY IN SDLC PHASES

Minimizing negative impact on an organization and need for sound basis in decision-making are the fundamental reasons organizations implement a risk management process for their IT systems. Effective risk

management must be totally integrated into the SDLC. IT system's SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. In some cases, an IT system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC. This section describes the characteristics of each SDLC phase and indicates how security and risk management can be performed.

A. 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.

Key security activities for this phase include [6]:

- Initial delineation of business requirements in terms of confidentiality, integrity, and availability;
- Determination of information categorization and identification of known special handling requirements to transmit, store, or create information such as personally identifiable information; and
- Determination of any privacy requirements.

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 [2]:

A.1 Control Gates

General types of control gates for this phase may include:

- A determination of the acquisition strategy to be used throughout the remainder of the development process;
- A system concept review that verifies that the concept is viable, complete, achievable, and in line with organizational mission objectives and budgetary constraints;
- A performance specification review that ensures that the initial system design has addressed all currently identified specified security requirements;
- An enterprise architecture (EA) alignment that harmonizes IT vision, standards, and business requirements, as well as security alignment with current and imminent security services;
- A financial review that verifies that the system will be aligned with CPIC artifacts and guidance while balancing the cost implications associated with risk management; and
- A risk management review that conforms to the recommended NIST risk management framework guidelines to reduce ambiguity in managing system risk. Included in this risk management review is a review of the information system security categorization results, which include identified information types, resulting impact levels, and the final system security categorization [9].

A.2 Major Security Activities:

A.2.1 Initiate Security Planning

Here is the list of major security activities that should begin in the initiation phase:

- Identify key security roles for the system development;
- Identify sources of security requirements, such as relevant laws, regulations, and standards;
- Ensure all key stakeholders have a common understanding, including security implications, considerations, and requirements; and
- Outline initial thoughts on key security milestones including time frames or development triggers that signal a security step is approaching.

This early involvement will enable the developers to plan security requirements and associated constraints into the project. It also reminds project leaders that many decisions being made have security implications that should be weighed appropriately, as the project continues.

A.2.2 Identification of Security Roles

Identification of the ISSO is an important step that should take into consideration the amount of time the individual will devote to this task, the skills needed to perform the duties, and the capability the individual has to effectively carry out the responsibilities. Identifying the ISSO early in the process provides the individual key insights into risk based decisions made early in the process and provides the other team members access to the ISSO for support in integrating security into the system development.

A.2.3 Stakeholder Security Integration Awareness

The ISSO provides the business owner and developer with an early understanding of the security steps, requirements, and expectations so security can be planned from the beginning. Topics may include:

- Security Responsibilities
- Security Reporting Metrics
- Common Security Controls Provided (if applicable)
- Certification & Accreditation Process
- Security Testing and Assessment Techniques
- Security Document & Requirement Deliverables
- Secure Design, Architecture, and Coding Practices
- Security Acquisition Considerations
- Major activities with development schedule and resource impact such as active testing, accreditation, and training

A2.4 Preliminary risk assessment

It should also be performed to develop a brief initial description of the basic security needs of the system, including needs to protect the integrity, availability, and confidentiality of system information. A preliminary risk assessment should define the threat environment in which the product or system will operate. This assessment is followed by an initial identification of required security controls that must be met to protect the product/system in the intended operational environment.

A.2.5. Assess Business Impact

An assessment of system impact on the agency lines of business correlates specific system components with the critical business services that are provided. That information is then used to characterize the business and mission consequences of a disruption to the system's components. An initial draft of this product early in the life cycle alerts system stakeholders to key IT and security decisions. This task should also take into account the availability impact level identified during the security categorization task.

A2.6 Assess Privacy Impact

When developing a new system, it is important to directly consider if the system will transmit, store, or create information that may be considered privacy information. This typically is identified during the security categorization process when identifying information types. Once identified as a system under development that will likely handle privacy information, the system owner should work towards identifying and implementing proper safeguards and security controls, including processes to address privacy information incident handling and reporting requirements.

B. Development/Acquisition Phase

During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. The first step in analyzing the security functional requirements is to identify the protection requirements for the system through a formal risk assessment process. The analysis will build on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific [5]. Thus, the organization should analyze security requirements; perform functional and security testing; prepare initial documents for system certification and accreditation; and design the security architecture [2]. 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.

