EVALUATING INFORMATION SECURITY CONTROLS APPLIED BY SERVICE-ORIENTED ARCHITECTURE GOVERNANCE FRAMEWORKS

Jacqui Chetty[1] and Marijke Coetzee[2]

[1]Department of Business Information Technology
[2]The Academy for Information Technology
University of Johannesburg

[1]jacquic@uj.ac.za
(011) 559 1177

[2]marijkec@uj.ac.za
(011) 559 2907

ABSTRACT

Ensuring a secure Service-Oriented Architecture implementation within an organisation is challenging. Without sound information security principles supporting a Service-Oriented Architecture implementation, the rate of success is low. The information security principles of identification, authentication, authorization, confidentiality, integrity, availability and accountability remain the same for Service-Oriented Architectures. However, the Service-Oriented Architecture environment consists of agile implementations, which are designed around principles that demand a different approach that can be to the detriment of information security. Unless all information security issues related specifically to Service-Oriented Architecture are taken into consideration, an organisation faces unnecessary risks. An organisation faced with these added challenges may choose to avoid confronting this architectural approach altogether. Regrettably, an organisation could also miss out on the advantages and potential value that a Service-Oriented Architecture has to offer.

In order to identify information security shortcomings regarding Service-Oriented Architecture governance frameworks, this paper evaluates two existing Service-Oriented Architecture governance frameworks against ISO/IEC 17799 (2005) controls. The paper presents an analysis and evaluation regarding the state of governance of information security for Service-Oriented Architectures, to assist managers on how this complex issue should be approached.

KEY WORDS

Information security, Service-Oriented Architecture, governance

EVALUATING INFORMATION SECURITY CONTROLS APPLIED BY SERVICE-ORIENTED ARCHITECTURE GOVERNANCE FRAMEWORKS

1. INTRODUCTION

Service Oriented Architecture (SOA) (Brown, et al., 2006) is a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains, and implemented using a variety of technology stacks. Although an SOA can be implemented using different technologies, web services (Champion, et al., 2002) is commonly used. Services can be shared and reused if design principles such as loose coupling, abstraction, discoverability, composition and the inclusion of a service contract are followed (Erl, 2006). Services implemented in this manner are vulnerable to information security threats, as they often expose the limitations of existing information security implementations (Buecker, et al., 2007).

SOA governance ensures that stakeholders define, implement and execute a business model and accountability framework for SOA. The main focus is to ensure that SOA policies are enforced by a policy enforcement model, which defines various policy enforcement mechanisms (Marks, 2008). Applying SOA governance in this manner may mean that information security controls are not comprehensively addressed.

The purpose of this paper is to evaluate whether existing SOA governance frameworks adequately address information security. Information security challenges for SOA are described in the following section. Section 3 evaluates two formal SOA governance frameworks. Section 4 describes ISO/IEC 17799 (2005) (ISO/IEC 17799, 2005) as a best practice for information security. Section 5 evaluates two SOA governance frameworks against ISO/IEC 17799 (2005), to illustrate which ISO/IEC 17799 (2005) controls are not adequately addressed in the frameworks. Section 6 concludes the paper.

2. SOA INFORMATION SECURITY CHALLLENGES

Traditional IT environments are governed by IT and information security governance frameworks such as Cobit (IT Governance Institute, 2007) and ISO/IEC 17799 (2005), shown by layers on the right of Figure 1.

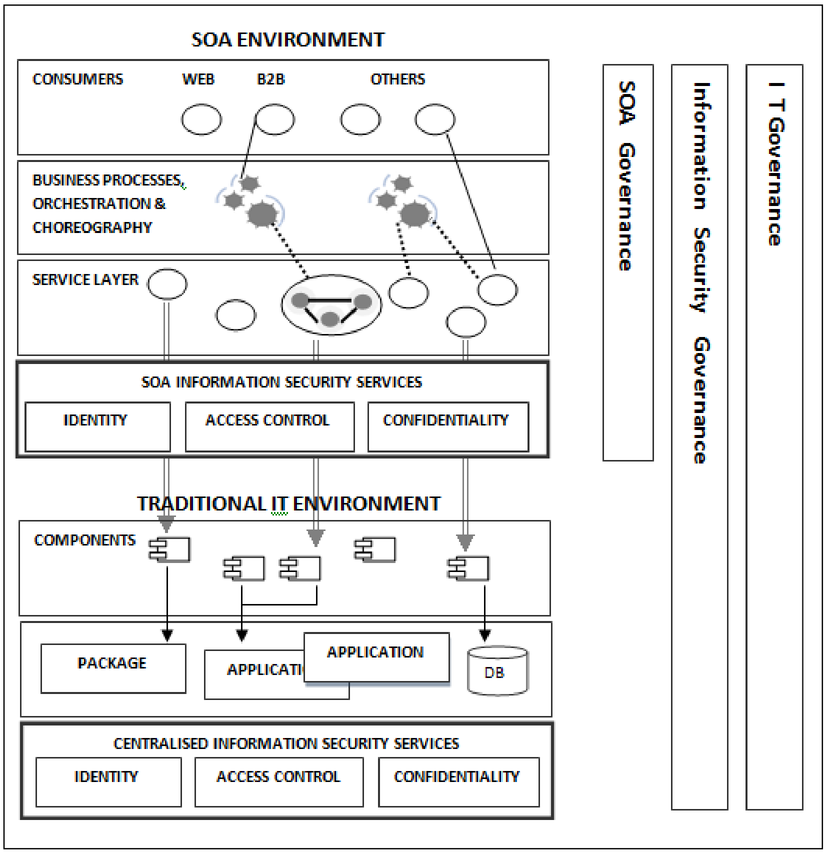

Figure 1: Traditional IT and SOA environments

Centralised information security services, shown at the bottom of Figure 1, protect this environment following a set of well-known best practises, defined by the IT and Information security governance layers. These controls are centralised, are characterised by human-to-machine interactions, have a fixed network perimeter to protect, address a singular information security context, and makes use of mechanisms of high assurance such as platform-dependent operating system access controls.

In contrast, an SOA environment consists of platform independent boundaries that are not fixed. Software components are exposed via service interfaces, as shown in Figure 1. Services can be composed or orchestrated into complex business processes and exposed to B2B transactions with remote partners. This complex environment needs another layer of governance, shown on the right of Figure 1, to cater for its complexity. Furthermore, service design principles such as loose coupling and composition have a detrimental effect on information security (Pulier & Taylor, 2006). Loosely coupled services do not form dependencies with other services or resources (Erl, 2008), regardless of context such as information security. Information security must be defined in a platform independent manner, to function unobtrusively to the service. The application of such security relies heavily on a policy infrastructure (Marks, 2008). When services are composed, the security context can only be determined at the time of composition. This increases the complexity of identification of service consumers, access control and accountability. Figure 1 indicates a new layer of SOA security services that make use of immature, emerging standards, are custom-built, complex, automated and policy-driven to cater for machine-to-machine interactions.

Figure 1 highlights the dilemma faced by management of SOA-enabled organisations. They may decide to govern the SOA and its security by using a SOA governance framework, as information security is generally addressed within such frameworks, and tool support is provided by vendors. Questions pertinent to address are whether SOA and information security governance frameworks are in alignment with one another? Do they function in a complementary manner to each other, or do they duplicate governance controls? Is all vital information security controls identified by these frameworks, or should new controls be identified? The following section describes SOA governance frameworks, emphasising information security.

3. SOA GOVERNANCE FRAMEWORKS

There is currently no standard framework that exists for SOA governance. The Generic SOA Governance Model by Niemann, Eckert and Steinmetz (Niemann, et al., 2008), referred to as NES here, has been defined by considering both vendor frameworks such as SAP AG (Brandt, 2009), Oracle (Hodgson, 2009) and IBM (Evans, 2009), and academic frameworks such as Marks/Bell (Marks & Bell, 2008) and Bieberstein, et al (2006). This framework, and the SOA Governance Reference Model by Marks (Marks, 2008) are chosen for the evaluation, due to their formal and comprehensive approach. Vendor-driven approaches are not considered, as they focus on technology and tool approaches. Table 1 describes the NES framework.

