Towards An Information Security Framework For Service-oriented Architecture

Jacqui Chetty
Business Information Technology
University of Johannesburg
Johannesburg, South Africa
jacquic@uj.ac.za

Marijke Coetzee
Academy of Information Technology
University of Johannesburg
Johannesburg, South Africa
marijkec@uj.ac.za

Abstract— **Service-oriented architectures support distributed heterogeneous environments where business transactions occur among loosely connected services. Ensuring a secure infrastructure for this environment is challenging. There are currently various approaches to addressing information security, each with its own set of benefits and difficulties. Additionally, organisations can adopt vendor-based information security frameworks to assist them in implementing adequate information security controls. Unfortunately, there is no standard information security framework that has been adopted for service-oriented architectures.**

This paper analyses the information security challenges faced by service-oriented architectures. Information security components for a service-oriented architecture environment are proposed. These components were developed collectively from service-oriented architecture design principles, the ISO/IEC 27002:2005 standard, and other service-oriented architecture governance frameworks. The information security framework can assist organisations in determining information security controls for service-oriented architectures, aligned to current ISO/IEC 27002:2005 standards.

Keywords-service-oriented architecture, design principles, governance, information security framework

I. INTRODUCTION

Traditional Information Technology (IT) environments are able to solve complex problems in an efficient way. Information security controls have been developed to ensure secure transactions between organisations. Controls such as Kerberos tickets, X.509 certificates, Access Control List's (ACL's), firewalls, encryption mechanisms and message digests are well developed, mature and they address information security services for identification, authentication, authorisation, confidentiality, integrity and non-repudiation. Unfortunately, they often restrict the manner in which organisations conduct business transactions as organisations are locked into a specific way of conducting business [1].

Service-oriented Architecture (SOA) [2] establishes an architectural model [3] to implement business processes, providing more flexibility and agility. It 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 technology [4] is commonly used. These services provide interoperability and agility for business transactions, if design principles such as loose coupling, abstraction, discoverability, composition and the inclusion of a service contract are followed [5]. They can provide a competitive edge for organisations that see IT as a burden, instead of a solution. Services can be reused, lowering development costs, or combined with other services to create composite applications. However, services implemented in this manner make use of open standards; apply different information security contexts; are platform-independent; expose information security controls to customers; can cross domains; and are vulnerable to information security threats. They often expose the limitations of existing information security implementations [6]. For example, all user credentials are stored in a repository such as a Lightweight Directory Access Protocol (LDAP) [3]. Traditional applications consult this repository to authenticate a user. If a service is invoked from another domain, this repository cannot provide authentication.

To overcome such limitations, more differentiated approaches to SOA information security need to be adopted [1] [7] [3]. Regardless of the approach adopted, SOA information security should be policy-based, and provide end-to-end protection concerning authentication, authorisation, encryption and integrity of messages.

The purpose of this paper is to analyse the challenges faced by organisations wanting to conduct secure transactions in a service-oriented manner. Furthermore, an SOA information security framework, which can assist organisations in developing information security for service-oriented transactions, is discussed and presented.

The paper is structured as follows: SOA design principles are discussed next. These design principles have a negative effect on information security, which leads to challenges for SOA information security, described in section III. To determine information security components for an SOA information security framework, section IV provides an analysis of the ISO/IEC 27002:2005 standard, and other SOA governance frameworks. The information security components described in section V, are collectively developed from the challenges discussed, the ISO/IEC 27002:2005 standard, and other SOA governance frameworks. The framework is presented and discussed in section VI. Section VII concludes the paper.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

II. SOA DESIGN PRINCIPLES

The success of an SOA is determined by the extent to which design principles are applied to service development [3]. These principles form the essence of service-orientation, providing a guideline for developing service logic that is interoperable and agile. The design principles are the inclusion of a service contract, loose coupling, abstraction, reusability, autonomy, statelessness, discoverability and composition [3] [1]. Applying traditional information security mechanisms inhibits how design principles can be applied to service transactions. Each of these principles is now discussed [3], focusing on information security implications. The service contract is discussed next.