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 [6].

B.1 Control Gates

General types of control gates for this phase may include[9]:

- An Architecture/Design Review that evaluates the planned system design and potential integration with other systems as well as incorporation of shared services and common security controls, such as authentication, disaster recovery, intrusion detection, or incident reporting.
- A system Performance Review that evaluates whether the system is delivering, or capable of delivering, to the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use. (For example, the ability of the system to maintain availability and data integrity at the expected extreme resource loads.)
- A system Functional Review that ensures functional requirements identified are sufficiently detailed and are testable.

- Mid-Project Status & Financial Review is important to detect major shifts in planned level of effort to ensure cost-benefit ratios are monitored and effective decisions are continued.
- A follow-on review of risk management decisions may be needed if, due to the aforementioned reviews, the system and/or its security controls and/or its requirements change.

B.2 Major Security Activities:

B.2.1 Formal Risk Assessment

The purpose of a risk assessment is to evaluate current knowledge of the system's design, stated requirements, and minimal security requirements derived from the security categorization process to determine their effectiveness to mitigate anticipated risks. Results should show that specified security controls provide appropriate protections or highlight areas where further planning is needed. To be successful, participation is needed from people who are knowledgeable in the disciplines within the system domain (e.g., users, technology experts, operations experts). The security risk assessment should be conducted before the approval of design specifications as it may result in additional specifications or provide further justification for specifications [9].

In addition to considering the security perspective of the system being developed/ acquired, organizations should also consider how the system might affect other systems to which it will be directly or indirectly connected. This may mean that there are inherited common controls to leverage or additional risks that need to be mitigated. In these cases, an enterprise review may be needed to provide a more comprehensive view of threats and vulnerabilities [6].

B.2.2 Select and Document Security Controls

The selection of security controls consists of three activities: the selection of baseline security controls (including common security controls); the application of security control tailoring guidance to adjust the initial security control baseline; and the supplementation of the tailored baseline with additional controls based on an assessment of risk and local conditions. An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business processes and the information systems and organizational infrastructure supporting those processes.

As with other aspects of security, the goal should be cost-effective implementation that meets the requirements for protection of an organization's information assets. In each situation, a balance should exist between the system security benefits to mission performance and the risks associated with operation of the system [7].

B.2.3 Design Security Architecture

With the increase in shared service providers and the centralization of some key security services within agencies, it is becoming more important to plan these services and understand how they will be integrated into the system. At the system level, security should be architected and then engineered into the design of the system. This may be accomplished by zoning or clustering services either together or distributed for either redundancy or additional layers of protection. Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users (e.g., customer service versus system administrators) [10].

This activity may be performed when reviewing from an IT development view the known bottlenecks and single points of failures. Minimal security requirements as well as requirements and constraints determined early in the process should provide the architects with a set of assumptions and constraints to build around. This activity can provide the most value for the system in lowering the total cost of ownership by planning the systems core components in a secure way.

B.2.4 Conduct Testing (Developmental, Functional, and Security)

Systems being developed or undergoing software, hardware, and/or communication modification(s) must be tested and evaluated prior to being implemented. The objective of the test and evaluation process is to validate that the developed system complies with the functional and security requirements [6].

The process focuses on specificity, repeatability, and iteration. For specificity, the testing must be scoped to test the relevant security requirement as it is intended for use in its environment. For repeatability, the testing process must be capable of the execution of a series of tests against an information system more than once (or against similar systems in parallel) and yield similar results each time. For iteration, each system will be required to execute functional tests in whole or in part a number of successive times in order to achieve an acceptable level of compliance with the requirements of the system. To achieve this, functional testing will be automated to the degree possible, and the test cases will be published, in detail, to ensure that the test process is repeatable and iterative. The use of automated testing tools and integration of the NIST Security Content Automation Protocol (SCAP) should be accomplished prior to the commencement of security control test and evaluation activities. Any security functionality not tested during the functional or automated testing will be

carefully examined to ensure compliance with the requirements during the explicit security control test and evaluation [9].