Table 1: Generic SOA Governance Model –NES

The model consists of two parts shown below:

- **The SOA Governance Control Cycle** – The cycle consists of four phases, namely planning, design, realisation and operation, providing a closed loop. Planning and design includes definition of policies and metrics. Realisation is where governance mechanisms such as metrics and policy enforcement are installed and processes are activated. Operation is where the SOA governance processes are evaluated and analysed for effectiveness. This ensures that the system complies with policies.
- **The SOA Governance Operational Model**
  a. *SOA Center of Excellence (SCE)* defines and enforces guidelines and policies throughout the organisation. Information security is also considered here.
  b. *Best Practices Catalog* stores all policy experiences, both positive and negative, to consistently improve an SOA.
  c. *Policies* divide the policy-related topics into governance areas, including an area for information security-related policies which focuses on data and communication security, systems security and authentication and authorisation mechanisms.
  d. *SOA Processes* defines the SOA system that needs to be governed, subject to governance policies.
  e. *Metrics* are defined by the SCE and are applied to SOA Processes. Business, process, performance, SLA and SOA conformance metrics are defined, which correspond to specific policies like information security-related polices. The results of the metrics are fed back to the SCE for compliance.
  f. *SOA Maturity Measurement* element describes how an SOA is adapting and operating within an organisation and contributes to monitoring policy effectiveness.

The model uniquely considers governance of cross-organisational interaction on a technical level. Information security forms part of this framework but there is no separate, comprehensive element for information security.

Table 2 briefly highlights the MARKS model. This model is a very comprehensive, detailed model to provide a good structure for organisations that would like to implement an SOA governance framework.

Table 2: SOA Governance Model - MARKS

The layers of the model are grouped into four tiers. The tiers are Enterprise / Strategic Governance, SOA Operating Model Governance, SOA and Service Lifecycle Governance and Governance Enabling Technology. The Governance Enabling Technology tier applies across the other three, and is responsible for policy creation and policy enforcement, which includes information security policy control. This tier is described further, as it is the only one that addresses information security.

- **Governance Enabling Technology –** Policies are created and enforced using technology and tools across the services lifecycle. Policies should be monitored and managed to ensure that each policy is specific and that they can relate to one another. The use of policy automation through technology is encouraged. There are many tools and standards available to implement and enforce policies, namely registries, repositories, policy engines and distributed enforcement points. These tools interact with, amongst others, information security infrastructure. Implementing policy-driven SOA governance means adhering to web services standards.

This model identifies an important aspect of SOA governance, namely policy automation via technology support, to cater for agile machine-to-machine interactions. As it is very comprehensive, organisations must research it extensively before it is implemented.

The following section introduces a best practice for information security to evaluate each of these frameworks against.

4. INFORMATION SECURITY BEST PRACTICE - ISO/IEC 17799

Information security is achieved be implementing, amongst others, controls. For governance, control means to ensure that adequate measures are in place to provide assurance that objectives will be achieved and undesirable events will be prevented or detected and corrected (IT Governance Institute, 2007). Da Veiga and Eloff (2008) demonstrate that ISO/IEC 17799 (2005) addresses a comprehensive set of information security controls for governance. It is now chosen here as a baseline for the evaluation of information security of SOA governance frameworks. ISO/IEC 17799 (2005) controls are described in Table 3.

Table 3: ISO/IEC 17799 (2005) Controls

Security Policy – An information security policy must be developed which reflects organisational objectives, management support and commitment.

Organizing Information Security – Management must establish a framework to initiate and control the implementation of information security. Information security must extend to external parties.

Asset Management – The organisational assets must receive an appropriate level of protection, an asset inventory list must be kept and ownership of assets must be classified and documented.

Human Resources Security – All parties, both internal and external must understand their responsibilities and roles, be aware of security threats and concerns, support the information policy and management information security must be applied throughout.

Physical and Environmental Security – To prevent unauthorised physical access, damage, theft and interference to organisational assets.

Communications and Operations Management – To ensure that the operational context is secure and to ensure that the appropriate level of information security is applied to third parties. To maintain adequate levels of information security and ensure that information is exchanged in a secure manner. Systems must be monitored and information security events recorded.

Access Control – To control the access to information, authorisation of user access rights and to ensure that authorised users understand their responsibilities and are co-operative both internally and externally.

Information Systems Acquisition, Development and Maintenance – To maintain information security throughout the systems development lifecycle. To protect the confidentiality, authenticity and integrity of information through cryptographic means.

Information Security Incident Management – To ensure that information security weaknesses and events are highlighted in a timely manner.

Business Continuity Management – To ensure that interruptions to business activities can be handled appropriately and timely.

Compliance – To ensure that organisations comply with legal, organisational policies and standards.

For a secure SOA, it would be imperative that these controls are comprehensively addressed. The next section evaluates the two mentioned SOA governance frameworks, with regards to information security.

5. EVALUATING SOA GOVERNANCE FRAMEWORKS

The evaluation is shown in Table 4. The first column lists ISO/IEC 17799 (2005) controls. NES and MARKS are evaluated against each control and either receives * (not mentioned), √ (mentioned), √√√ (explicitly addressed) or ° **(**control should be addressed by the general information security governance of an organisation). A framework receives three ticks if it adheres to any of the following: security services are specifically mentioned, are defined as separate controls, controls are automated, or cross-organisational communication is considered.

Table 4: Evaluating SOA Governance Models against ISO/IEC 17799 (2005)

ISO/IEC 17799 (2005) CLAUSE	**NES**	**MARKS**
Security Policy	√√√	√
Organizing Information Security - Internally - Externally	* √√√	* *
Asset Management	√√√	√√√
Human Resources Security	√√√	√√√
Physical and Environmental Security	°	°
Comm. and Operations Man - Oper. procedure and 3rd party delivery - System Planning - Software protection	√√√ * °	√√√ * °
Access Control	√√√	√√√
Information Systems Acquisition, Development and Maintenance - Maintain information security throughout SDLC - Protect the confidentiality, authenticity and integrity using cryptographic means	 * *	 * √√√
Information Security Incident Management	√	√
Business Continuity Management	°	°
Compliance - Legally - Policies and standards - Effectiveness of auditing process is maximised	√ √ *	√ √ *

The table reveals that SOA governance does attempt to address information security controls, shown by the number of √√√s. The number of *s and √s indicates that information security is not addressed holistically.

A closer look reveals that:

- Information security is not addressed holistically, as there is no information security framework that specifically addresses how to initiate and control the implementation of information security across all layers of an organisation;
- Information security for external parties, which may be pertinent to secure cross-organisational interactions, is not always considered;
- Information security controls are not always applied across the systems development lifecycle;
- Not all security services such as encryption are explicitly mentioned;
- Considering the automated manner in which service interaction is performed, a concern is that auditing, which can validate the existence and persistence of SOA information security enforcement, is not comprehensively addressed.
- In line with the previous concern, auditable records of compliance that are automated does not form part of the frameworks;

Management and governance methodologies such as Cobit and ISO/IEC 17799 (2005), applied to the traditional IT environment as shown in Figure 1, are robust and mature. The evaluation of SOA governance frameworks with ISO/IEC 17799 (2005) is valuable as it indicates that SOA environments, rich with technology and having a different focus on application design and implementation, requires a different focus to how it is controlled. Generally, ISO/IEC 17799 (2005) does not address SOA or any other application development methodology directly. It does highlight that information security controls such as security policies, access controls and compliance to security policies are vital to SOA service delivery. The high level of complexity present in an SOA requires that its information security controls must address agile services that are policy driven; control dynamically changing security contexts; and have centrally controlled governance that is extensible and interoperable between domains. Principles like loose coupling, composition and discoverability, while attractive for business solutions, require stringent information security and governance.

The specific information security controls used in traditional IT environments do not cover these issues. It is important that the concepts and features of ISO/IEC 17799 (2005) controls are followed when specific information security controls are defined, to protect SOAs more comprehensively. The process of correlating SOA governance frameworks with ISO/IEC 17799 (2005) controls is a complex undertaking.

