AN ICT SECURITY MANAGEMENT FRAMEWORK

Aristeidis Chatzipoulidis and Ioannis Mavridis
Department of Applied Informatics, University of Macedonia, Egnatia 156, Thessaloniki, Greece

Keywords: Risk management, ICT security, Information system controls.

Abstract: Recently, organizations started to realize that managing information security is more than a software solution; it is a strategic discipline. This realization has emerged a major challenge in the business and technology field, the integration of all governance, risk, and compliance (GRC) activities to operate in synergy and balance in configuration with the business and security objectives. The goal of this paper is to develop a comprehensive ICT security management framework as a unified platform against the evolving GRC complexity. Considering the endemic nature of risk, the risk approach requires periodical rethinking in order to keep pace with security changes and prevent undesirable incidents while preserving the stakeholders' interests continuously. Such an approach depends on the risk management maturity level, and the portfolio of monitoring controls.

1 INTRODUCTION

In a time of intense pressure on budgets and investments, enterprises of all types and sizes are struggling to contain legal expenses, reduce costs, strengthen decision-making processes and improve business performance. Many have found that a strong governance, risk and compliance (GRC) discipline will enable them to integrate inefficient, outdated and isolated programs, processes and systems into effective and efficient, enterprise-wide, risk-based internal control structures (Adler, 2006). This paper aims to justify that consistency towards information computer technology (ICT) security objectives is not mere repetition of duties and procedures but rather a re-evaluation of the initially planned security goals. Hence, the development of an ICT security management framework can help enterprises maintain security continuity and adapt smoothly to emerging trends, new behaviours and ongoing GRC changes.

Information security (Johnson and Goetz, 2007) can be described as the securing of information identified as confidential by computer-based and human-based procedures. The need to assure that information security is fulfilled developed a range of ICT systems as technical tools for operational activities. When security vulnerabilities were first exploited, the initial focus was to embrace the appropriate ICT controls to protect related corporate assets. But after several high profile breaches, government agencies around the world were forced to create a form of standardization producing series of often vague regulations (Meints, 2009) such as the Sarbanes-Oxley Act and the European Union Data Privacy. Also, security standards and policies such as the International Organization for Standardization (ISO) 27000 series, the Information Technology Infrastructure Library (ITIL), and the Common Criteria emerged in an attempt to standardize operational activities and regulate the business environment.

Over time, organizations have been able to build and strengthen internal control activities by utilizing automated controls. Automated controls are considered the most effective types of managing procedures since they can be programmed to offer reliable and repeated results (Agrawal et al, 2008). However, human involvement makes almost impossible to automate all business and security operations. Thus, reaching the proper balance in control activities can reduce transaction costs and errors, strengthen the environment of prevention, embed compliance into the core processes and enhance quality of the monitoring activities.

2 CONTROLS OPTIMIZATION

Identifying and improving process effectiveness caused the need for ICT security frameworks and

Chatzipoulidis A. and Mavridis I. (2010).
AN ICT SECURITY MANAGEMENT FRAMEWORK.
In *Proceedings of the International Conference on Security and Cryptography*, pages 459-462
DOI: 10.5220/0002989304590462

controls aiming to secure an incorruptible flow of information and transactions within and across organizations. Such span a wide variety of international security policies and activities that typically involve people executing processes with technological support. In fact, the majority of enterprises started to realize challenges in managing the regulatory aspects due to inefficient controls and overhead costs. Challenges (Hubbard, 2009) mainly derive from errors and loss of productivity manifesting from manual processes in terms of delays, revenue lost, incorrect duties, financial fines, and corporate offences.

In an attempt to maximize compliance efforts and reduce security spending, Protiviti (2006), an independent risk consulting firm, recommends that organizations should achieve the proper balance in control mechanisms namely between manual and automated controls as well as between preventive and detective controls. This control optimization has its drivers. Drivers for change are considered the increase in stakeholders' expectations, the decrease in costs and complexity and the need to maintain performance through significant change. Yet, establishing effective and efficient controls with a positive return on investment (ROI) is dependent on developments in the wider risk management approach (Peltier, 2008).

Driving business value through controls monitoring is about understanding governance, risk and compliance at a maturity level. Such a desired level depends on the capacity to manage embedded monitoring activities such as financial, operational and regulatory processes as means of improving the decision-making process. The effort and time required to implement a sophisticated control monitoring solution differs from the maturity level of the compliance program, the ratio of manual to automated controls and the heterogeneous environment under which firms operate (Kumbakara, 2008).