B.2.5 Develop Security Documentation

While the most prominent document is the System Security Plan, documentation supporting it may include [6]

- Configuration management plan
- Contingency plan (including a Business Impact Assessment)
- Continuous monitoring plan
- Security awareness, training and education (SATE) plan
- Incident response plan
- Privacy impact assessment (PIA)

Development of these documents should consider the maturity of the security services being documented. In some cases, these documents may contain only known requirements, common controls, and templates. Filling in these documents should begin as early as possible during the project. Documenting as the system development progresses can provide cost savings and enhance decision-making capabilities through a comprehensive approach that allows early detection of gaps.

C. Implementation/Assessment 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 [2].

C.1 Control Gates:

General types of control gates for this phase may include:

- System Test Readiness Review
- C&A Review
- Final Project Status and Financial Review
- Deployment Readiness Review
- Authorizing Official (AO) Decision
- IT Deployment or Connection Approval.

C.2 Major Security Activities

C.2.1 Create a Detailed Plan for C&A

Because the Authorizing Official (AO) is responsible for accepting the risk of operating the system, the AO can advise the development team if the risks associated with eventual operation of the system appear to be unacceptable. Specifications can impose excessive burden and costs if the acceptable residual risks are not known. The involvement of the AO is required for this determination of acceptable residual risks. It is easier to incorporate requirement changes during the planning stage of a system acquisition than during the solicitation, source selection, or contract administration stages [9].

C.2.2 Integrated Security into Established Environments and Systems

System integration occurs at the operational site when the information system is to be deployed for operation. Integration and acceptance testing occur after information system delivery and installation. Security control settings are enabled in accordance with manufacturers' instructions, available security implementation guidance, and documented security specification.

C.2.3. Assess System Security

Systems being developed or undergoing software, hardware, and/or communication modification(s) must be formally assessed prior to being granted formal accreditation. The objective of the security assessment process is to validate that the system complies with the functional and security requirements and will operate within an acceptable level of residual security risk [9].

C.2.4. Authorize the Information System

This authorization, granted by a senior agency official, is based on the verified effectiveness of security controls to some agreed-upon level of assurance and an identified residual risk to agency assets or operations. The security authorization decision is a risk-based decision that depends heavily, but not exclusively, on the security testing and evaluation results produced during the security control verification process. An authorizing official relies primarily on: (i) the completed system security plan; (ii) the security test and evaluation results; and (iii) the POA&M for reducing or eliminating information system vulnerabilities, in making the security authorization decision to permit operation of the information system and to accept explicitly the residual risk to agency assets or operations [6].

D. Operations/Maintenance Phase

Operations and Maintenance encompasses all of the activities required to keep the system working as needed. It can include preventive maintenance on hardware, patch management, as well as application fault remediation. It does not include user functionality enhancements. Additional functionality would require entering the Requirements Analysis Phase again. The Operation/Maintenance Phase continues for as long as the system exists in a production environment [10].

Key security activities for this phase include:

- Conduct an operational readiness review;
- Manage the configuration of the system;
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and
- Perform reauthorization as required.

D.1 Control Gates

General types of control gates for this phase may include:

- Operational Readiness Review
- Change Control Board Review of Proposed Changes
- Review of POA&Ms
- Accreditation Decisions (Every three years or after a major system change).

D.2 Major Security Activities

D2.1. Review Operational Readiness

Many times when a system transitions to a production environment, unplanned modifications to the system occur. If changes are significant, a modified test of security controls, such as configurations, may be needed to ensure the integrity of the security controls. This step is not always needed; however, it should be considered to help mitigate risk and efficiently address last-minute surprises [6].

D.2.2 Perform Configuration Management and Control

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 [2].

D.2.3. Conduct Continuous Monitoring

The ultimate objective of continuous monitoring is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates.

A well-designed and well-managed continuous monitoring process can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials. This information can be used to take appropriate risk mitigation actions and make credible, risk-based authorization decisions regarding the continued operation of the information system and the explicit acceptance of risk that results from that decision.

The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways, including security reviews, self-assessments, configuration management, antivirus management, patch management, security testing and evaluation, or audits. Automation should be leveraged where possible to reduce level of effort and ensure repeatability [9].

E. Disposal Phase

Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly.

When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that government resources and assets are protected [2].

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.

Key security activities for this phase include:

- Build and Execute a Disposal/Transition Plan;
- Archive of critical information;
- Sanitization of media; and
- Disposal of hardware and software.

E.1 Control Gates

General types of control gates for this phase may include [6]:

- System Closure Review
- Change Control Board
- Security Review of Closure.

E.2 Major Security Activities

E.2.1. Build and Execute a Disposal/Transition Plan

Building a disposal / transition plan ensures that all stakeholders are aware of the future plan for the system and its information. This plan should account for the disposal / transition status for all critical components, services, and information.

In many cases, disposed systems or system components have remained dormant but still connected to the infrastructure. As a result, these components are often overlooked, unaccounted for, or maintained at suboptimal security protection levels thus, providing additional and unnecessary risk to the infrastructure and all connected systems. A transition plan assists in mitigating these possible outcomes [9].

E.2.2 Ensure Information Preservation

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 [2].

E.2.3. Sanitize Media

NIST SP 800-88, Guidelines for Media Sanitization, divides media sanitization into four categories: disposal, clearing, purging and destroying. It further suggests that the system owner categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, decide on the appropriate sanitization process. The selected process should be assessed as to cost, environmental impact, etc., and a decision made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process [4].

Several factors should be considered along with the security categorization of the system confidentiality when making sanitization decisions. The cost versus benefit of a media sanitization process should be understood prior to a final decision. For instance, it may not be cost-effective to degauss inexpensive media such as diskettes.

E.2.4. Disposal of Hardware and Software

Hardware and software can be sold, given away, or discarded as provided by applicable law or regulation. The disposal of software should comply with license or other agreements with the developer and with government regulations.

E.2.5. Closure of System

The information system is formally shut down and disassembled at this point [10].

V. MAINTAINING SUCCESSFUL RISK MANAGEMENT PROGRAM

In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks

previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving [1]. This section lists few factors that will lead to a successful risk management program:

A. Good Security Practice

The risk assessment process should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization's business objectives or mission. There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies [3].

B. KeysFor Success

A successful risk management program will rely on: senior management's commitment, the full support and participation of the IT team, the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization, the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and an ongoing evaluation and assessment of the IT-related mission risks.

C. Continuous Monitoring

The monitoring program should be integrated into the organization's system development life cycle processes. The monitoring process involves active involvement of information system owners and common control providers, chief information officers, senior information security officers, and authorizing officials. The monitoring process allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions or business processes. Near real-time, risk management of information systems can be facilitated by employing automated support tools to execute various steps in the risk management function including authorization-related activities. In addition to vulnerability scanning tools, system and network monitoring tools, and other automated support tools that can help to determine the security state of an information system, organizations can employ automated security management and reporting tools to update key documents in the authorization package including the security plan, security assessment report, and plan of action and milestones [5].

REFERENCES

- [1] "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (2010)". NIST Special Publication 800-37, Revision 1, Gaithersburg, MD.
- [2] Shirley Radack (2008), 'The System Development Life Cycle (SDLC)', NIST Special Publication 800-64, Revision 2, Gaithersburg, MD.
- [3] Gary Stoneburner, Alice Goguen, and Alexis Fringa (2002). "Risk Management Guide for Information Technology Systems". NIST Special Publication 800-30, Gaithersburg, MD.
- [4] Bender RBT (2003), 'Systems Development Lifecycle: Objective and Requirements', Bender RBT Inc
- [5] Tim Grance, Joan Hash, Marc Stevens (2003), 'Security Considerations in Information System Development Life Cycle', NIST Special Publication 800-64 Revision 1, Gaithersburg, MD.
- [6] Richard Kissel and et. al. (2008), 'Security Considerations in System Development Life Cycle', NIST Special Publication 800-64 Revision 2
- [7] Steve Lipner and Michael Howard (2005), 'The Trustworthy Computing Security Development Life Cycle', Microsoft Corporation
- [8] Carol V. Brown and et al. (2012). "Managing Information Security." Pearson Education Inc, New Jersey.
- [9] Matthew Metheny (2007). "Federal Risk Authorization Management Program." One Enterprise Consulting Group, LLC.
- [10] www.onpointcorp.com/documents/Security_in_the_SDLC.pdf
- [11] Shirley Radack (2009). "The System Development Life Cycle (SDLC)". Computer Security Division, NIST.