The following list provides some suggestions to enhance information security controls for SOA governance. It should be noted that this list is by no means complete.

- A separate, comprehensive SOA information security framework is needed to initiate and control the implementation of information security for services. This is to ensure that organisations do not overlook the complexity of information security that is embedded into an SOA governance framework.
- A Plan, Do, Act, Check (PDCA) model should be used to ensure a closed loop, SOA governance control cycle.
- A SOA governing body such as the SOA Centre of Excellence should include an information security committee, to liaise with that of the organisation to ensure that information security is addressed holistically, and that controls are not duplicated or left out.
- Cross-organisational Centres of Excellence are needed to ensure that cross-organisational cooperation is governed by information security policies, where possible.
- An automated policy framework is needed to control, enforce and monitor automated service interactions.
- The auditing of dynamically changing service interactions, to ensure that the information security policy is consistently being applied across all security contexts, is needed.
- As services are machine-to-machine interactions, automated mechanisms, not requiring human intervention are needed to ensure that policy specification, enforcement and monitoring are effectively applied.

- The use of standards such as WS-Trust (Nadalin, et al., 2007), WS-Provisioning (Schwartz, 2006), WS-Policy (Bajaj, et al., 2006) and XACML (Moses, 2005) is imperative to ensure that web services-based information security services can be integrated across platforms.

From this list it is clear that current information security controls needs to be extended for the purpose of information security for SOA governance. Figure 1 shows this, as SOA governance, which includes an information security component, is defined over IT governance, and Information Security governance.

For example, a Cobit control such as DS5 "ensure systems security" is addressed by ISO/IEC 17799 (2005) controls such as the definition of formal access control policies. This control needs to be extended for SOA to the definition of machine-readable access control policies, to be used by SOA specific access control services. The difficult task facing an organisation is ensuring that these frameworks are aligned with each other. This can only be achieved if comprehensive information security architecture is developed. The following section provides a conclusion and future work.

6. CONCLUSION AND FUTURE WORK

Governance has made an impact on information security and organisations. Consequently, organisations need to relook their information security frameworks. SOAs are not immune to these developments. A governance standard such as ISO/IEC 17799 (2005) was used to evaluate the extent to which information security is addressed in SOA governance frameworks. It has been identified that information security is not holistically addressed for SOA governance frameworks and adequate controls are not in place. It is important that information security is integrated into such a framework and forms part of all activities related to the framework. Future work will focus on evaluating other standards such as Cobit and ISO/IEC 27000, to develop a comprehensive information security model that can be embedded into SOA governance frameworks.

7. REFERENCES

Bajaj, S., Box, D., Chappell, D., Curbera, F., Daniels, G., Hallam-Baker, P., Hondo, M., Kaler, C., Langworthy, D., Nadalin, A., Nagaratnam, N., Prafullchandra, H., von Riegen, C., Roth, D., Schlimmer (Editor), J., Sharp, C., Shewchuk, J., Vedamuthu, A., Yalçinalp, U. & Orchard, D. (2006). *Web Services Policy 1.2 - Framework (WS-Policy)*. Available from: http://www.w3.org/Submission/WS-Policy. (Accessed 6 June 2008).

Beucker, A., Ashley, P., Borrett, M., Lu, M., Muppidi, S. & Readshaw, N. (2007), *Understanding SOA Security Design and Implementation IBM*. Redbooks

Bieberstein, N., Bose, S., Fiammante, M., Jones, K., Shah, R.: (2006) Service-Oriented Architecture (SOA) Compass - Business Value, Planning, and Enterprise Roadmap. IBM developerWorks

Brandt, N. (2009). *Bauer, Conergy, Infineon, Post, SAP AG: German Equity Preview*. Available from: http://www.bloomberg.com/apps/news?pid=20601100&sid=a1RiMsNUcbtk&refer=germany. (Accessed 12 April 2009).

Carter, S. (2007). *The new language of business: SOA and Web 2.0.* IBM Press.