A. Service contract

A service contract is a public, technical document that expresses the rules of engagement, as well as the requirements and constraints that need to be adhered to for service interaction [5]. Unlike traditional platform-dependent IT environments, where all clients are known and configured beforehand, SOA service consumers are not known in advance, and can be hosted by other domains and platforms. To allow service consumers to secure their messages correctly, information security mechanisms need to be abstracted from the platform and associated rules of engagement need to be provided in a service contract. This ensures that consumers can apply required security mechanisms and controls to messages when they consume a service method [3].

A service contract is separated from the underlying logic. If a service contract is designed correctly, it can be used for different contexts, not bound to a particular business process. The service contract is said to promote loose coupling, discussed next.

B. Loosely coupled services

Loose coupling refers to modules of code that are independent of one another [5]. A module can be changed without it affecting the operation of other modules. Traditional applications consist of modules, which can include information security controls with application code. There is thus a tight boundary between code and security controls are used within a singular security context. For loosely coupled information security, a service contract must be generic enough to protect any number of security contexts as service contracts are invoked for different security contexts, by different consumers, across platform-independent domains.

The amount of information in a service contract may over-expose or under expose information security controls. This relates to the level of abstraction that is used to develop a service contract, discussed next.

C. Service abstraction

Service abstraction is ensuring that the level of detail within a service contract is equivalent to the level of detail exposed to a service consumer [3]. Loose coupling is preserved by service abstraction. The level of abstraction negatively influences information security, as a low level of abstraction can result in over-exposing information security controls, leading to service attacks. A high level of abstraction results in insufficient exposure of information security controls, leading to consumers making assumptions regarding information security [1]. For example, a consumer may be able to deploy a method without proper authentication. Although managing and controlling the degree of abstraction is difficult, the type of information exposed can also negatively influence information security.

Abstraction regulates the quantity and type of information exposed and published. By achieving this, reuse potential, discussed next, is maximised.

D. Service reusability

Service reusability refers to code that can be used for more than one purpose, and forms the backbone on which service-orientation is built [5]. It is difficult to ensure reusability as reusable services must be adaptable to various contexts; generic enough to accommodate different types of consumers; provide a service contract that is flexible; and allow multiple consumers simultaneous access [3]. Consequently, reuse cannot be viewed in isolation to loose coupling and abstraction. By limiting dependencies between services and abstracting underlying logic they can be reused for other contexts. For example, a security service that provides audit logs could do so for any application.

Reusable services are independent units of code that can be applied to different security contexts. These services exhibit autonomous behaviour, discussed next.

E. Service autonomy

Service autonomy is the ability for services to maintain a high level of control over their underlying business logic implementation [3]. Autonomy is well suited to services that are deployed individually, although services, which form part of a composition, develop dependencies on one another, lowering autonomy [1]. Achieving autonomy has implications for information security. It may be difficult for autonomous services to inherently trust one another. An interface does not indicate whether a service will behave in a predictable manner.

Statelessness, discussed next, can be influenced by autonomy.

F. Service statelessness

Statelessness refers to services that do not keep track of transaction or session information [5]. This design principle implies state information, including security context data, is kept within a SOAP header of a message. Therefore, if consumers are exposed to the correct set of functions, the correct state information related to that security context can be found in the SOAP headers.

Service discoverability, discussed next, ensures that consumers can only access a set of functions intended for them.

G. Service discoverability

Service discoverability means that service metadata is accurately defined, clearly documented, centrally stored, accessible, easily searched for, and clearly understood [1] [3]. A service contract, stored in a registry, provides an interface, exposed to consumers. There are information security implications to consider such as exposing information security

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

controls and mechanisms to consumers. The quantity of information exposed to a consumer needs to be controlled. Depending on the type of consumer, the interface intended for that consumer only, should be revealed.

Design principles discussed thus far all support service composition [3], discussed next.

H. *Service composition*

Service composition is assembling service capabilities that consist of smaller units of logic to solve larger problems [3]. The manner in which all other design principles are applied, affects service composition. For service composition, a service contract must be flexible enough; services must be loosely coupled; hiding composition details is favourable; services must be reusable; high levels of autonomy is required; stateful information is kept in SOAP headers; and accurately defining metadata for discovery purposes is beneficial. Consequently, all information security implications discussed for other design principles, apply to service composition. Furthermore, combining services with different security contexts to reflect a business process is difficult.

Design principles have a negative effect on developing secure services [1]. This demanding environment poses many challenges, discussed next [1] [8].

III. SOA INFORMATION SECURITY CHALLENGES

To take advantage of the benefits associated with service-orientation, it is essential to apply SOA design principles to service design. In addition to traditional information security, careful consideration must be given to ensure SOA information security, as these design principles can create challenges for an SOA [7] [3] [9]. From the previous discussion the challenges associated with designing service contracts and their respective services are identified as:

- Develop a generic service contract that exposes an interface and protects exposed interfaces and registries;
- Information security mechanisms need to be machine-readable, policy-based and platform-independent to provide secure service interaction across domains;
- The management and control of information security mechanisms where services are deployed from other domains with unknown information security requirements;
- The degree of loose coupling and abstraction needs to be managed and controlled to ensure that an adequate amount of metadata is contained within a service contract;
- The level of information security required and the type of content needed to secure a message for a particular context must be determined;
- Build information security requirements that are flexible enough to be reused for varying contexts where state security information regarding a context can be audited;
- Build a trust component;

Although an SOA has the potential to change the way in which applications are developed and deployed, there are information security challenges that must be overcome. Understanding these challenges can positively contribute to the development of an SOA information security framework. The following section evaluates current information security practices for traditional IT environments and SOA-based environments, to establish a baseline towards developing such a framework.

IV. EVALUATING SOA INFORMATION SECURITY

SOA information security plays an important part in SOA governance. Figure 1 below illustrates the layers of governance needed for a traditional IT environment and an SOA environment. In figure 1, an SOA environment is an extension of a traditional IT environment, bound by traditional information security services. Unlike the traditional environment, which has fixed perimeters, is platform-independent and addresses a singular security context, services are deployed across boundaries, are platform-independent, and address multiple contexts. To this end, an additional layer of SOA governance, illustrated in figure 1, is needed.

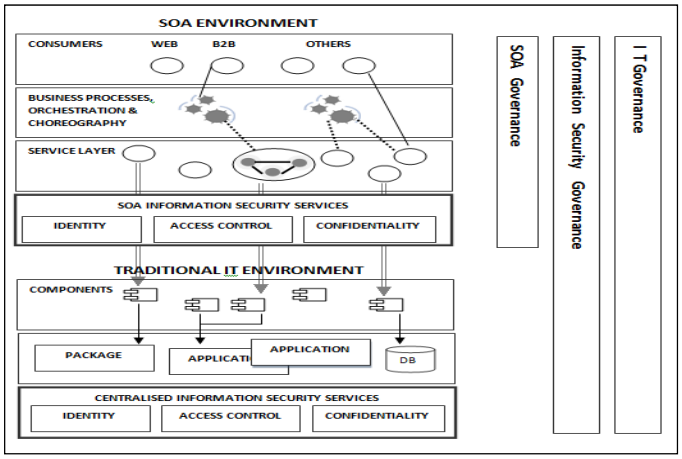

Figure 1. Traditional IT and SOA environments

Consequently, additional information security controls are needed because of the challenges that arise. As traditional IT environments create a baseline for information security, current practices must first be analysed. The ISO/IEC 27002:2005 [10] standard that is an international best practice in support of IT governance is discussed next.

A. *ISO/IEC 27002:2005 standard*

Information security is achieved by, amongst others, implementing controls. Da Veiga and Eloff [11] demonstrate the strength of the ISO/IEC 27002:2005 standard [12] when addressing a comprehensive set of information security controls for governance. These controls are mature and well developed for traditional environments. They provide a baseline to develop information security within an organisation.

The controls related to the ISO/IEC 27002:2005 are traditional IT controls, which consequently also apply to an SOA environment. However, the manner in which these

controls are implemented for an SOA differs to that of a traditional IT environment. Services are designed using principles that provide interoperability and agility, which threaten traditional information security practices. To this end, it is helpful to evaluate current information security SOA practices and SOA frameworks, of which information security is included.

B. SOA governance frameworks

SOA governance defines policies, and introduces mechanisms to control their enforcement [9]. Information security policies are fundamental to this development. There are various frameworks to implement SOA governance [12]. Some frameworks focus on specific aspects while others provide a generic approach to governance [9] [7]. One such framework is the Generic SOA Governance Model [9], which consists of an SOA governance control cycle and an SOA governance model. Controls such as a Center of Excellence (CSE), Best Practices Catalog, Security-related Policies and Metrics are described. Previous research by the authors [12] evaluated SOA governance frameworks [7] [9] against the ISO/IEC 27002:2005 and determined the extent to which SOA governance addresses information security controls. It was found that information security for SOA-based environments is not holistically addressed. Some challenges include that information security for external parties is not always considered; information security controls are not always applied across the systems development lifecycle; and not all security services such as encryption are explicitly mentioned;

TABLE I. SOA INFORMATION SECURITY CONTROLS

SOA INFORMATION SECURITY CHALLENGE	SOA INFORMATION SECURITY CONTROL
Expose generic service contracts and protect exposed interfaces and registries	– Service governance – Design time / run time management – Service inventory – Policy-driven security – Lifecycle policy management
Develop machine-readable, policy-based, platform-independent information security controls which cross domains	– Service governance – Policy-driven security – Lifecycle policy management
Manage and control information security mechanisms for services deployed across domains with unknown information security requirements	– Service governance – Security services – Message-level security – Policy enforcement mechanisms (PEM's)
Manage and control the degree of loose coupling and abstraction to ensure adequate amounts of metadata contained within a service contract	– Design time / run time management – Lifecycle policy management
Determine the level of information security required and the type of content needed to secure a message for a particular context	– Service governance – Policy-based security – Security services – Lifecycle policy management – Policy enforcement mechanisms (PEM's)
Build information security requirements which are flexible enough to be reused for varying contexts and audit state security information for a context;	– Service governance – Lifecycle policy management – Auditing
Build a trust component;	– Security services – Lifecycle policy management

Although the ISO/IEC 27002:2005 and SOA governance frameworks do not holistically address SOA information security, they do however provide a baseline on which to build SOA information security. Additionally, various organisations and researchers have defined controls such as Web services standards, policy-based security, security services and awareness and training, for SOA information security [1] [13]. Considering all of these controls collectively, and taking into consideration that finding solutions to these challenges can guide the development of a framework for SOA information security, Table 1 identifies controls which provide solutions for these challenges.

These controls can be categorised into components since components are the principles that enable the implementation and maintenance of information security [11]. The researchers now propose the following four components:

- SOA information security governance
- SOA information security management
- SOA information security model
- Policy information security framework

The following section discusses these components in more detail, taking into consideration the challenges and controls.

V. INFORMATION SECURITY COMPONENTS

From the discussion thus far, it is clear that additional information security controls need to be established for SOA information security. These controls do not replace traditional information security but supplement traditional information security, to compensate for the manner in which services are designed. For example, including a service contract when designing services means that information security mechanisms are exposed to consumers. By designing a service contract in a particular manner and including a control such as a security service, can reduce the level of information security mechanisms exposed. This section describes these components. SOA information security governance is discussed next.

A. SOA information security governance

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 [7]. The governance process must reflect decisions made by business to develop and deploy business services. Service governance, a subset of SOA governance, controls, enforces and monitors the design, development, deployment, maintenance, versioning and testing of service contracts and services [7]. Service governance develops best practices [7] and standard practices, which must be catalogued, describing how service contracts must be developed.

Information security governance is the manner in which information security controls and mechanisms are deployed to mitigate risks [11]. For SOA this is critical as service design principles challenge traditional information security controls. SOA information security governance is realised through policy-driven security, which dictates behaviour of services [7]. It must ensure that service contracts are: developed in a generic manner to meet individual consumer needs; platform-independent to provide cross-domain interaction; able to secure a particular context. Attention must be given to ensuring that the level of information security required and the type of

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

content needed to secure a message for a particular context, is correct. These controls must be enforceable within and across domains.

Providing governance allows management to strategically make decisions regarding the development of information security policies and ensures that policies are enforceable. SOA information security governance must be complemented with SOA information security management to ensure that these strategic decisions are implemented across managerial levels. This component is discussed next.

B. SOA information security management

It is important to separate governance from management, as governance deals with deciding on the critical aspects related to SOA information security and management focuses on implementing these decisions [7]. Once decisions pertaining to SOA information security have been made, these decisions need to be executed [14]. Management is responsible for design time and run time management, service inventories, auditing and training and awareness. Each management aspect is discussed next.

1) Design time and run time management

Design time and run time management is responsible for ensuring that a generic service contract consists of the correct level of abstraction to ensure that an adequate amount of metadata is contained within the service contract. For SOA information security, design time and run time management centralises this process. Standardised information security controls can be applied, which increases interoperability and agility between services. This in turn also provides an opportunity to apply design principles such as loose coupling, reusability and composability. For example, a generic service contract that expresses standardised information security controls, exhibiting loose coupling, becomes highly reusable and in turn can be used for service compositions.

2) Service inventories

Service inventories represent reusable, agnostic services, derived from business tasks, catalogued and maintained. Service inventories, which are dynamically linked to a registry, should also allow services to be discovered. These inventories must be controlled and maintained to avoid redundancy between inventories and registries used for discovery.

3) Auditing

Auditing has become a mandatory requirement as recent regulations in Europe and the USA dictates that organisational assets must, not only be secure, but organisations must also prove this fact. Furthermore, the King III report [15] stipulates that a committee must oversee integrated reporting. Security state information can be extracted from SOAP headers, related to a transaction, stored in dedicated databases, for further monitoring and reporting.

4) Training and awareness

SOA management is responsible for providing training and awareness [16]. Employees must be aware of SOA information security and receive adequate training. This is the primary means of ensuring that SOA information security management is successfully implemented. Developers and administrators need to be aware of the challenges faced by SOA information security. Furthermore, they need to be trained regarding any SOA information security models and frameworks that must be implemented.

Implementing management practices for SOA information security requires technological building blocks and new approaches, to ensure that authentication, authorisation and encryption remain intact, and SOA information security challenges are minimised. An SOA information security model that includes policy-driven security, security-as-a service and message-level security uses technologies to implement SOA information security.

C. SOA information security model

SOA industry standards were developed without much thought given to information security practices [17]. Consequently, the manner in which information security is applied requires an information security model [1] for SOA. To compensate for the lack of information security standards, a separate layer of information security, as seen in figure 1, is required [1] [17]. In addition to traditional information security, which is robust and mature [18], it is strongly recommended that this layer consist of policy-driven security [1] [17], security as a service [19] [1] and message-level security [1]. Each category is now discussed.

1) Policy-driven security

A policy-driven approach has been adopted for service interaction, which ensures interoperability between services. These machine-readable expressions convey requirements, rules and constraints regarding message exchange [1]. Security policies expressed in a service contract can be exposed to consumers. The manner in which policies are expressed can affect information security. For example, a policy can express that it is mandatory to use SAML tokens for authentication. Furthermore, policy requirements can be grouped, which provides a consumer an opportunity to choose a group of policy requirements that best suits their needs. For example, a policy can state that either a SAML token or X.509 certificates can be chosen to authenticate potential consumers. Although policy-driven security communicates requirements to consumers, it does have inadequacies.

Although these standards consist of shortcomings they are comprehensive enough to provide interoperability and reuse. Some of the shortcomings can be addressed by implementing security-as-a-service.

2) Security-as-a- service

Security-as-a-service is a security service that acts as an intermediary to authenticate and authorise potential consumers wanting to interact with other services [1]. A security service decouples security from the service logic. It consists of a generic interface using standards such as WS-Trust [20] and SAML, which can authenticate tokens, X.509 certificates and Kerberos tickets. Once authentication has taken place, a mechanism can authorise actions. A security service can ensure that requests to authenticate and authorise actions will only be granted if a consumer provides the correct credentials, regardless of the context, the type of information security requirements or the domain.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

Although SAML tokens provide the assurance that a consumer has been authenticated, it is important, from a consumer perspective, to decide whether a service is predictable, based on past behaviour. Part of a security service can act as a trust component to determine the reputation of a service, and convey this to a consumer.

For services to communicate with an intermediary such as a security service or with other services, secure message-level security is needed. Message-level security is discussed next.

