

Security as a Dimension of Quality

Information security is implemented through processes, yet the well-developed disciplines of quality process management are rarely used to implement robust infosec processes.

This paper discusses how quality process management disciplines were used at an insurance company to create a new process and improve the company's security posture.

Introduction

We do not believe that information security managers need more war stories about regulatory compliance, dissatisfied customers, IT cost justification, or the next great security technology investment. Professional managers are acutely aware of the pressures of their office and the need to better manage their security processes.

Whether the key issues are compliance, assurance, or cost, the underlying issue is always performance. In our opinion, most managers have failed to create an infrastructure for systemic and continuous performance improvement. We believe the shortcoming does not lie in the recognition of the problem or the desire to take action. Rather, the challenge lies in understanding the variables that influence process performance and the powerful tools developed to manage it.

A fundamental shift in how organizations approach information security is needed. Quality management learned long ago that extrinsic, compliance- and inspection-driven approaches—typical of information security today—are inherently limited, if not fundamen-

tally flawed. The revolution in quality management disciplines and techniques over the last few decades, championed by such luminaries as Deming and Juran, provides undeniable evidence for a better way to achieve the goals of information security.

This paper focuses on the application of quality management disciplines and techniques for information security, and specifically documents the creation of a new process using tools and methods that would readily be recognized by Six Sigma Black Belts. Our experience with Security Kaizen (“continual improvement for security”) started at a very large Japanese company that had a desire to use information security as a strategic market differentiator by mobilizing virtually every employee and over 650 Security Kaizen teams. More recently, our path has led us to adapt Security Kaizen to U.S. management styles both to improve existing processes and to create and deploy new processes.

Leaders who manage with data find a better way—not just an easier way—to achieve business results.

Synopsis

Client Profile

A publicly traded, high growth auto insurance company with operations in 16 states. An industry leader, pioneering Internet business models with approximately 30,000 employees—on pace to double within 10 years.

The Situation

With business demands high, application server deployments posed significant risk due to lack of conformity and change management and out-of-date policies. Accountability and performance improvement were difficult without a common criteria and the business impact was widespread.

The Solution

The wide range of teams involved with configuration management required a unified build and maintenance process that ensured workflow consistency along common criteria throughout the organization. A measurement system that identified needed improvements and integrated audit and remediation activities was built.

The Return

Process variation was improved threefold over a three month period. Complete scan cycle touching every server was reduced to 10 weeks' time, or five times per year. Server configuration variance and process time was significantly reduced. The project is forecasted to reach break-even after 7 months and return 73% on investment after the first year of operation.

The methods and tools are well-developed and can be organized into three dimensions of quality: (1) quality of design (deciding what is important to manage); (2) quality of conformance (ensuring you can manage what is important); and (3) quality of performance (ensuring that the effective management of processes is having the desired effect on the company business).

This paper illustrates the benefits and challenges that one large organization faced when employing quality management to improve the cross functional process of asset configuration management. It is important to note, however, that the principles and methods applied here can be applied to any information security process. Inside this paper you will learn how a top-five insurance company redesigned a complex server configuration management function, eliminating waste by “instrumenting” the process and establishing process control disciplines.

The Project Challenge

In January 2006, CSS was engaged by a large Midwestern insurance carrier to design a new process to control security settings for network servers. The company had experienced rapid growth, doubling its size in two years. Now at 30,000 employees, the company forecast its maturation of 60,000 in the near future. With most revenue driven by web-based services and independent agents nationwide, the organization deployed 1,000 new servers each year and 1,000 new clients each month. Availability and security were increasingly key concerns for IT service. Each server and client asset has a large variety of potential hardware and software configurations that affect functionality. While some configurations and settings provide users with needed capabilities, some restrict system capabilities in order to protect the confidentiality, integrity, and availability of systems and information assets.

As deployed, a formal system of configuration management only controlled server and client asset settings during the initial build stage of their life cycles. The system had no capability to translate security policies into technical specifications for deployment. Further, once servers and clients became operational, their configurations were often tailored, modified, or simply became outdated, which rendered them non-compliant to IT and security policies. No formal and documented audit and remediation process existed to ensure complete security compliance for servers or clients and new requirements from the Payment Card Industry mandated a formal set of controls.

As a result, even where the process was well controlled, it did not fully implement current security policy, and where it was uncontrolled, it exposed business and customer information assets to risks of unknown magnitude and criticality.

Establishing a control system had challenges because the organization had little experience with establishing standardized processes and the existing mix of system configurations out in the field was completely unknown. Even the effects of establishing a configuration standard were unknown because application developers had no experience working with a restricted control system.

Building the Team and Scoping the Project

A cross-functional team was formed of both server and client representatives and each pledged up to four hours per week participation during the aggressive 10-week design phase. The Security Kaizen approach was chosen because it leveraged the power of proven quality management methods and delivered a process design along with a management system to provide agility and continual improvement.

The goal of the Security Configuration Project was to design a standardized process for deploying security policy into the server deployment life cycle. Audit and remediation cycles were included in the process. A controlled pilot implementation would establish process capability and ensure that internal IT customers would support and comply with the new requirements. The process would be driven by the evolving security architecture and security technical standards, which

Project Payback

A significant area of financial benefit arose inside help desk operations. The improved process performance showed second tier technical support calls initially lower by 30 minutes per staff member per week. This conservative estimate alone realizes a payback inside two and one half years.

operationally define compliant security settings for initial, build, and operational stages in the server life cycle. The end result would be a process that is repeatable, i.e., consistently driving compliant configurations and remediation for non-compliant systems, and reproducible, i.e., the process serves multiple IT assets (both servers and clients) and is OS and technology agnostic.