Improving the effectiveness of monitoring and control systems is determined by training efforts to demonstrate that the monitoring process (Bordogna and Baxter, 2009) is not a stand-alone program that requires resources from existing business and security activities but a sustainable process for monitoring the current and evolving risk issues. Research has uncovered (Drew, 2007) that process controls and ICT security management frameworks remain critical functions to avoid serious incidents. Such a set of security concepts and practices, such as the ITIL and ISO/IEC 27000 series, address the constantly changing ICT infrastructure and data-center configurations from the standpoint of services delivered to end users.

For optimum usefulness, such practices should progress from inconsistently applied efforts throughout the enterprise to become culture-centric and framework-integrated. This enhanced state of visibility and transparency implies a change in the mindset of employees and broader public. According to a benchmarking annual research (KPMG, 2009) leading companies expect less of an impact to their control environment and are planning to keep the number of controls in 2010 consistent with 2009 totals or even higher.

In reality, manual controls will always exist. However, since the probability of human failure is great and the cost of human monitoring high, organizations should define a realistic ratio of automated controls to manual. A reasonable goal is to achieve a 75 percent of the controls portfolio with preventive automated controls (Jose, 2005) whereas this depends on business, industry and strategic planning. Getting the balance wrong can lead to excessive controls impacting the bottom line or ineffective safeguards leaving an organization exposed to risks. Planning strategically can provide integration of the business process controls (compliance policies, system controls, audit tests), application and security controls (segregation of duties, authentication and authorization controls) and infrastructure controls (database security, encryption) into a single and comprehensive controls monitoring solution. Ideally, this solution should be tailored to fit an organization's unique culture and risk appetite.

3 ACHIEVING A UNIFIED VIEW TOWARDS RISK

The greatest challenge in constructing a unified and holistic approach to ICT risk is not just the gathering of similar information within an organization but instead the failure to correlate successfully different information outside the scope of business operations. In response to the changing risk environment that defines modern business operations, new risk approaches to information security infrastructure have to be developed. Previous security management models (Soo Hoo, 2000) have focused on demonstrating in a structured way the factors affecting compliance and risk procedures by allocating responsibilities according to duties. However, many of them have failed to fulfil the expectations of ongoing compliance pressures and evolving challenges. The reasons for failing can be

found at the static development of the security framework, the lack of feedback communication between organizational departments and most important, the missing aspect of an evolving risk management approach capable to support the GRC initiatives. Hence, the goal of a unified approach to ICT security management is not just to fulfil security requirements but to offer continuous testing with ongoing security principles, becoming a highly integrated business process.

The proposed framework can be used as a starting point for security-conscious business departments who opt for a holistic and unified ICT security management approach. Additionally, it can improve any existing information security formation already in practice. The cornerstone of this framework is the recognition that human involvement complicates the status of a security system due to the changing behaviour patterns. Thus, building a dynamic and scalable platform towards ICT security management starts with acquiring and retaining a highly professional workforce. In case, a well-trained, highly-qualified personnel with professional codes of conduct and moral ethics can ensure that monitoring and performing security procedures is a culture-centric state of conducting business. Human responsibility towards monitoring and enforcing security countermeasures depends on team effectiveness within and outside an organization (King, 2009). Key issues involved in building stuff competency is to identify and match duties to specific roles, nurture a security-conscious culture and make human resource management a fully integrated strategic process.

Ensuring that the workforce is adequately competent to confront with emerging security risks, the effort should be focused on standardising processes using automated controls to minimize overhead costs and offer consistent results. Thus, achieving the proper balance between automated and manual controls is the next step required in the proposed ICT security management framework. The acquisition and implementation of existing security management models, such as the ISO 27000 series, CobiT and ITIL, require a balance between automated controls and human monitoring, which indeed can lead to best implementation of security practices and create a weighting scale of security measurement (Pink Elephant, 2008).

In the next level, organizations should conduct internal audits to ensure that the risk management process is up to the task, evaluate the reporting of key risks, reviewing the management of risks and assuring that employees are following the restrictions defined in the ICT usage policy. Specifically, an internal audit (Stanford University, 2009) is the process of collecting and evaluating evidence of an organization's information systems, practices and operations. Obtained evidence evaluation through the risk management program can ensure whether ICT systems and humans can safeguard assets, maintain data integrity, confidentiality, availability and operate effectively and efficiently to achieve the organizational objectives.

The fourth stage refers to the selection, adaption and implementation of ICT security practices and standards into the core of the organisation. In this stage, administrators deal with challenges such as standards complexity, implementation costs, compatibility issues and the need to infuse the risk appetite throughout the organizational culture. In the final phase, external audit is necessary to conduct controls in order to validate security performance and provide a form of certification under which internal controls operate. Effective internal and external audit programs (Basel Committee, 2008) are a critical defence against fraud and provide vital information to the board of directors about the effectiveness of internal control systems. Risk communication and continuous feedback will flow results to employees and managers supporting the entire GRC management effort. The diagram below (figure 1) shows the proposed unified ICT security management framework.