3) Message-level security

Implementing security for services using traditional mechanisms can pose problems [1]. For example, SSL/TLS [1] is responsible for ensuring that a message reaches it's destination in a confidential manner. Only the sender and the receiver can access the message. Conversely, services may interact with intermediaries such as security services, before reaching their destination. SSL/TLS is unable to cater for such service interactions. For services, it is imperative to make use of message-level security. WS-Security applies different levels of security to different parts of a message. WS-Security [21] can be applied to a SOAP header, only viewed by authorised intermediaries such as security services, which have been mandated to view such detail [17]. This ensures that the confidentiality and integrity of messages is maintained.

For information security this means that a SOAP header can, through WS-Security, express authentication information in a secure manner. Authorised intermediaries can make use of this information to determine the validity of a claim. Furthermore, security state information can be held in a SOAP header, viewed only by authorised intermediaries or by the destination end-point itself. This information can be kept for auditing purposes. Making use of WS-Security standardises all SOAP headers, which ensures interoperability between SOAP headers and security services across domains.

A framework can be used to guide the implementation of an SOA information security model. The policy information security framework is discussed next.

D. Policy information security framework

In today's competitive environment where there is an explosion of information that needs to be constrained, it is complex for developers and administrators to effectively create, manage, and monitor policies. These policies form part of service contracts, which must be developed using standards to ensure platform independence. Policies must be developed from design principles, achieving a balance between these principles. Additionally, service contracts must be enforceable. To achieve this, a policy information security framework that consists of SOA standards, lifecycle policy management and policy enforcement mechanisms, is needed. These aspects are discussed next.

1) SOA information security standards

Many organisations such as OASIS [13] provide open standards. WS-Security, WS-Trust and WS-Policy [22] are standards for security services to authenticate, authorise and manage claims made by services. Providing standards permits an organisation to catalogue mandatory information security standards, which an organisation must conform to. This ensures that information security mechanisms are platform-independent, enabling them to communicate with other services across domains. This in turn provides interoperability and agility. Standards alone cannot ensure good information security practices. The manner in which policies are designed, developed and deployed can affect the implementation of information security.

2) Lifecycle policy management

Lifecycle policy management is the process of design, develop, deploy and manage [14]. Firstly, the design of policies must ensure that business requirements are considered. An important goal of an SOA is that service contracts and services be designed from business requirements [5]. This ensures that policies, which describe information security controls, are determined by business analysts and developers collectively, communicating business requirements for that service. Service inventories must be consulted to determine whether a service exists before design can begin.

Secondly, policy development must ensure generic service contracts, which contain the correct level of loose coupling and abstraction, to guarantee that the service contract is flexible enough for reuse. The type of content exposed must allow a wide range of interface options to consumers. Determining this balance establishes whether information security controls will be effective enough to provide secure interactions for services or whether these controls will be open to information security attacks. Lifecycle policy management must distinguish between internal and external consumers as information security controls will differ for each.

Thirdly, when policies are deployed, care must be taken to ensure that interfaces are only exposed to valid consumers.

Fourthly, managing registries such as service inventories, policy versioning, and auditing the effectiveness of policies, must be considered. For example, a policy that is updated must consider the impact that the updated information security controls will have on consumers. Unless policies are enforced, they become ineffective as security controls.

3) Policy enforcement mechanism

Providing policy declarations regarding the interaction of a service is only beneficial if there is a manner in which these declarations can be enforced. A policy enforcement mechanism (PEM) [23] is a proactive mechanism that can validate whether an action can take place or not. Without PEM's at various policy enforcement points (PEP) [7], policy-based information security cannot be effective. PEM's such as XML firewalls and enterprise service buses or similar proprietary intermediaries should be considered.

This section has discussed information security controls, developed from SOA information security challenges, categorised into various components. Table 2 below summarises the information security challenges for SOA and indicates which component, namely SOA information security governance (1), SOA information security management (2), SOA information security model (3), or SOA information security framework (4) provides a control for that challenge.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

TABLE II. ADDRESSING SOA INFORMATION SECURITY CHALLENGES

SOA information security challenge	1	2	3	4
Expose generic service contracts and protect exposed interfaces and registries	√	√	√	√
Develop machine-readable, policy-based, platform-independent information security controls which cross domains	√		√	√
Manage and control information security mechanisms for services deployed across domains with unknown information security requirements	√		√	√
Manage and control the degree of loose coupling and abstraction to ensure adequate amounts of metadata contained within a service contract		√		√
Determine the level of information security required and the type of content needed to secure a message for a particular context	√	√	√	√
Build information security requirements which are flexible enough to be reused for varying contexts and audit state security information regarding a context;	√		√	√
Build a trust component;			√	√

These components form part of an SOA information security framework. The following section illustrates and discusses a proposed SOA information security framework.

VI. SOA INFORMATION SECURITY FRAMEWORK

This framework was collectively derived from two information security governance frameworks developed by Booz Allen Hamilton [24] and by Da Viega and Eloff [11]. Booz Allen Hamilton incorporates functional processes similar to the ISO/IEC 27002:2005 controls seen in figure 2. These controls ensure the day-to-day IT operations within an organisation [24]. Da Viega and Eloff define managerial levels such as strategic, managerial/operational, and technical. In the proposed framework, each component within a level provides direction to that managerial level [11] regarding SOA information security. Each level is discussed next.

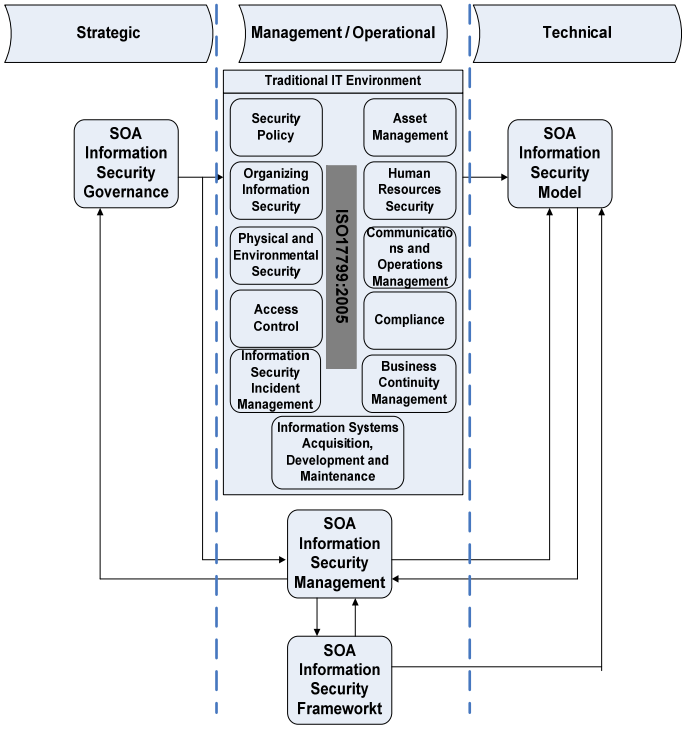

Figure 2. An SOA information security framework

1) *Strategic level*

Figure 2 illustrates that the SOA information security governance component provides direction at a strategic level. The SOA information security governance component develops best practices for the design, development, deployment, maintenance, versioning and testing of service contracts and services. Its role is to ensure that information security policies are developed, stipulating controls and mechanisms necessary to dictate behaviour. Furthermore, strategic management must decide how these policies become enforceable. Information security policies for the following information security challenges must be included:

- Exposure of generic service contracts;
- Protect interfaces and registries from consumers;
- Develop machine-readable, policy-based, platform-independent information security controls;
- Manage information security controls across domains;
- Provide adequate and correct information security controls to secure a context;
- Ensure that design principles are used to encourage reuse, interoperability and agility;
- Develop a policy enforcement model that determines PEM's [7];

These policies must be aligned to current IT information security practices as traditional information security forms the foundation on which SOA information security is built. Additionally, security policies must be communicated to the SOA information security management component.

2) *Management/Operational level*

Figure 2 illustrates that the SOA information security management component provides direction at a management/operational level. Information security policies mandated at the strategic level must become operational. This component is responsible for ensuring that service contracts and services are designed and deployed; service contracts, services and service inventories are protected; security state information is maintained; and employees are familiar with SOA information security policies, practices and frameworks. Feedback is given to the SOA information security governance component. To implement this management function, the policy information security framework component is required.

The SOA information security framework component and the SOA information security management component are collectively in alignment with the traditional IT environment, seen as an extension. The SOA information security management component communicates mandated information security policies to the SOA information security framework component. This component ensures that service contracts and services depict these policies through lifecycle policy management. PEM's determined at a strategic level are implemented according to the policy enforcement model.