Champion, M., Ferris, C., Newcomer, E. & Orchard, D. (Editors) (2002) *Web Services Architecture*. Available from: http://www.w3.org/TR/2002/WD-ws-arch-20021114/. (Accessed 24 March 2009).

Christensen, E., Curbera, F., Meredith, G. & Weerawarana, S. (2001). *Web Services Description Language (WSDL) Version 1.1*. Available from: http://www.w3.org/TR/wsdl. (Accessed 14 November 2007).

Da Veiga, A, & Eloff, J.H.P. (2007). *An Information Security Governance Framework.* Information Systems Management, 24:361-372

Eloff, J.H.P. & Eloff, M. (2005). *Integrated Information Security Architecture,* Computer Fraud and Security, 2005 (11), 10-16.

Erl, T. (2006), *Service Oriented Architecture: Concepts, Technology, and Design.* New York: Prentice Hall

Erl, T. (2008). *SOA Principles of Service Design.* Indiana:Prentice Hall
Evans, B. (2009). *IBM CFO: We Had 62 Unix Competitive Displacements In Q1.* Available from: http://www.informationweek.com/blog/main/archives/2009/04/ibm_cfo_we_had.html . (Accessed 19 April 2009).

Hodgson, J. (2009). *With Sun, Oracle May Be Serious About Hardware.* Available from: http://online.wsj.com/article/BT-CO-20090427-714253.html. (Accessed 27 March 2009).

ISO/IEC 17799 (2005). Information technology. Security techniques. Code of practice for information security management, South Africa.

IT Governance Institute. (2007). *Cobit 4.1*. Illoinois: IT Governance Institute.

Kanneganti, R. & Chodavarapu, P. (2006). *SOA Security in Action.* Manning (unedited draft)

Marks, E.A. & Bell, M. (2006), *Service-oriented Architecture A Planning and Implementation Guide for Business and Technology*. Wiley
Marks, Eric A. (2008), *Service-Oriented Architecture Governance for the Services Driven Enterprise*. Wiley

Moses, T. (2005). *eXtensible Access Control Markup Language 3 (XACML) Version 2.0.* Available from : http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf. (Accessed 17 March 2009).

Nadalin, A., Goodner, M., Gudgin, M., Barbir, A. & Granqvist, H. (Editors) (2007). *WS-Trust 1.3.* Available from: http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html. (Accessed 12 February 2009).

Niemann, M. (2008). *Governance for Service-oriented Architectures: An Implementation Approach.* Available from: http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-374/I-ESA2008_MichaelNiemann.pdf. (Accessed 5 January 2009).

Niemann, M., Eckert, J. & Steinmetz, R. (2008). *Towards a Generic Governance Model for Service-Oriented Architectures*. Available from: Americas Conference on Information Systems (AMCIS), AMCIS 2008 Proceedings, http//aisel.aisnet.org/amcis2008/361. (Accessed 4 February 2009).

Pulier, E. & Taylor, H. (2006). *Security in a Loosely Coupled SOA Environment*. Available from: http://www.developer.com/design/print.php/10925_3605836_1. (Accessed 2 March 2009).

Rahaman, M. A., Schaad, A. & Rits, M. (2006). *Towards Secure SOAP Message Exchange in a SOA.* Available from: ACM 1-59593-546-0/06/0011

Schwartz, M. (2006). *Web Services Gets SPML 2.0 Boost.* Available from: http://esj.com/articles/2006/05/02/web-services-gets-spml-20-boost.aspx. (Accessed 8 April 2009).

SDA India (2008). *IT Audit and Information Security*. Available from: http://iaudit.blogspot.com/2008/03/soa-mitigate-compliance-and-security.html (Accessed 27 January 2009).

Von Solms, H. & Eloff, Jan H.P. (2004). *Information Security*. RAU

Von Solms, S.H. & Von Solms, (2006). *Information Security Governance*. Unpublished draft.

Weill, P. & Ross, J. (2004): *IT Governance*. Harvard Business School Press
Whitman M. E. & Mattord H. J. (2009). *Principles of Information Security*. Course Technology