**System Development Life Cycle (SDLC)**

Megan Celestino, Shane Byrne, Damian Parker, Donald Oxley

University of Phoenix

CYB/407

July 28, 2020

Steven Johnson

**System Development Life Cycle (SDLC)**

| **SDLC Phase** | **Description of Phase** | **Control Gates used in this phase.** | **Expected Outputs and Policies** | **Assurance Professional Approval** |
| --- | --- | --- | --- | --- |
| **Phase 1**  **Initiation** | * This establishes the 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 (exempli gratia, personally identifiable information (PII)). | * Ascertainment of the appropriate strategy to be used throughout the remainder of the development process. * Generation of a conceptual review of the system that verifies that the concept is viable, complete, achievable, and in line with the organizations mission objectives, as well as budgetary limitations. * Performance specification is reviewed that ensures the system design has addressed all currently identified specified security requirements. * Enterprise architecture (EA) alignment that harmonizes IT vision, standards, and business requirements; security alignment with current and imminent security services are also a part of the EA. * Financial review that verifies that the system will be aligned with Capital Planning and Investments Control (CPIC) artifacts and guidance and balancing the cost implications associated with risk management. * Establishment of a risk management review that conforms to the recommended NIST risk management framework guidelines to reduce ambiguity in managing system risk. | * Understanding of security expectations. * Initial schedule of security activities or decisions. * Security categorization. * High-level security requirements. * Level of effort estimates. * Identification of businesses supported by the system and how lines of business will be impacted. * Identification of core system components needed to maintain minimal functionality. * Identification of the length of time the system can be down before the business is impacted. * Identification of the business tolerance for loss of data. * Privacy impact assessment. * Development phase security training. * Quality assurance techniques, deliverables, and milestones. | * chief information officers * senior agency information security officers * authorizing officals |
| **Phase 2**  **Development/Acquisition** | * This phase of the project takes place after the company decides on what kind of system they will be using. * It could be purchased, designed, and programmed by our own tech team, or otherwise constructed via a vendor. | * Architecture and Design Review * Performance Review * Functional Review * Financial Review | -Documented analysis of laws and regulations  - System Security Plan  - Schematic of security integration | IT Dept. Managers, CISO (Or CIO if there is no CISO) |
| **Phase 3**  **Implementation**  **/Assessment** | * System is installed and evaluated * Information system is integrated into organization's environment * System certification activities are created and executed in sync with testing security controls * System accreditation activities are completed | * System Test Readiness Review * C&A Review * Final Project Status and Financial Review * Deployment Readiness Review * Authorization Decision * IT Deployment or Connection Approval | * Initial Work Plan * Verified list of operational security controls * System Documentation * Security Assessment Report * Input for POA&M * Potential documentation updates * Security Authorization Package * Security Authorization Decision * Final Security Authorization Package | Authorizing Official (AO) |
| **Phase 4**  **Operations/Maintenance** | * Maintain the system by doing proper updates and following most recent security protocols * Manage configurations of the system * Verify and document any changes necessary when swapping a system from QA to production | * Conduct readiness reviews * Review plan of actions * Accreditation Decisions | * Create policies regarding patching and updating (IE Patch Tuesday) * Create policies for continuous monitoring and what to do in the event of failures * Evaluation security implications after system changes | System Administrators and Security Engineers |
| **Phase 5**  **Disposal** | * Document the devices being disposed of with serial numbers and signatures proving they were properly disposed of * make sure hard drives are properly wiped or destroyed to prevent data loss * Dispose the devices * Create backups of all information in case needed later if the project may be continued | * System Closure Review * Change Control Board * Security review of closure | Documented disposal/transition plan for closing or transitioning the system and/or its information | Management |

**References**

National Institute of Standards and Technology. (n.d.).  NIST Special Publication 800-64 revision 2, security considerations in the system development life cycle. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf