ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 6.047

Volume 5, Issue 3, March 2017

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

# *Risk Management in System Development Life Cycle (SDLC)*

**Varun Vohra**
Merck
New Jersey, USA

***Abstract:*** ***System Development Life Cycle (SDLC) is a standard framework which details steps to build a system. Standard SDLC framework needs to be enhanced to address security and risk concerns. There are different schools of thought related to this approach with some supporting risk management only in requirement and design phases of SDLC. However with the changing risk and threat landscape and to ensure optimal security, risk management needs to be tightly integrated in all phases of SDLC. This paper is inclined towards providing an overview about the significance of risk management and its integration in all phases of SDLC.***

***Keywords: Risk, Threat, Vulnerability, Control, Mitigation, Security, SDLC.***

## I. INTRODUCTION

Risk is the potential harm that may arise from a current process or a future event. It is not possible to reduce risk to zero, therefore every organization operates in a risk environment with varying degrees of risk in different areas. Risk management is all about managing risks by identifying and addressing them. It helps the organizations to perform a cost benefit analysis of the cost to protect an asset vs. the cost when it gets compromised or is not available. A simple example can be a car security system. If the cost to get the car security system is greater than the value of the assets getting protected, then it is not worth a deal. SDLC is a standard framework for system development which includes various phases as illustrated in Figure 1 below.

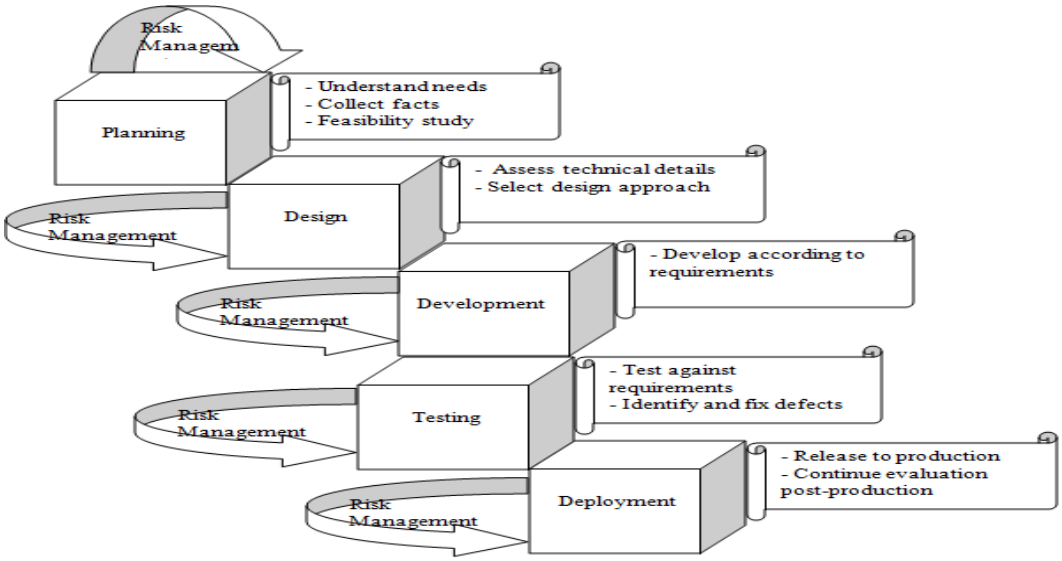


Fig. 1 Key stage gates in SDLC

When we look at the SDLC framework, it talks about key processes around system development but not the risks involved during these processes. According to the data by Standish group, around 31% of projects get cancelled before they are completed while 52% of projects have 189% cost overrun [1]. This data clearly articulates that risks are being overlooked in

 

different phases of SDLC resulting in failure. Therefore, it is very important that risk management is tightly integrated within all phases of SDLC i.e. planning, design, development, testing and deployment. Risk management involves two key stage gates – Risk identification and Risk mitigation [2]. The important thing to note here is that risk management process remains same for all phases of SDLC and should be triggered in every phase. The next section helps understand the two stages gates of the risk management process which is repeatable across different phases of SDLC.

## II. RISK IDENTIFICATION

Risk identification is an important step in the risk management process. The outcome from this step acts as input to the risk mitigation process. Risk identification is a collection of five key steps as described below.

### *A. System and Infrastructure Assessment*

This step involves understanding the landscape of the system and supporting infrastructure. It is also known as risk profiling to identify the criticality of the system and supporting infrastructure [3]. The focus areas to look at should be the type of data processed, business process supported, interface with upstream and downstream systems and the regulatory impact [2]. It will help build a good picture of the composition of the IT environment.

### *B. Threats and Vulnerabilities Identification*

The focus of this step is to identify both technical and non-technical vulnerabilities [2] which if exploited by threat sources can lead to actual threats. Some common natural threat sources are floods, earthquakes, etc. and human threat sources are malicious attack, espionage, etc. Security scans done by automated tools and system logs are some sources to identify technical vulnerabilities. We need to note that output from the scan performed by most of the automated tools are potential and confirmed vulnerabilities. Potential vulnerabilities need further analysis as they can turn out to be false positives for a specific IT environment [4].

### *C. Impact Analysis*

CIA (Confidentiality, Integrity and Availability) is a widely accepted security model which is applicable in any secure system. This step evaluates the impact if a threat occurred by considering CIA model as the foundation of a secure system [2]. The impact is analysed for one or more of the three pillars of CIA model i.e. Confidentiality, Integrity and Availability.

### *D. Risk Determination*

Taking impact analysis as input, this step focuses to assess the risk level. It can be done using a quantitative or a qualitative approach. The quantitative approach is heavily dependent on data as it is based on the probability or likelihood of each risk materializing and the impact if it occurs. The final outcome is a cross product of these two parameters. Based on the numerical value, it can be categorized as high if a risk has high probability of materializing and high impact or it can be categorized as low if a risk has low probability of materializing and low impact. Data is not always available so quantitative approach though being good cannot always be adopted. On the other hand, qualitative approach provides the flexibility to decide whether the probability of risk materializing is high, medium, or low as well as the impact if it occurs. The final outcome is judgmentally categorized as high if a risk has high probability of materializing and high impact or it can be categorized as low if a risk has low probability of materializing and low impact [2].

### *E. Control Requirements*

Based on the risks identified from the steps above, control requirements are outlined which can either mitigate these identified risks or minimize them to an acceptable level [2]. These control requirements are the final outcome from the risk identification process and acts as an input to the risk mitigation process [3].

 

## III. Risk Mitigation

Risk mitigation is the final step in the risk management process which helps reduce the risk to an acceptable level. There are various methodologies related to risk mitigation but only one of them is widely adopted i.e. risk limitation. It is often considered as an amalgam of risk acceptance and risk avoidance [4]. It is achieved through implementation of controls identified in the last step of the risk identification process. For example, if there is a risk of an unauthorized change being deployed in production, it can be limited by implementing a change control process where all activities in production are logged and monitored. Below are the some other risk mitigation methodologies.

### *A. Risk Avoidance*

It involves eliminating the root cause of the risk altogether and therefore has a cost associated to it [2]. For example, if a system is storing personal identifiable information and is not encrypted, there is a risk of the data getting compromised. This risk can be avoided by either not storing the data or enabling encryption and both these options have an associated cost.

### *B. Risk Acceptance*

This methodology is generally adopted when the cost associated with the materialization of the risk is less than the cost associated with mitigating the risk [2]. For example, if accounts in a certain system are not locked after five consecutive failed login attempts due to technical limitations and the risk is fairly low as rest of the password parameters are strong enough. In addition if the cost to implement any external solution to enable locking of accounts is much higher than the cost associated with materialization of the risk, it is a perfect scenario for risk acceptance.

### *C. Risk Transfer*

As the name suggests, it involves transfer of risk to a third party and is generally used if the cost to mitigate the risk is much higher than insuring it [2]. For example, cyber security is an emerging risk for all organizations and the cost to implement various solutions to protect the organization from cyber threats is much higher than purchasing the cyber security insurance, a risk transfer approach is the best solution in this scenario.

An overview of how risk management can be performed in SDLC is illustrated in Figure 2 below.

