EDPACS: The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uedp20

# Integrating Information Security through Total Quality Management

Sarah Schiltz

Published online: 10 Oct 2014.

To cite this article: Sarah Schiltz (2014) Integrating Information Security through Total Quality Management, EDPACS: The EDP Audit, Control, and Security Newsletter, 50:5, 16-23, DOI: 10.1080/07366981.2014.962301

To link to this article: http://dx.doi.org/10.1080/07366981.2014.962301

EDPACS 2014

# INTEGRATING INFORMATION SECURITY THROUGH TOTAL QUALITY MANAGEMENT

SARAH SCHILTZ

**Abstract.** As companies begin to increase their electronic presence, digitizing increasingly more of their private and sensitive information, the need for information security becomes mandatory. While the relationship between technology and business functionality expands, information security has safeguarded the information the business needs to survive. Organizations are increasingly aware of information security issues and are constantly seeking control measures. Information security studies predominantly focused on the presence of information security controls rather than the quality of those controls. Security, as an element of quality, must be addressed in the development, implementation, and monitoring of strategy and policy. In order to ensure that adequate controls are established for information systems, quality assurance and information systems auditors should maintain a close working relationship. Total Quality Management is mandatory in the successful application and proliferation of information security controls.

Information security is a common topic discussed in offices of practically any business today. The need to defend information from unauthorized access is mandatory as organizations increasingly store sensitive and personal information in electronic systems. While information security is integral in safeguarding this information, quality management is also necessary in providing continuity and consistency. The union of Information Security (InfoSec) and Quality management results in a collaborative relationship, however, only a few organizations have fully realized the benefits of this paradigm. Information is only beneficial if it is correct and complete (Floridi, 2013). Integrating key components of Total Quality Management (TQM) into InfoSec, organizations can protect the availability, confidentiality, and integrity of information by securing people, processes, and technology on a social and organizational level.

Information Security used to be easy, important documents were simply put in a safe or contained in a locked room. *Information Security Principles* (2008) explains that InfoSec encompasses the confidentiality, integrity, and availability of information. Controls are put in place to ensure these qualities are maintained and data remains viable. While the relationship between technology and business functionality expands, information security has equally expanded to safeguard its essential information. Additionally, many organizations are multinational and require the ability to send sensitive information quickly and securely. Organizations attempt to identify the most effective way to counteract threats to security but managing security risks has become less about quality and more about quantity (Stoneburner, Goguen, & Feringa, 2002). In response to the growing need for InfoSec, technological innovation has helped to establish a safe environment. Unfortunately, advances in technology cannot correct all information security issues. InfoSec should be controlled and maintained using a comprehensive approach to securing people, processes and technology on a social and organizational level. TQM and InfoSec implementation together can facilitate a cohesive holistic path to security and customer satisfaction.

The International Standardization Organization (ISO) helps to ensure that a product manufactured anywhere in the world has a basic system for quality management compliance. Today, some of the more widely used standards such as the ISO9000 and the ISO27000 series, help define the management and manufacturing process by which products are made (Gillies, 2011). TQM is the predominant organizational strategy to implement quality. Prior to the introduction of TQM, quality systems involved simply individual audits and inspections. The ISO considers TQM as a management approach centered on quality with the goal of long-term success and directed by customer satisfaction. Security, as an element of quality, must be addressed throughout an organization in the development, implementation, and monitoring of strategy and policy. TQM involves everyone in all aspects of an organization. It asserts a shift in organizational culture and requires teamwork and cooperation by all departments. TQM is created by top-level management and is cascaded to all levels. This total involvement recognizes that every activity enhances or detracts from quality. Management's role in TQM is to create a quality strategy, aligning InfoSec with the organization business objectives, and to deploy this strategy to all organizational levels (Martinez-Lorente, Dewhurst, & Dale, 1998).

Emerging technology is an unyielding stream of growth and development. It is critical that policy leaders understand which technologies will affect the information controlled by an organization and respond appropriately (Stoneburner, Goguen, & Feringa, 2002). Additionally, hackers are a constant threat to information security as they can directly affect information integrity. A fundamental belief of TQM is the best way to product improvement is to constantly improve product creation. TQM aligns well with technological advances, and with defending against new methods of invasion from hackers, in this belief. According to Facebook creator, Mark Zuckerberg, "The Hacker Way is an approach to building that involves continuous improvement and iteration. Hackers believe that something can always be better and that nothing is ever complete" (Rosoff, 2012, para. 7). By incorporating continuous improvement into the InfoSec processes an organization can better protect itself as technologies grow and change. Developing a continuous process improvement policy (CPI) framework within the InfoSec department will allow managers to direct employees on how best to protect the confidentiality, integrity, and availability of information.