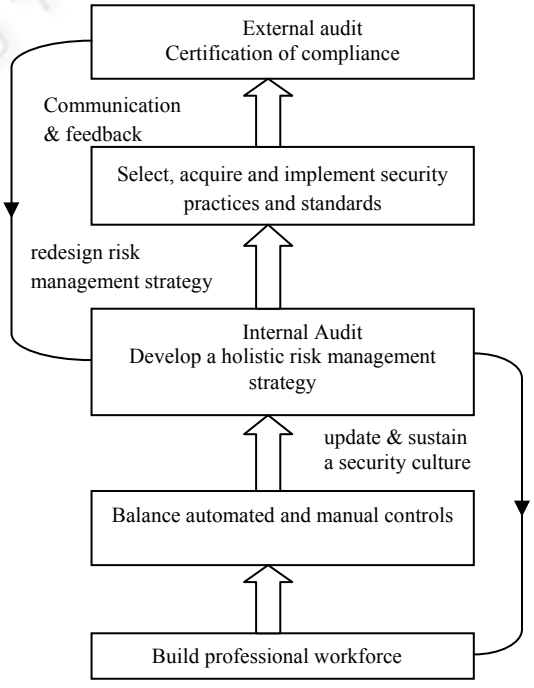

Figure 1: ICT Security Management Framework.

4 CONCLUSIONS

Since achieving a perfect security system is practically infeasible, firms are using risk management techniques and IT security practices in an attempt to mitigate risk in reasonable levels. The proposed ICT risk management framework may serve as a unified approach towards managing the ongoing GRC complexity. Yet, such an approach should be tailored to fit the unique environment of the organization and risk limits, becoming the linking component between employees and external groups. In addition to failures, the security value can be maximized only when it is deployed and communicated both as an opportunity and misfortune via the security awareness programs. To conclude, management of human involvement is still regarded as the most variable information asset, thus raising awareness decreases the probability of future risk. Eventually, in the name of research, traditional risk management will be compelled to abandon narrow-lined security frameworks and assume place in the front line of maintaining performance in turbulent times while becoming subject to change upon request.

REFERENCES

Adler, M. P., 2006. A Unified Approach to Information Security Compliance, *EDUCAUSE Review*, Vol. 41, No. 5, September/October 2006, pp. 46–61

Drew, M., 2007, Information risk management and compliance, expect the unexpected, *BT Technology Journal*, Vol. 25, Issue 1, pp. 19-29

Hubbard, D., 2009. *The Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley & Sons, pp. 42-49.

Johnson, M. E., Goetz, E., 2007. *Embedding Information Security into the Organization*, IEEE Computer Society, [Online], http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=4218547&isnumber=4218538

José, A., 2005. Security Metrics and Measurements for IT", *The European Journal for the Informatics Professional*, Vol. VI, No. 4, August 2005.

King, S., 2008. *Reducing the cost of information security*, July,[Online],<http://www.computerweekly.com/blogs/stuart_king/2008/07/reducing-security-costs.html>

KPMG, 2009. Maintaining Your Control Environment in Turbulent Times, *Fifth Annual Benchmark Study*, [Online],http://www.404institute.com/docs/2009BenchmarkStudy.pdf

Kumbakara, N., 2008. Managed IT services: the role of IT standards, *Journal of Information Management & Computer Security*, Vol. 16, No 4, pp.336-359 Meints, M., 2009. *The Relationship between Data Protection Legislation and Information Security Related Standards*, Springer Publications, Vol. 298, pp. 254-267, [Online], <http://www.springerlink.com/content/137q4x111r355371/>

Peltier, T. R., 2008. *How to complete a risk assessment in 5 days or less*, AUERBACH Publications, pp. 137-174.

Pink Elephant, 2008. *IT service management tools: compatibility considerations*, [Online], <https://www.pinkelephant.com/NR/rdonlyres/3C2328634423430EB5C68358A2D217B9/4340/PinkVERIFYServiceWhitepaperV333.pdf>

Protiviti Corporation, 2006. *Automated and preventive controls can decrease compliance costs*, [Online], <http://www.knowledgeleader.com/KnowledgeLeader/content.nsf/Web+Content/WPA_ControlsComplianceandtheRoleofContinuousMonitoring!OpenDocument>

Soo Hoo K., J., 2000. *How Much Is Enough? A Risk-Management Approach to Computer Security*, Working paper, [Online], <http://iis-db.stanford.edu/pubs/11900/soohoo.pdf>

Stanford University, 2009. *Stanford IT Audit and Information Security Standards*, [Online], <http://www.stanford.edu/dept/InternalAudit/infosec/>