3) Technical level

Figure 2 illustrates that the SOA information security model component provides direction at a technical level by implementing standards and technologies, which allow service contracts and services to interact with one another, in a secure manner. Policy-driven security is the primary means of implementing SOA information security governance. Machine-readable expressions convey information security policies, mandated at a strategic level, managed by the SOA information security management component. Similarly, security services must ensure that authentication and authorisation mechanisms mandated at the strategic level are implemented. Message-level security ensures that parts of a message such as a SOAP header are secured, and reach the destination end-point. The SOA information security model provides feedback such as auditing of security state information, to the SOA information security management component.

The proposed SOA information security framework can be used by an organisation as a starting point to develop guidelines and implement controls, which address SOA information security challenges. This framework provides managers and developers with effective information security components for an SOA.

VII. CONCLUSION

The manner in which service contracts and services are designed poses challenges for SOA information security. Consequently, organisations need to review their information security controls for SOA information security. It has been identified that traditional information security controls and SOA governance frameworks do not holistically addressed for SOA information security. These controls do, however, provide a baseline to build an SOA information security framework.

This paper proposes an SOA information security framework, based on components, which consist of a variety of controls that can minimise the challenges of SOA information security. These components collectively provide direction for strategic, management/operational and technical levels to implement SOA information security. Management and executives can use the framework as a reference for implementing SOA information security. Future work will focus on further analysing and extending this framework.

REFERENCES

[1] Kanneganti, R. and P. Chodavarapu, SOA Security. 2008: Manning.

[2] OASIS, OASIS: Reference Model For Service-Oriented Architecture 1.0. 2006.

[3] Erl, T., SOA Principles of Service Design. 1 ed. 2008, Indiana: Prentice Hall.

[4] Champion, M., et al., Web Services Architecture. 2002.

[5] Erl, T., Service-oriented Architecture: Concepts, Technology and Design. 2006, New York: Prentice Hall.

[6] Beucker, A., et al., Understanding SOA Security Design and Implementation. 2007, IBM.

[7] Marks, E.A., Service-oriented Architecture Governance for the Service Driven Enterprise. 2008: Wiley.

[8] de Leusse, P., T. Dimitrakos, and D. Brossard. A governance model for SOA. in 2009 IEEE International Conference on Web Services. 2009.

[9] Niemann, M., J. Eckart, and R. Steinmetz. Towards a generic governance model for service-oriented architectures. in AMCIS. 2008.

[10] 27002:2005, I., ISO 27002.(2005). ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Management (1st ed.). Switzerland:International Organization for Standardization. 2005.

[11] Da Veiga, A. and J.H.P. Eloff, An Information Security Governance Framework. Information Systems Management, 2008(24): p. 361-372.

[12] Chetty, J. and M. Coetzee. Evaluating Information Security Controls Applied By Service-oriented Architecture Governance Frameworks. in ISSA2009. 2009. Johannesburg, South Africa.

[13] OASIS, Advancing open standards for the information society. 2010.

[14] Marks, E.A. and M. Bell, Service-oriented Architecture A Planning and Implementation Guide for Business and Technology. . 2006, New Jersey: Wiley.

[15] Africa, I.o.d.i.S., King Report on governance for South Africa. 2009.

[16] (NIST), N.S.f.S.a.T., Information Security Handbook: A Guide for Managers. 2006.

[17] Pulier, E. and H. Taylor, Understanding Enterprise SOA. 2006, Manning.

[18] Pfleeger, C.P. and S.L. Pfleeger, Security in Computing. 4th ed. 2006: Prentice Hall.

[19] Miele, A. and R. Steinmetz, Cross-organizational Service Security - Solutions for Attack Modeling and Defense.

[20] Nadalin, A., et al. (2007) WS-Trust 1.3.

[21] Hallam-Baker, P., et al., Web Services Security: SOAP Message Security 1.1. . 2006.

[22] Bajaj, S., et al. (2008) Web Services Policy 1.2 - Framework (WS-Policy).

[23] Newcomer, E., Understanding Web Services XML, WSDL, SOAP, and UDDI. 2002: Addison Wesley.

[24] Miller, J., L. Candler, and H. Wald (2009) Information Security Governance.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE