International Journal of Business Quantitative Economics and Applied Management Research

Volume-3, Issue-11, Month – April 2017 ISSN No: 2349-5677

REDEFINING KEY CONTROLS FOR SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) COMPLIANCE

Varun Vohra
Merck
New Jersey, USA
varunvohra83@gmail.com

Abstract

System Development Life Cycle (SDLC) is a standard framework which governs the life span of a system from inception to end. Every phase of SDLC has its own significance and distinct requirements. No one can undermine the importance of these requirements but in order to gain reasonable assurance over the effectiveness of the system control environment, it is important to identify the key controls from each of the SDLC phases. It enables to achieve greater compliance rather than focusing on everything. This paper is inclined towards providing an overview of the key controls across all SDLC phases to achieve the above objective.

Keywords—SDLC, Controls, Compliance, Development, Deliverable, Requirements, Deployment

I. INTRODUCTION

It is usual human behavior that one tends to lose focus when you have a number of complex tasks on hand. On the contrary if critical tasks are identified from this pool of tasks, it increases focus and efficiency. The same philosophy applies to almost all complex areas including System Development Life Cycle (SDLC). SDLC is a very important process for any organization as it deals with new systems or major releases for existing systems and their compliance with policy and regulatory requirements. It is obvious that non-compliance with SDLC can put organizations in a tight spot. SDLC comprises of six different phases across the life cycle of a system and each phase has its own commitments in the form of deliverables. If it is that simple why is SDLC compliance a painstaking task for all organizations? The answer to it lies in the fact that SDLC is a complex process which spans across various cross-functional teams, timelines and numerous deliverables which are open to interpretation. All past work done in this area only highlight the nuances of the SDLC process and the numerous complex requirements around each phase. A lot of work has also been done to assess efficiency of different SDLC models which typically have the same underlying foundation of SDLC controls and requirements. However, none of the past work discusses any means to enhance compliance by simplifying the foundational SDLC process and deliverables. Therefore, there is an opportunity and need to simplify this process by identifying key control requirements from each phase which can provide reasonable assurance over the system control environment and compliance with SDLC requirements. It will also ensure that the SDLC process is understood clearly by one and all. The next sections help us understand the distinct requirements across various SDLC phases and a simplified version of key controls for SDLC compliance.

II. OBJECTIVES OF THIS STUDY

In line with the above mentioned research problem, the aim of this paper is to figure out a solution which can achieve the following objectives:

- Take out complexity from the SDLC process and deliverables to make it simpler which can help in achieving greater compliance.
- Identify key control requirements from each SDLC phase which can provide reasonable assurance over the system control environment and help achieve the above goal.

III. REQUIREMENTS ACROSS SDLC PHASES

SDLC is a process of developing, deploying and de-commissioning information systems through a multi facet approach across six different phases. Below sections discuss various requirements and corresponding deliverables for each SDLC phase.

3.1 Requirements Phase

Once the project is approved by the business sponsors, functional and technology teams take it up from here. All members of the project team are trained in SDLC control requirements across all phases prior to the commencement of the project. The first step in this phase is to gather the business requirements from key stakeholders and perform the feasibility analysis which will enable to draft a Requirement Specifications document [1]. The next step is to evaluate the risk profile of the information system i.e. type of data which will be processed and stored, significance from a disaster recovery and business continuity standpoint, etc. Further, a security risk and privacy assessment is performed to understand the complete IT landscape around the system. If a third party is involved in the project, a third party assessment is also performed. Lastly, a Quality Assurance Plan is completed which defines objective, roles and responsibilities, tasks and the project schedule. It also identifies the repository for retention of all approved SDLC deliverables.

3.2 Design and Development Phase

In this phase, Design Specifications and Development Plan are completed based on the system and software design prepared from the Requirement Specifications and QAP which were completed in the first phase [1]. As the code development progresses, static and dynamic code reviews are performed. It is followed by performing unit and system testing of the developed code in order to ensure everything is in accordance with the Design Specifications and Development Plan [2]. Finally, a Design and Development Summary Report is completed which include results from all activities performed based on Design Specifications and Development Plan. All exclusions are also documented in this summary report.

3.3 Testing Phase

In this phase, test cases are created which have the ability to test the system for its intended business use. These test cases are run as part of the overall Acceptance Testing performed by business users [3]. The results from this User Acceptance Testing indicating the Success/Failure of these test cases are documented as part of a Test Summary Report. The infrastructure supporting the system is also qualified for installation and operations in this phase.

