Chapter 5
Information Systems Security Risk

ABSTRACT

Proposed method is applied to Software Engineering for security software quality management. DMAIC framework applies stochastic techniques to risk management. Hypothetical software project is considered with specified delivery target date and quality goal. Testing project is analysed uncompleted with weeks of testing remaining. Simulation considers testing defects and predicts the number defects at the end of test. If simulation confirms that the quality goal will be met, testing continues as is. Simulation regularly checks quality goal as testing progresses. If the predicted quality is missing targets, simulation predicts when the target will be achieved. There are two options, either more resources should be allocated to the project to rectify the problem, or the project should be delayed. An improvement project is defined to rectify the problem. Control is shown by using a very similar scenario with data for Quality Control, which applies slightly different models.

INTRODUCTION

This chapter presents the Quality Management application class of the method. It is applied in Software Engineering to manage the risk of the security software quality.

Information systems security breaches heavily impact all human activities, including individuals, organisations and corporate businesses, resulting

DOI: 10.4018/978-1-5225-2703-9.ch005

in enormous and irrecoverable damages and costs. Therefore, managing information systems security risk is essential today. Security software is a major part of every information system, so, the quality of the security software is a crucial contributor to information systems security. Information systems security is very important today, so a key objective for security software is to achieve Six Sigma quality assurance. Implementing security software with Six Sigma quality into information systems will ultimately reduce the information systems security risk.

Achieving Six Sigma quality for security software is an imperative to software projects across the IT industry today. This chapter presents the Six Sigma DMAIC structured approach to manage security software quality and achieve the Six Sigma quality goal in an ongoing software project.

Software quality is a multidimensional property of a software product including customer satisfaction factors such as reliability, functionality, usability, performance, capability, install-ability, serviceability, maintainability and documentation. Software processes are inherently variable and uncertain, thus involving potential risks. A key factor in software quality is *Software Reliability* as it is the quality attribute most exposed to customer observation. In this chapter, the terms "reliability" and "quality" are used interchangeably. Software Reliability is a main subject in *Software Reliability Engineering (SRE)* (Lyu 1996).

Evolution

The software reliability analytic models have been used since the early 1970s (Xie 1991, Lyu 1996, Kan 2002). For example, Orthogonal Defect Classification (ODC) was elaborated by *Chillarege* and implemented by IBM™; the Inflection S-shaped Software Reliability Growth Model was used in this work (Lyu 1996, Chapter 9).

The need for a simulation approach to software reliability was recognised in 1993 by *Von Mayrhauser et al.* (1993). Subsequently, substantial work on simulation was published (Tausworthe & Lyu 1996; Gokhale, Lyu, & Trivedi 1997, 1998; Lakey 2002). Also, *Gokhale & Lyu* (2005) applied simulation for tailoring the testing and repair strategies.

Applications of Six Sigma in software development have been published since 1985 (Mandl 1985, Tatsumi 1987, Brownlie & Phadke 1992, Bernstein & Yuhas 1993, Tayntor 2002). Six Sigma software practitioners usually