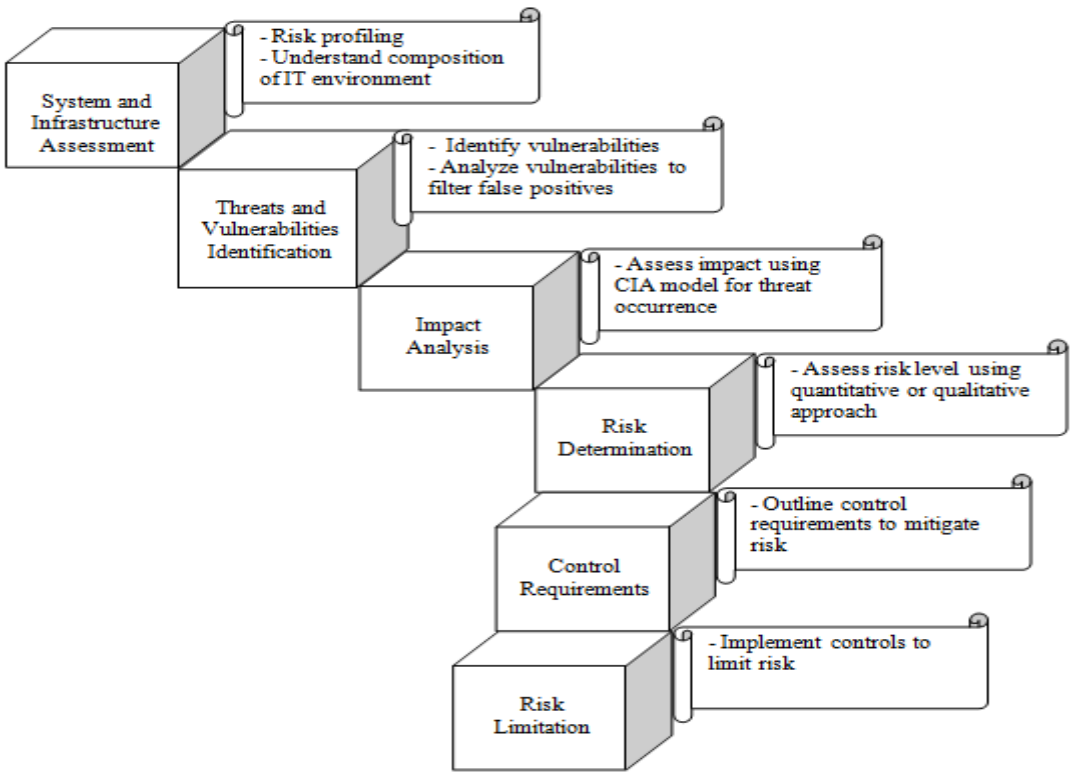


Fig. 2 Risk Management in SDLC

## IV. Conclusion

Risk management is a process to identify the risks along with the remediation steps to minimize their impact while SDLC is the framework which articulates steps to build a robust system [5]. In today's era where information and cyber security is one of the top priorities for any organization, it is very important to draw synergies from both these areas in order to ensure that all systems are secure and it is only achievable if risk management is tightly integrated in the DNA of SDLC. This paper provides the details of risk management process along with its integration across all phases of SDLC.

## References

1. T. Clancy, "The Standish Group Report Chaos-Project Smart," The Standish Group, 1995.
2. G. Stoneburner, A. Goguen and A. Feringa, "Risk Management Guide for Information Technology Systems," NIST, 2002, Report No. 800-30.
3. M. Unuakhalu, D. Sigdel, M. Garikapati, "Integrating Risk Management in System Development Life Cycle," International Journal of Software and Web Sciences, pp. 1-9, 2014.
4. K. Sahu, Rajshree, R. Kumar, "Risk Management Perspective in SDLC," International Journal of Advanced Research in Computer Science and Software Engineering,, Vol. 4, Issue 3, pp. 1247-1251, March, 2014.
5. H. Hijazi, T. Khdour, A. Alarabeyyat, "A Review of Risk Management in Different Software Development Methodologies," International Journal of Software Applications, Vol. 45- No. 7, pp. 8-12, May, 2012.

## Author(s) Profile

**Varun Vohra,** received his MS degree in Management Information Systems from State University of New York at Buffalo (US) and B.Tech degree in Computer Science & Engineering from Vellore Institute of Technology, India in 2011 and 2006, respectively. He has extensive experience in the area of IT audit, risk and compliance with special focus on information security. He is currently working in a senior position in one of the world's largest pharmaceutical company in the US.

 