3.4 Deployment Phase

Prior to the deployment of the system in production, few more checks and balances are performed. Data migration and conversion plans are executed and completed and any exceptions are clearly documented. Based on the criticality of the system, a Disaster Recovery Plan and Business Continuity Plan are completed. All test accounts are removed from the system and a vulnerability scan is performed to ensure there are no high risk vulnerabilities prior to deployment in production. Procedures related to operational areas like change management, user account management, incident management etc. are also completed. Finally, a summary of all key activities up till this phase are documented as part of a Quality Assurance Summary Report [4]. This summary report includes the dispositioning of the activities proposed in the Quality Assurance Plan in the Requirements phase and the final go-ahead for deployment of the system in production.

3.5 Maintenance Phase

Once the system is deployed in production, it is ensured that it is always in compliance with all policies and procedures in operational areas like change management, user account management, incident management, back-up, disaster recovery etc. In addition, security controls in areas like logging and monitoring, vulnerability and patch management, intrusion detection etc. are maintained [1]. Periodic assessments and audits are performed to ensure compliance in production environment. In case the system goes through any major upgrade or modification, SDLC is triggered and the whole cycle is followed again [5].

3.6 Decommissioning Phase

Once the system reaches its end life, the system is prepared for decommissioning. A Decommissioning Plan is created which details the activities to be followed for data retention and archival, removal of accounts, data migration, etc. [6]. A Decommissioning Summary report is drafted upon completion of these activities. This summary report includes the dispositioning of the activities proposed in the Decommissioning Plan and the final go-ahead for decommissioning.

IV. KEY CONTROLS FOR SDLC COMPLIANCE

SDLC has a number of deliverables across every phase as discussed in above section. All deliverables are important but few of them can be termed as the key control points for each phase. Let me clarify that it does not undermine the importance of other deliverables but only implies that these key controls are able to provide reasonable assurance on the system control environment for SDLC compliance. Below sections discuss the key controls for each SDLC phase. An overview of all the key controls across all six SDLC phases is also illustrated in Fig. 1.

4.1 Requirements Phase

Security risk and privacy assessment along with the Quality Assurance Plan are the key controls in this phase. Security risk and privacy assessment is able to tell us the risk posture of the IT environment while Quality Assurance Plan outlays the project plan along with its execution strategy. There are other deliverables in this phase but these two deliverables have some level of dependency on other deliverables which have to be worked upon in order to complete both these deliverables. Therefore, both these deliverables approved by business and technical teams are able to act as control points for this phase and provide reasonable assurance from an SDLC perspective.

4.2 Design and Development Phase

Design and Development Summary Report is the key control in this phase as this summary report includes all key details from other deliverables like Design Specifications and Development Plan. Therefore, this deliverable alone approved by business and technical teams is able to act as a control point for this phase and provide reasonable assurance from an SDLC perspective.

4.3 Testing Phase

User Acceptance Test Summary Report is the key control in this phase. Individual test cases are run by business users as part of the acceptance testing and result into a Success/Failure. This Test Summary Report details the collective results after running all the test cases and is approved by business and technical teams to act as a control point for this phase and provide reasonable assurance from an SDLC perspective.

4.4 Deployment Phase

A Quality Assurance Summary Report is the key control in this phase. There are a number of other deliverables in this phase but all the key activities up till deployment are dispositioned in this summary report including the final go-ahead by both business and technical teams for deployment of the system in production. Therefore considering the dependency of this deliverable on other deliverables, it is a key control point for this phase and provides reasonable assurance from an SDLC perspective.

4.5 Maintenance Phase

Periodic assessments and audits are the key controls in this phase. As the system is in production, these assessments act as a control point for this phase to ensure compliance with all policies and procedures in operational and security areas.

4.6 Decommissioning Phase

A Decommissioning Summary report is the key control in this phase. This summary report includes the dispositioning of the activities proposed in other deliverables in this phase including the final go-ahead for decommissioning by both business and technical teams. Therefore considering the dependency of this deliverable on other deliverables, it is a key control point for this phase and provides reasonable assurance from an SDLC perspective.