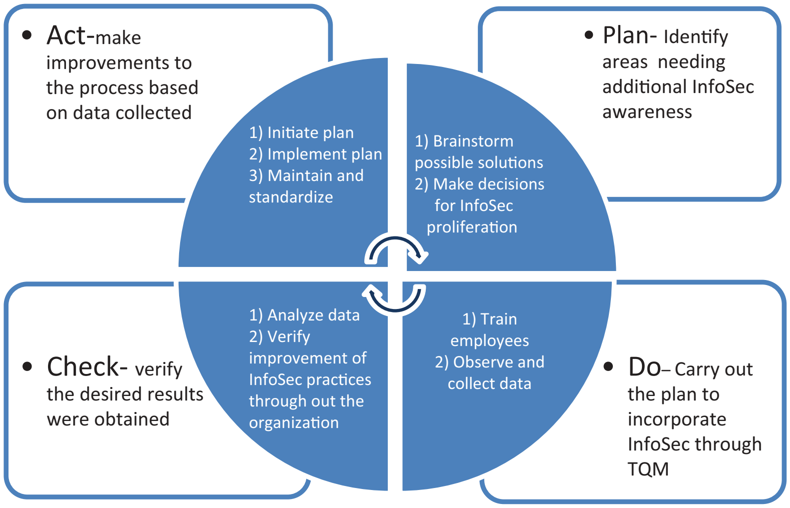
November 30, 2013 is a day that will not soon be forgotten for Target executives, employees, and customers. While shoppers rushed to the company's 1,797 U.S. stores seeking the best Black Friday deals, hackers were lying in wait. Malware, designed to steal credit card information at the completion of the customer's transaction, was installed and executed on Target's payment processing system. The malware successfully accessed 40 million credit card numbers and 70 million addresses and phone numbers while Target stood by and watched an entirely preventable attack take place. As quoted from the Bloomberg Businessweek article "Missed Alarms and 40 million Stolen Credit Card Numbers: How Target Blew It" (Riley et al., 2014) Target Chairman, President, and Chief Executive Officer Gregg Steinhafel issued an e-mailed statement: "Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach. As a result, we are conducting an end-to-end review of our people, processes and technology to understand our opportunities to improve data security and are committed to learning from this experience." Due to a lack of appropriate InfoSec procedure following an alert, Target suffered dramatically. Target has spent upward of $61 million in response to the breach and will incur additional costs in litigating more than 90 lawsuits filed by Target customers for negligence and compensatory damages. A well-defined and proliferated policy concerning procedure taken in the event of an alert could have prevented Target's breach and saved the company's money and reputation.

The TQM process is not about creating absolute definitive change but constantly changing the approach with which operational effectiveness and customer satisfaction are accomplished. An organization should form a sense of responsibility, ownership, and commitment by involving employees in proactive process improvement. There are predominantly three techniques in TQM development: reengineering, benchmarking, and empowerment. Incorporating InfoSec controls during the TQM initiation will create a cost-effective culture change with an emphasis on information security (Badiger & Laxman, 2013).

The reengineering phase of TQM is possibly the most labor intensive. Reengineering involves discontinuing existing procedures and essentially rethinking and developing a new process. A fundamental redesign can uncover areas of waste and realize areas where InfoSec practices can be proliferated. Change agents such as Kaizen events, Gemba walks, and value stream mapping should be used in the initiation of the reengineering phase as they can give a clear representation of workflow. A popular tool used in TQM for continuous process improvement is the Plan-Do-Check-Act cycle (n.d.). The PDCA cycle teaches an organization that it should plan an action, do it, check to see how it complies and act on what has been learned. Utilization of the PDCA cycle complements the constant evolution of technology as the cycle is a continuous loop. New technology or new threats would be discussed during the Act phase and the remaining steps function in filtering this new information throughout the organization and taking action where needed. Figure 1 shows how InfoSec proliferation fits into the PDCA cycle.

Brainstorming sessions including members of both the Quality and InfoSec departments allow for free-flowing ideas and suggestions with the ultimate goal of continuous improvement and

**Figure 1** ***Integrating InfoSec with PDCA.***


Act-make improvements to the process based on data collected
1) Initiate plan
2) Implement plan
3) Maintain and standardize
Plan- Identify areas needing additional InfoSec awareness
1) Brainstorm possible solutions
2) Make decisions for InfoSec proliferation
Check- verify the desired results were obtained
1) Analyze data
2) Verify improvement of InfoSec practices through out the organization
1) Train employees
2) Observe and collect data
Do- Carry out the plan to incorporate InfoSec through TQM

customer satisfaction. Incorporating InfoSec policy and procedures during the reengineering phase is a cost effective way to add organizational assurance measures as management can clearly identify when and where such measures are necessary. Organizational InfoSec policy implementation is a priority to all staff members, not just a specific department. InfoSec policy should be fully supported by a range of documents covering expected InfoSec standards, protocol for how to do things correctly and appropriate procedures for protecting and assuring data integrity. System and compliance audits should be conducted to reveal any fluctuations in security incidents impacting the organization. Optimally, the reengineering phase will begin the culture change needed to fully integrate InfoSec through TQM; however, it is necessary to constantly reassess its relevance as technology changes and advances are made. Continuous improvement is vital to maintain a holistic approach to securing the information, people, and processes within an organization (Badiger & Laxman, 2013).

The incorporation of metrics during the reengineering phase is recommended to support and sustain InfoSec integration through TQM unfortunately InfoSec metrics are difficult to define. Metrics can be used to quantify data in order to assess the state of security at a given organization by collecting data from appropriate data points. For a given field to be considered a "metric" it must be SMART; specific, measurable, attainable, and time dependent. Creating metrics based on IT/InfoSec goals and objectives can produce an acceptable baseline from which an organization can chart continuous improvement. Development of best practices in InfoSec metrics is still in its infancy and is beyond the scope of this article; however, when applied appropriately metrics should define, measure and analyze InfoSec data to ensure the consistent and proactive improvement of InfoSec practices (Payne, 2006).

The benchmarking phase involves "measuring your performance against the best in class companies, determining how they achieve those performance levels and using the information as a basis for your own company's targets, strategies and implementation" (as cited in Badiger & Laxman, 2013, p. 36). A "best" practice should evolve as advances are discovered and continuous improvement should be made. Benchmarking is the mechanism to achieve best practices as set by other organizations. nCircle (2012) is a company focused on assessing information risk and security performance management solutions and can help acquire fact-based data necessary to support the decisions of upper-level management. The Information Security Forum (ISF) is a global nonprofit association of organizations dedicated to investigating, analyzing and settling key issues in InfoSec. The ISF also aids businesses in developing best practice methodologies, processes and solutions. Groups such as nCircle and ISF can help an organization assess their InfoSec processes, compare them to industry leaders and provide them with the best solutions for the protection of customer information (Badiger & Laxman, 2013).

Until recently, information security was considered a responsibility of the information technology (IT) department. Discussion of information security rarely happened outside IT and this compartmentalization left a gaping hole in any organization's defense as it did not address the most common and effective way to create a breach in digital security: social engineering. The only way to prevent social engineering as an agent of security breach is to involve its potential victims in prevention ("The Risk of Social Engineering on Information Security: A Survey of IT Professionals," 2011). The empowerment phase of TQM initiation involves management delegating responsibilities to lower level staff and is the best time to express what InfoSec actions they can take to ensure information integrity and compliance. Empowering an educated employee to make independent decisions in line with the company's mission can create a strong culture of ownership and accountability. Benefits to involving employees in aligning InfoSec with an organization's quality movement include improved productivity and cost reduction, confidence in information quality (data integrity), decreased incidence of data and software security breaches, and increased participation and job satisfaction (Badiger & Laxman, 2013).

The U.S. National Institute of Standards and Technology (NIST) lists three categories of InfoSec controls: technical, operational, and management. Technical controls include products and processes that focus on protecting information and communication technology. Operational controls consist of application mechanisms and strategy for correcting operational issues that a threat could exploit. Management controls includes policy creation, continuity planning, and employee training to target InfoSec's nontechnical areas. While it makes sense that InfoSec programs focus the majority of their energy on technical and operational controls, it may be more beneficial to implement management controls to attain a company-wide understanding of the importance of InfoSec (Stoneburner, Goguen, & Feringa, 2002).

In "Is Information Security Under Control?" Wade H. Baker, PhD, and associate professor Linda Wallace introduce a study to understand how organizations use controls to regulate information security risks. Several security experts aided in the selection of 80 security controls in sixteen general security domains. These controls represented a balanced InfoSec program and included many international standard controls. The study was an anonymous Web-based survey involving 349 security practitioners; 34 percent had less than 100 computer systems, 38 percent had between 101 and 1,000, and 28 percent had more than 1,000 computers. Participants were asked to rate the quality of their organizations' current implementation of each of the 80 NIST-categorized security control practices on a scale of 0–6; zero meaning no implementation and six meaning comprehensive implementation of the specified security control. Not surprisingly, the study found that antivirus practices topped the list for implementation control with system patching and backups not far behind. On the lower end of quality implementation the study showed the tracking and identification of modem connections, training on how to prevent social engineering attacks, and business continuity procedures (Baker & Wallace, 2007).