Gathering Requirements

Because of the anticipated impact of establishing a new process, collaborative design with the participation and support of the user community was critical to the success of the project. A powerful and flexible method of gathering the Voice of the Customer (VoC) was used to establish design requirements. Key questions about the new process were drafted and members of the team were trained both as interviewers and notetakers to conduct live interviews with key stakeholders. Several members noted that the interview training and listening skills were valuable lessons they would use throughout their careers. The resulting notes captured verbatim design requirements that were translated into Critical-to-Quality (CTQ) design elements. To ensure the requirements were multidimensional, the Kano Method of categorizing requirements as “basic,” “specified,” or “exciting” provided added depth and meaning to the stakeholder interviews.

Designing the Process

Three primary domains of the project became apparent following the VoC analysis: 1) translating the new security policies into machine settings, 2) installing process controls during the server build phases, and 3)



Figure 1. Security Kaizen—Four Cycle Model

establishing a network audit and remediation process. Subteams were selected to map the workflow of each domain and specify the inputs and outputs of each step in the form of a SIPOC (supplier-input-process-output-customer) diagram.

Teams were encouraged to be creative in the detailed process design and used a process of Stretch-Step-Leap to brainstorm innovative ideas. A “Stretch” design fulfills all the VoC CTQs and takes into account the current environment and organizational skill sets. A “Step” design is more revolutionary in that it may call for new skill sets or infrastructure. A “Leap” design is even more radical in that it may demand technology changes to accomplish process goals. An additional enhancement of the design process was to maximize selected process capabilities called “illities” (e.g., installability, adaptability, serviceability, documentability, reliability, testability) and minimize the “ings” that increase process costs and complexity (e.g., varying, exacting, complicating, sorting, sensing, complying, demanding new skills).

Design concepts are the specific subprocess that implement the CTQs mapped from the VoC verbatims. Once design concepts were developed with a completed SIPOC, a direct mapping of the VoC verbatims to the CTQs to process allowed the team to establish performance measures for project progress and process capability.

Establishing the Management System

Designing a new performance measurement system requires that each metric be deconstructed into the primitive measures that go into its calculation (e.g., gasoline mileage for an automobile is calculated by the primitives “amount of gasoline used” and “distance traveled.”) With the primitive measures defined, we were able to evaluate the performance metrics for their cost and difficulty of acquisition and their granularity and accuracy. A metric correlation matrix clarified the interactions between performance elements and provided the foundation for causal analysis of the overall system performance.

A formal control plan established exactly how each measure would be captured, who would be responsible, and how the data would be displayed. Statistical Process Control (SPC) is the go-to method for translating performance data into actions to control or improve performance. The finished data charts were posted on a series of dashboards customized for executive review, business performance, and process performance. A two-

person team of “Data Wranglers” were trained specifically for this purpose. Once the process was implemented, they would take on the additional responsibility of training process owners to interpret the data presented to them in the form of performance dashboards.

At this point the process was fully vetted out and a RACI (responsibility-accountability-contribution-information) diagram provided details on process workflow as well as organizational contributions to key steps in the process.

Pilot & Optimization

It is said that no battle plan survives the first encounter with the enemy—and process design is no different. As the team piloted the process, details about what actually happened in the process were captured on process flowcharts, using a formal method called Business Process Modeling Notation (BPMN). This method clarified the gritty details of actually performing the steps and allowed us to identify steps that could operate in parallel.

As the process is piloted in the real world, a Failure Mode and Effects Analysis (FMEA) is being conducted to identify potential problems, spot opportunities to standardize, and make the process robust against foreseeable problems. A guiding principle in process design is that you do not control a process by controlling procedures. Procedures are about “doing things right” not “doing the right things.” Every attempt is made to keep the process lean, agile, and malleable to the needs of the process workforce. Processes must always be built to allow workers to question and refine process requirements.

Throughout the pilot phase, visibility and support from all levels of management is important. Especially as the project moves from the fun of the “romance” phase to the hard work of the “marriage” phase—project champions must maintain a high level of interest in learning the process lessons.

The Value Proposition

The project had two significant phases. First, collecting voice of the customer, designing a version of the process for pilot testing, designing the process performance dashboards, and deploying the audit and remediation system. The second phase was designed to educate and train configuration and security management personnel in the use of statistical process control techniques and process management skills.

These two phases improved process consistency by reducing configuration variation by December 2006. The project uncovered many undocumented processes at the application layer that lead to unknown changes in configurations.

The process management documentation provides in-depth knowledge that can be invaluable during security and compliance audits.

Reliability was improved by providing predictability and insight into the security dependent process of configuration management. Clarity around roles, responsibilities, workflow, and performance dependencies lead to faster and more secure deployments.

The help desk service ticket costs were reduced by an estimated \$18,000 per month (\$216,000 annually). The overall improved effectiveness of the server configuration management process has shortened the cycle time and significantly reduced variation results.

Beyond the performance benefits, the client experienced significant value with improved policy that reflects real world operations and best practice industry standards.

Certified Security Solutions, Inc. is a nationwide information security consulting firm, with headquarters in Seattle, Washington. CSS helps clients leverage existing and emerging technologies in practical ways to reduce risk and protect information assets. CSS specializes in three critical areas of information security: security performance management , application and platform security, and identity and access management. For more information and for a complete list of branch offices, visit www.css-security.com or e-mail sales@css-security.com.