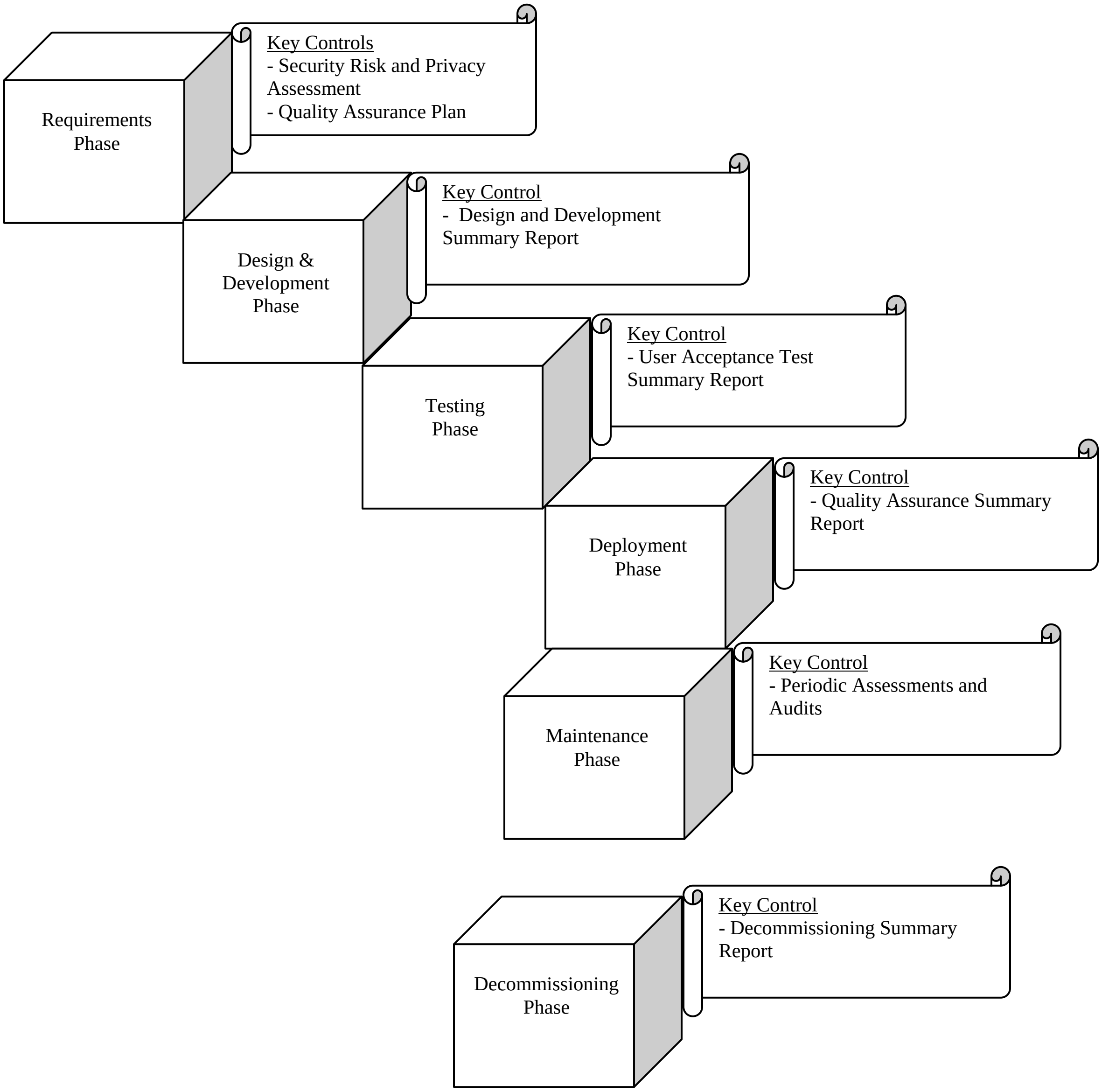
Requirements Phase
Key Controls
- Security Risk and Privacy Assessment
- Quality Assurance Plan
Design & Development Phase
Key Control
- Design and Development Summary Report
Testing Phase
Key Control
- User Acceptance Test Summary Report
Deployment Phase
Key Control
- Quality Assurance Summary Report
Maintenance Phase
Key Control
- Periodic Assessments and Audits
Decommissioning Phase
Key Control
- Decommissioning Summary Report

Fig. 1 Key controls across SDLC phases

V. CONCLUSION

- SDLC is embedded in the DNA of an organization and needs to be adhered to all the time. Therefore, it is of utmost importance for any organization to ensure SDLC is followed for all newly developed systems to minimize the risk in the control environment.

- Complexity always leads to confusion so the only way to achieve SDLC compliance is by taking out complexities from the overall SDLC process and deliverables by making it simple so that key SDLC controls are understood and adhered to by all.

- This paper helps in re-defining SDLC requirements and deliverables by providing an overview of a simple set of key controls across all SDLC phases in order to achieve greater compliance.

REFERENCES

[1] M. Saini, and K. Kaur, “A review of open source software development life cycle models,” International Journal of Software Engineering and Its Applications, vol. 8, no. 3, 2014, pp. 417-434.

[2] R. Scroggins, “SDLC and development methodologies,” Global Journal of Compute Science and Technology, vol. 14, issue 7, ver. 1, 2014, pp. 20-22.

[3] S. Kaur, “A review of software development life cycle models,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, issue 11, 2015, pp. 354-360.

[4] J. Lannen, “Why SDLC controls are important for a project,” 2013, Turnkey IT Solutions.

[5] V. Silver, “Auditing the SDLC for the non-IT auditor,” Group1 Solutions.

[6] S. Radack, “The system development life cycle”, NIST, 2008, Report No. 800-64.