MANAGING SECURITY AND COMPLIANCE RISKS OF OUTSOURCED IT PROJECTS

Moneef Almutairi and Stephen Riddle

School of Computing Science, Newcastle University,
Newcastle Upon Tyne, UK

ABSTRACT

Several constraints, such as business, financial, and legal can lead organizations to outsource some of their IT services. Consequently, this might introduce different security risks to major security services such as confidentiality, integrity and availability. Analysing and managing the potential security risks in the early stages of project execution allows organizations to avoid or minimize such security risks. In this paper, we propose an approach that is capable of managing the security and compliance risks of outsourced IT projects. Such an approach aims to allow organizations to minimize, mitigate, or eliminate security risks in the early stages of project execution. It is designed to manage variation in security requirements, as well as provide a methodology to guide organizations for the purpose of security management and implementation.

KEYWORDS

Security and compliance management, outsourced IT projects, security management approach.

1. INTRODUCTION

As a result of globalization and heightened competition, many organizations today are confronted with significant challenges in developing services that satisfy customer requirements, and these needs must be met on time despite limited resources [1]. With the emergence of cloud computing and advances in web technology, such challenges and customer demands continue to expand. In response, many organizations have considered outsourcing to deliver and improve their IT services. Over the last two decades, Information Systems (IS) outsourcing has grown rapidly. This growth has prompted academia and industry to investigate the benefits that organizations may gain from outsourcing, and to determine the reduction in risk that might be achieved when adopting such a choice [2],[3].

Information Systems outsourcing has been defined in [2],[1],[4] as:

a business practice in which an organization subcontracts with a preferred third party to develop, operate, manage, or maintain its information system functions partially or totally for a specific period of time.

Outsourcing is an attractive option for organizations, offering benefits including cost reduction and the opportunity to concentrate on core business activities [5], [6], [7]. However, it is an option which must be managed properly as it brings risk, such as to security, contract violations,

Brajesh Kumar Kaushik et al. (Eds) : CCNET, CSIP, SCOM, DBDM - 2017
pp. 33– 42, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.70504

and the loss of technology skills for the organization [6],[8],[9]. Failure to manage these risks could lead to major issues not only in a particular project, but also for the entire organization or business [10].

The rest of this paper is structured as follows: section 2 gives information about the background and related work. In section 3, we present our framework. Section 4 is used to give an example. In section 5, we conclude this paper.

2. Background and Related Work

Securing information systems should follow a systematic approach which does not necessarily rely only on technical aspects, but also takes into account other aspects such as people and environment [11],[12],[13]. Such a systematic approach can help organizations achieve business continuity and minimize security risks [14],[15]. The most common systematic approaches are Information Security Management System (ISMS) standards and frameworks such as the ISO/IEC 2700x family [16], OCTAVE [17], and COBIT [18]. These standards and frameworks represent general security best practice guidance of IT processes and procedures, and can be adopted by organizations to achieve information systems confidentiality, integrity, and availability, and reduce associated security risks [16],[19],[20]. Ensuring compliance with ISMS standards and frameworks is an essential part of information systems security, as unenforced ISMS will not achieve the expected value of such practices [21]. The status of the compliance with the ISMS standards and frameworks is normally achieved via audit or self-assessment. However, although audits can provide good outcomes, they suffer from a lack of broad assessment, and are time consuming. Moreover, while self-assessment can provide broader assessment, it may also suffer from a lack of depth assessment [22],[23].

Although many organizations have adopted ISMS standards and frameworks to secure their information systems, these represent general best practice of ISMS and do not consider that security requirements differ from one organization to another [24]. Moreover, there is no adequate guidance for implementing or complying with such standards and frameworks, and nor are they designed to manage the security and compliance risks of outsourced IT project [25]. Updating these standards and frameworks to fit the outsourced IT project context might make them more complicated and increase time and resource consumption. Instead, our proposal is designed to overcome these weaknesses.

When outsourcing IT services, two main parties are involved: a client and a provider. Security requirements need to be documented in project documents such as the project contract and Service Level Agreement (SLA). The provider has to comply with these security requirements to deliver these IT services to the client correctly.

IT organizations today deal with diverse security risks such as terrorist attacks and natural disasters [14]. Such security risks force organizations to take action to minimize, mitigate, or eliminate issues as early as possible before they are exploited by attackers or their systems are damaged. To manage the security and compliance risks of outsourced IT project effectively, specific requirements need to be met:

- Security requirements management: the security program or framework should be comprehensive and systematic as well as establishing a complete methodology that is capable of adequately managing the security of outsourced IT projects. This includes security policies, access controls, plans, and procedures.

- Risk Management: Security risks are not only technical, and so the security program should manage risks from different perspectives such as technical, human, and environmental and physical risks.
- Compliance management: The security program should establish a method to enforce compliance properly.
- Usability: The security program should be usable from different perspectives such as cost effectiveness, time efficiency, and simplicity.

3. MANAGING SECURITY AND COMPLIANCE RISKS OF OUTSOURCED IT PROJECTS

We propose a framework for managing the security and compliance risks of outsourced IT projects. The framework utilizes project phases (initiating, execution, monitoring and controlling, and closing) and the Plan-Do-Check-Act (PDCA) model [26], as shown in Fig 1. Each project phase has its own security activities. During the planning, execution, and monitoring and controlling phases, the PDCA model is applied. Managing project security should be aligned with the project phases in consideration of improvements during the project execution. This improves flexibility, simplicity, and ease of use, regardless of the project size, cost, or any other constraints. The framework uses a hybrid threat modelling approach that is designed for the outsourcing context, in which environments are less stable and more systems are integrated. The threat modelling approach in such environments needs to achieve some desired properties. It should be exclusive, exhaustive, unambiguous, repeatable, comprehensive and useful to capture the largest possibility of potential security threats [27], [28], [29]. The hybrid threat modelling is designed to overcome the limitations of existing threat modelling approaches that use only two or three criteria, and the lack of consideration of the desired properties [30],[31]. It combines different threat modelling criteria and considers threats from different perspectives such as external threats, provider threats, client threats, and physical and environmental threats. It is designed to be capable of capturing the largest possibilities of potential security threats that might occur during the project execution.