The study clearly showed that the NIST categories on the top ten list were predominantly technical and operational controls, while only one management control made the list; however, there are six management controls appearing in the bottom of the list. Baker and Wallace hypothesize that organizations should be incorporating more Quality management controls and empirically assessed the value added by management control implementation. The study shows a statistical comparison between security policies and their respective implementation level for four different security domains in InfoSec. The analysis showed that significantly higher quality ratings for non policy controls were found in organizations with an above average rating in governing policy implementation. This interrelationship suggests a correlation between management controls and strong policies resulting in quality improvement, thereby, playing a pivotal role in organizational security (Baker & Wallace, 2007).

Furthermore, Baker and Wallace tested the relationship between security incidents and quality control. Participants were asked if any of the 10 most common security incidents had affected their organization over the past year. The results determined that organizations with advanced security programs (rating 5–6 for implementation quality) were less likely to report incidents than organizations with poor implementation quality (between 0–2). These results seem to propose that increased quality controls decrease the likelihood of security incidents. It is important to note the security incident types vary and the benefits in higher implementation quality can vary depending on threat combinations and control (Baker & Wallace, 2007).

Unfortunately for many InfoSec programs, security risk has become more about quantity than quality. Confused managers utilize as many controls as possible in an attempt to remedy an attack or defend vulnerability. In "The Economics of Information Security Investment" (2002) Larry Gordon and Marty Loeb express that fully implementing every control available is not an efficient use of funds and an organization should invest in security only to the point that marginal cost and benefit are equal. A commonly used strategy for deriving optimal quality levels in a system is through the use of Armand Feigenbaum's four costs of quality. Feigenbaum, (1983) defines prevention costs, appraisal costs, internal failure costs, and external failure costs as the quality-based areas that management and quality practitioners can evaluate to uncover cost improvement and profit enhancement. The steps taken to control risk within an organization should find a balance between cost of the measures employed and business impact if risks occur. The cost of this shift in culture should not outweigh the benefits.

High quality Information Security is mandatory whenever information is secured electronically to ensure its availability, confidentiality, and integrity. Large organizations have an obligation to protect customers' information or risk financial loss. TQM should be used to reengineer InfoSec's current organizational presence, benchmark practices, and empower employees. Further research in the integration of metrics during the TQM reengineering phase is needed to harness the full potential of InfoSec data within an organization. Deploying InfoSec TQM is not an easy task but can improve the productivity of its information staff, reduce security threats to the organization, and improve customer satisfaction. Integrating InfoSec policies and best practice procedures through TQM will create a culture of informed and empowered employees holding information security as a top priority.

## References

Badiger, S., & Laxman, R. (2013). Total quality management and organisational development. *International Journal of Business and Management Invention*, *2*, 34–37.

Baker, W., & Wallace, L. (2007). Is information security under control? *Security and Privacy, IEEE*, *5*, 36–44.

Feigenbaum, A. V. (1983). *Total quality control*. New York, NY: McGraw-Hill.

Floridi, L. (2013). Information quality. *Philosophy and Technology, 26*, 1–6. Retrieved, from http://link.springer.com.jproxy.lib.ecu.edu/article/10.1007%2Fs13347-013-0101-3#

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM Journal*, *23*(4), 367–376. doi:http://dx.doi.org/10.1108/17542731111139455

Gordon, L., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4),438–457.

Information security principles. (2008). Swindon: BCS Learning & Development Limited.Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/189252270?accountid=10639

Martínez-Lorente, A., Dewhurst, F., & Dale, B. (1998). Total quality management: Origins and evolution of the term. *The TQM Magazine*, 10(5),378–386. doi:10.1108/09544789810231261

nCircle presents "security benchmarking" webinar. (2012). *Entertainment Close-Up*. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1038553433?accountid=10639

Payne, S. C. (2006). *A guide to security metrics*. Bethesda, MD: Sans Institute. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

Plan-Do-Check-Act (PDCA): Implementing new ideas in a controlled way. (n.d.). *Plan-Do-Check-Act (PDCA)*. Retrieved from http://www.mindtools.com/pages/article/newPPM_89.htm

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014, March 13). Missed alarms and 40 million stolen credit card numbers: How Target blew it. Retrieved from http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Rosoff, M. (2012, February 1). Mark Zuckerberg's letter to Facebook investors. *Business Insider*. Retrieved from http://www.businessinsider.com/mark-zuckerberg-explains-the-hacker-way-to-facebook-investors-2012-2

Stoneburner, G., Goguen, A. & Feringa, A. (2002). *Risk management guide for information technology systems*. National Institute of Standards and Technology Special Publication. Retrieved from http://webharvest.gov/peth04/20041027044131/http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

The Risk of Social Engineering on Information Security: A Survey of IT Professionals. (2011, January 1). Retrieved from http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf

*Sarah Schiltz is currently a graduate student in the Technology Systems Department at East Carolina University and received her B.S. in Biology from UNC—Wilmington. She has multiple years experience working in Quality and functions as the Quality Assurance Coordinator for a local non-profit organization. She can be reached atyuhass04@students.ecu.edu*