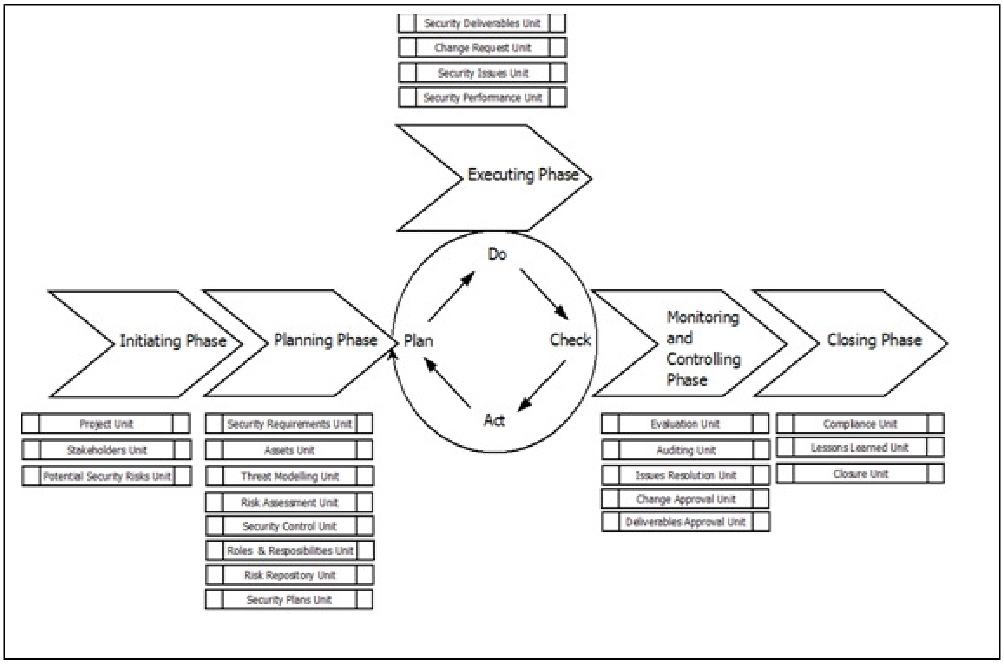

Figure 1 : Security and compliance risks management framework

3.1. Initiating Phase

The aim of this phase is to establish the project's unique details, and identify major project stakeholders and general security risks to which the project might be exposed. The client is responsible for this phase, as no provider has yet been selected. This phase achieves its objectives through the following units:

- Project unit: designed to handle (create, update) essential project data such as project Id, name, code…etc.
- Stakeholders unit: the aim of this unit is to identify all project stakeholders and their roles and responsibilities in the project.
- Potential security risks unit: the aim of this unit is to identify potential security risks that might take place while executing the project. This allows decision makers to take the right decision whether to outsource or not.

3.2. Planning Phase

The planning phase is the core part of this framework. It corresponds to the Plan stage of the PDCA model. The main parties involved in the project execution carry out all core security activities at this phase. The primary parties are the client and the provider. If other stakeholders are involved in executing security activities, then they participate with the primary parties in preparing the required security analysis and plans. The planning phase aims are achieved in units as follows:

- Security requirements unit: the project security requirements are documented and signed off by the client and the provider through this unit.
- Assets unit: all project assets are identified and categorized (hardware, software, information, or network) through this unit. It answers what should be protected. If the project affects any organization's assets, then they should be identified and categorized as well.
- Threat modelling unit: a hybrid threat modelling approach is designed to be capable of capturing the largest number of potential security threats that might occur during the project execution. In another words, it identifies what to protect from. This threat modelling approach uses six criteria:
    - Threat Source: it represents the origin of the threat, which can be external threats, client threats, provider threats, or environmental and physical threats.
    - Threat agent: the agent that causes the threat. This can be technical, human, or organizational.
    - Asset type: the type of the asset impacted by this threat, such as networks, software, hardware, or information.
    - Threat intention: the type of human behaviour who caused the threat. It can be accidental or intentional.
    - Environmental and physical threat type: the type of environmental and physical threat. It can be controlled or uncontrolled.
    - Threat impact: the result of the threat when it occurs. This can be any breach in confidentiality, integrity, or availability.

- Risk assessment unit: the ultimate aim of this unit is to estimate and prioritize the impact of the potential security risk on project assets. The risk assessment unit has five steps: vulnerabilities identification, risk likelihood determination, risk magnitude determination, risk estimation, and risk prioritization.

- Security controls unit: through this unit, security controls or countermeasures that can mitigate identified security risks are selected. Countermeasures determine how to protect project or organization assets. Countermeasures are categorized in this framework to technical, human, or organizational.

- Roles and responsibilities unit: The aim of this unit is to assign security activities to project teams using a clear method that helps prevent any ambiguities between the project teams, especially if there is another client or stakeholder team involved. In this framework, we propose a role based on the responsible, accountable, consult, and inform method (RACI) for assigning the roles and responsibilities of project security activities.

- Risk repository unit: this unit contains all thus-far identified project security risks. Any risk that has been logged into the risk repository unit should have sufficient information about the risk such as risk Id, description, impact, asset name, and so on.

- Security plans unit: This unit is responsible for developing security plans that will be used to achieve project security goals and contribute to building a secure and protected environment such as an incident management plan, business continuity management plan, and so on.

3.3. Executing phase

In the previous phase, the project teams engaged in planning security activities and controls that mitigate and minimize potential security risks associated with the project. In this phase, which represents the Do stage of the PDCA model, the security plans and controls proposed in the previous phase are implemented. Any security issues that might be experienced at this phase are documented and monitored. If there is any need for improvements or changes, the project team will record them. This phase has four units:

- Performance unit: prepare and submit security performance reports. These reports are reviewed and signed off by the project steering committee in the next phase.

- Security issues unit: record any security issues that might be experienced during the project execution.

- Change requests unit: if there is any need to change any security plan or control, the change is raised through this unit.

- Security deliverables unit: ensure that security deliverables are submitted on time to avoid any delay, which might lead to penalties.

3.4. Monitoring and controlling phase

The project execution needs to be monitored and controlled not only by the project manager, but also by the project steering committee to ensure that it meets its requirements and provide all the support that contributes to the achievement of the security and non-security goals while executing the project. The aim of this phase, which represents the Check and Act stages of the PDCA model, is to review the execution performance reports, and assess if there is any need for improvement. Moreover, the project steering committee supports the project manager in resolving security issues that require intervention. Security change requests and security deliverables are reviewed and approved during this phase too. The monitoring and controlling phase has five units:

- Evaluation unit: the security performance reports are reviewed and assessed. Based on this review, the project steering committee may propose improvements that help achieve project security goals in an effective and efficient way. If the performance is good and there is no need for any improvement, then the steering committee signs off existing performance reports.

- Auditing unit: this unit is designed to enforce compliance with the security requirements to reduce any security violations. Security countermeasures and plans are audited to assess their conformance to what have been planned and agreed.

- Issues resolution unit: security issues that might be experienced during the project execution are resolved. Security issues resolution might be beyond the ability of the project manager, and therefore intervention by the project steering committee might help in their resolution.

- Change approval unit: the project steering committee analyses security changes and assesses their potential impact on different aspects such as the project budget and schedule. If these changes can be tolerated by both parties, then they approve them.

- Deliverables approval unit: the security deliverables that have been achieved so far are reviewed and approved, or rejected.

3.5. Closing Phase

When the project is completed, it will be handed over to the client. Before control is taken by the client, the project requirements including security requirements need to be verified to ensure that the project has achieved its security and non-security goals. The aim of this phase is to audit and verify the project requirements to close the project officially and issue the provider with a closure certificate. Moreover, the lessons learned during the project phases are documented at this phase for future use. The closing phase has three units:

- Compliance unit: demonstrate that the applications or the products being delivered by the project are secure and work according to the requirements agreed in the project scope of the work.

- Lessons learned unit: document all security lessons learned for future use.

- Closure unit: issue the provider with the project closure certificate and officially close the project.

4. EXAMPLE SCENARIO

Let us assume that a government agent, who runs major IT systems for a government, has contracted with a provider to develop e-services using their existing systems. After completing the project, the agent discovers that the confidentiality of their watch list data has been breached by the provider staff while they were integrating the e-services with the watch list systems, and by external attackers when an attack on e-services took place. Although this example is very simple, it illustrates some of the security issues that might arise when outsourcing in the absence of a comprehensive and systematic approach to the management of security risks. Breaches of confidentiality can be avoided or mitigated by using the proposed framework as follows:

- In this scenario, the agent identifies confidentiality breaches of private data by the provider staff or attackers, as these e-services are provided over the internet. In the absence of this step, the agent may enter a contract without knowing the risk level involved. This step allows decision makers to take the right decision in advance concerning whether to outsource, after considering appropriate security countermeasures that mitigate such a security risk, or consider alternatives such as in-house development.

- If the agent has taken the decision to outsource, then there should be a comprehensive and systematic method of effectively identifying and managing potential security risks. The proposed framework provides that method. In our example, the security requirement is to protect the agent's data confidentiality. The asset under impact is the agent data, which is categorized in our framework as information. By using the proposed hybrid thread modelling approach, the asset is exposed in this scenario to some threats, which include external threats by attackers and provider threats such as information disclosure. The risk of exposure to these threats should be estimated and prioritized based on the proposed semi-quantitative approach that the proposed framework provides. This risk may be mitigated by technical countermeasures such as cryptography and firewalls for external threats and organizational countermeasures, such as a non-disclosure agreement for provider threats. Finally, countermeasures implementation is assigned to the correct teams, and the required security plans are developed.

- Having analysed and assessed security risks in addition to planning security countermeasures that help mitigate potential security risks, the project execution starts by following what has been planned. This prevents security changes that might violate the security requirements being made without approval, and help in achieving security activities on time, as they will be part of the project master schedule. In our example, this includes executing technical and organizational countermeasures and security plans.

- To enforce compliance, the proposed framework allows the project steering committee to review, evaluate, and audit security requirements and controls as well as approve or reject security changes while the project team engage in executing the project. This allows the agent and provider to minimize compliance violations as much as possible. In our scenario, this includes auditing the cryptography and security plans implementation.

- At the end of the project execution, the proposed framework provides a way of demonstrating that the project complies with the project security requirements as well as officially closing the project. In our scenario, this includes demonstrating that cryptography and security plans work as claimed.

4. CONCLUSION

In this paper, we propose a framework for the management of security and compliance risks of outsourced IT projects. It is designed to meet all identified requirements and overcome any weaknesses in existing information security system standards and frameworks. Risks associated with all parties involved in project execution are analysed and managed in a systematic way. It is a structured approach, which uses project phases to manage and control project security risks. The framework is flexible as it follows the PDCA model, which allows the project teams involved in managing security risks to monitor and evaluate security controls continuously, and implement any improvements or changes. Simplicity and ease of use are other features of this framework as it utilizes project phases for the management of security risks, which allows the separate management of security risks during each phase. Utilizing project phases makes the framework applicable to any project regardless of size, time, or other constraints. The risks analysis and threat modelling of the current project can be applied to new projects that have similarities, making reusability another feature of this framework. We aim to apply this framework to a real case study in the near future, and also to use a focus group to provide independent validation evidence.

REFERENCES

[1] I. Oshri, J. Kotlarsky, and L. P. Willcocks, The Handbook of Global Outsourcing and Offshoring 3rd Edition: Springer, 2015.

[2] J. Dibbern, T. Goles, R. Hirschheim, and B. Jayatilaka, "Information systems outsourcing: a survey and analysis of the literature," ACM Sigmis Database, vol. 35, pp. 6-102, 2004.

[3] C. Brandas, "Risks and audit objectives for IT outsourcing," Informatica Economica Journal, vol. 14, pp. 113-118, 2010.

[4] Q. Hu, C. Saunders, and M. Gebelt, "Research report: Diffusion of information systems outsourcing: A reevaluation of influence sources," Information Systems Research, vol. 8, pp. 288-301, 1997.

[5] K. Han and S. Mithas, "Information Technology Outsourcing and Non-IT Operating Costs: An Empirical Investigation," MIS Quarterly, vol. 37, pp. 315-331, 2013.

[6] R. Gonzalez, J. Gasco, and J. Llopis, "Information systems outsourcing reasons and risks: an empirical study," International Journal of Human and Social Sciences, vol. 4, pp. 181-192, 2009.

[7] C. Schwarz, "Toward an understanding of the nature and conceptualization of outsourcing success," Information & Management, vol. 51, pp. 152-164, 2014.

[8] R. Gonzalez, J. Gasco, and J. Llopis, "Information systems outsourcing risks: a study of large firms," Industrial management & Data systems, vol. 105, pp. 45-62, 2005.

[9] R. Gonzalez, J. Gasco, and J. Llopis, "Information systems outsourcing reasons and risks: a new assessment," Industrial Management & Data Systems, vol. 110, pp. 284-303, 2010.

[10] J. Iqbal, R. Binti Ahmad, and M. A. Noor, "Frequently occurring risks for IT outsourcing projects," In Proceedings of the International Conference on Computer and Communication Engineering (ICCCE), pp. 957-960, 2012.

[11] J. Holappa and T. Wiander, "Practical Implementation of ISO 17799. Compliant Information Security Management System Using Novel ASD Method,", In Technical Report, 2006.

[12] D. Tse, "Security in modern business: Security assessment model for information security practices," In Proceeding of the Pacific Asia Conference of Information Systems, pp. 1509-1519, 2004.

[13] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Computers & Security, vol. 31, pp. 83-95, 2012.

[14] R. Saint-Germain, "Information security management best practice based on ISO/IEC 17799," Information Management, vol. 39, pp. 60-66, 2005.

[15] J. Eloff and M. Eloff, "Information security architecture," Computer Fraud & Security 2005, pp. 10-16, 2005.

[16] E. Humphreys, "Information security management system standards," Datenschutz und Datensicherheit-DuD, vol. 35, pp. 7-11, 2011.

[17] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," Pittsburgh, PA, Carnegie Mellon University, 2003.

[18] G. Ridley, J. Young, and P. Carroll, "COBIT and its Utilization: A framework from the literature," In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004.

[19] E. Humphreys, "Information security management standards: Compliance, governance and risk management," information security technical report, vol. 13, pp. 247-255, 2008.

[20] J. S. Broderick, "ISMS, security standards and security regulations," information security technical report, vol. 11, pp. 26-31, 2006.

[21] S. B. von Solms, "Information Security Governance–compliance management vs operational management," Computers & Security, vol. 24, pp. 443-447, 2005.

[22] M. Vogel and V. Broer, "Security Compliance Monitoring–The next Evolution of Information Security Management," ISSE 2013 Securing Electronic Business Processes, pp. 183-194, 2013.

[23] A.-M. Ghirana and V. P. Bresfelean, "Compliance Requirements for Dealing with Risks and Governance," Procedia Economics and Finance, vol. 3, pp. 752-756, 2012.

[24] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," Information & Management, vol. 46, pp. 267-270, 2009.

[25] T. Wiander, "Positive and negative findings of the ISO/IEC 17799 framework," In Proceedingsof 18th Australian Conference on Information Systems (ACIS 2007), 2007.

[26] R. Moen and C. Norman, "Evolution of the PDCA cycle," In Proceedings of the Asian Network for Quality Congress, pp.15-19, 2009.

[27] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of security threats in information systems," Procedia Computer Science, vol. 32, pp. 489-496, 2014.

[28] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," In Proceedings of the 1997 IEEE Symposium on Security & Privacy, pp. 154-163, 1997.

[29] F. Farahmand, S. B. Navathe, G. P. Sharp, and P. H. Enslow, "A management perspective on risk of security threats to information systems," Information Technology and Management, vol. 6, pp. 203-225, 2005.

[30] M. Alhabeeb, A. Almuhaideb, P. D. Le, and B. Srinivasan, "Information security threats classification pyramid," In 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA, pp. 208-213, 2010.

[31] S. Gerić and Ž. Hutinski, "Information system security threats classifications," Journal of Information and Organizational Sciences, vol. 31, pp. 51-61, 2007.

AUTHORS

Moneef Almutairi

Mr.Almutairi received his bachelor degree in information systems from King Saud University (KSA) in 2001, and his master degree from Newcastle University (UK) in 2009. He is currently doing his PhD in computer science at Newcastle University (UK).

Stephen Riddle

Dr Riddle obtained his BSc in Computer Software Technology at the University of Bath in 1991, and completed a PhD at Bath in 1997 on the use of partial specifications and refinement theory to aid the process of explaining complex systems. Dr Riddle currentlly works at Newcastle University and delivers courses in formal specification (VDM-SL) and software development techniques at undergraduate level; software engineering, dependable systems, Java programming and high-integrity software development (SPARK) at postgraduate level. His research interests include: software engineering, security risk management, and requirements specifications for systems of the systems.