Identity based Management:
Extending the ISMS for Federation

S. Woodhouse & P. White
Department of Lands
Panorama Ave, Bathurst NSW 2795 Australia
email: steven.woodhouse@lands.nsw.gov.au, peter.white@lands.nsw.gov.au

Abstract

Organisations usually have identified valid business requirements to share information and resources with other organisations. To achieve this sharing of information the organisations have to enter into some form of federation which can, and usually does, dramatically change their risk posture. Organisations develop and implement an Information Security Management System as part of good business management or to meet regulatory and certification requirements.

This paper examines the implications of an organisation joining a federation and using Identity based Management as part of its normal operations. It investigates the requirements that must be met internally, and externally, in order for an organisation to attempt to create a federation with external organisations. It then proposes a framework for using Identity based Management within a federation.

Introduction

Many enterprises have a business need to share information with, or consume resources from, other enterprises. Access to these resources can be provided either on an individual user basis or by establishing a federation between the enterprises involved.

In many cases, if the end users are individuals, access is provided on an individual basis. This usually uses an authentication method such as a username and password combination. This authentication pair has to be set up for each individual user requiring access. However, if the end-user is another enterprise with a number of users, the enterprise publishing the resources may offer access through a federation in order to reduce the administrative burden on itself.

A federation is created when an enterprise publishes some internal resources externally and allows other remote enterprises to consume those resources, using their individual internal authentication [1]. The enterprise that publishes the resources is known as the federation master, while enterprises that consume those resources are known as federation members (Fig. 1). Typically, the federation master allows users in a federation member enterprise to authenticate and consume the published resources using their own internal identity and authentication credentials. This allows the federation master to publish resources to a number of external enterprises without the administration overhead of additional user identities and authentication credentials.

The use of federation as a solution for the authentication of remote enterprise users to access a published resource is becoming more popular. There are now a number of accepted models of federation described in the literature, ranging from the standard Federation model described above to a Distributed model and an Internet

model that is designed for use with a third-party trusted Identity Provider. These models share some basic characteristics:

- The federation master publishes the resources on offer.
- Any enterprise seeking access to the resources must enter into a trust relationship with the federation master.
- Authentication of users occurs at the originating enterprise, not at the federation master.

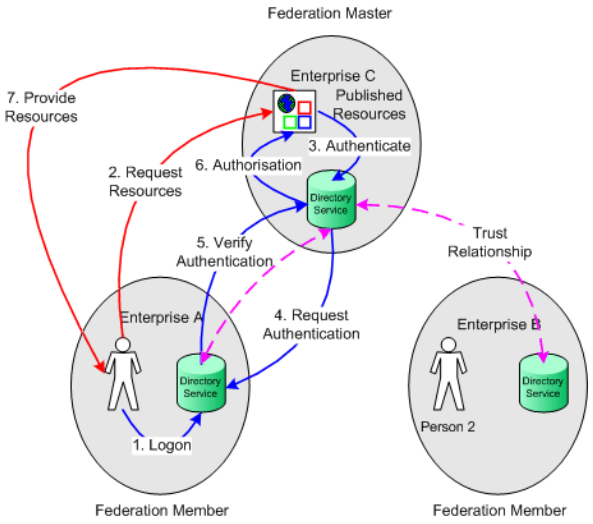

Figure 1: Federation Model

These characteristics tend to lead enterprises to consider the introduction and use of Identity based Management solutions when forming federations. The introduction of Identity based Management gives an enterprise a number of advantages, including:

- A method of identifying and reducing risk through the use of verified identity, documented process and audit;
- The creation of a series of security chokepoints;
- Increased business flexibility by being able to quickly adapt and apply business strengths to opportunities [2].

However, much of the security focus of enterprises remains at the network and hardware level and there is a tendency to have a primary focus on external threats to the enterprise. Many enterprises may be unaware if any of their digital identities have been compromised or if their authentication is sufficiently strong. Consequently, many enterprises may not include their federation partners, external authentication issues, or published resource access as part of their Threat and Risk Assessment (TRA) and thus their Information Security Management System (ISMS). It is our contention that by joining a federation, an enterprise must change the focus of its ISMS so that it also takes account the threats and risk associated with federation and modifies its policies and procedures to accommodate this changed risk posture.

No organisation can develop effective information security measures unless it has a clear understanding of what it is trying to protect itself from [3]. In this context a threat can be defined as "…any potential source of harm to the reliability or integrity of the IT system…" [4].

This paper will examine some of the issues and problems that an enterprise considering federation needs to consider. It will propose an extension to the ISMS that will provide an enterprise with a method of creating an Information Exchange Agreement that will address some of these issues.

Issues

It is unlikely that an enterprise will be able to impose its internal ISMS policies on an external enterprise in a federation. However, when an enterprise joins a federation it must enter into a trust arrangement with other enterprises in the federation. Normally, this trust arrangement is created as the result of a negotiated Information Exchange Agreement (IEA) or some other legal agreement as an out come of the enterprises TRA. This trust arrangement must then be taken into account within the enterprise's ISMS.

One of the issues that may create a problem for the enterprise is the issue of chains of trust [5]. A chain of trust can occur when an enterprise trusts another enterprise to access its resources. The trusting enterprise may find that the trust extends beyond the original grant of trust if the trusted enterprise also has relationships with other enterprises. An enterprise must consider whether the fact of joining a federation involves it in a chain of trust that extends beyond the trust arrangement that it has agreed to. This may lead to indirect external trusts to unknown partners involving a higher level of risk than the enterprise anticipated. This may allow a user from a non-trusted remote enterprise to access the local enterprise's resources based on that user's access to another mutually trusted enterprise.

The enterprise must consider the possibility of a chain of trust occurring and include this possibility and the potential consequences in its TRA.

Another problem that can arise in a federation context is the issue of identity compromise. Most enterprises recognise that the core of their information system is the information that it holds and employ a series of measures to ensure the integrity and security of that information. Many enterprises consider their data secure because it is stored in a database on an internal network where only authorised users access the data. Unfortunately, it is not always recognised that the users who are authorised to enter, manage and manipulate that data are just as critical as the information itself. The security of the data relies, in part, on who has access to the data and "…anyone who steals the identity of one of your users becomes that user and has access to your most sensitive systems and data. If just one user's identity is compromised, your systems are vulnerable" [6].

In a federation, external users can gain access to a local resource based on their authentication which occurs at the remote originating enterprise. The local enterprise has a trust relationship with the remote enterprise and, as a result, trusts the users that it authenticates. But this trust relationship also includes trusting that the user's identity has not been compromised by a third party and the identity is who it claims to be.

This identity compromise issue may be addressed by an enterprise that negotiates, as part of its IEA, that a framework should be used for authentication, authorisation and access management within members of the federation. A key stipulation of any such framework must be that it is capable of being implemented using an enterprise's existing systems. The framework must also offer a verifiable method of auditing authentication. This will act to assure the federation partners that the risk of intrusion has been reduced to an acceptable level.

Security Management

The aim of planning, designing and implementing security in and around information systems is to ensure not only the confidentiality and integrity of the information produced, stored and used but also the continued availability of both the information and supporting infrastructure [7-11].

ISO/IEC 27001:2005, titled "Information Security Management - Specification with Guidance for Use", is the international standard that supersedes AS/NZS 7799.2:2003. The basic objective of the standard is to help establish and maintain an effective information management system, using a continual improvement approach.

ISO/IEC 27001:2005 is a generic, advisory document. It lays out a structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. While none of the controls are mandatory, an enterprise may choose to adopt only some controls, but they should be prepared to demonstrate that this decision was reached through a rational process.

The standard contains 39 control objectives to protect information assets against threats to their confidentiality, integrity and availability. These control objectives comprise the functional requirements specification for an enterprise's information security management architecture. However, a few controls are not applicable in every case, and the generic wording of the standard may not necessarily reflect the enterprise's precise requirements.

The final version of ISO 27001 was published in October 2005. It should be noted, however, that this is in fact only the first of a series of standards to support information security. However, it may well be the most important, at least from a 'top down' perspective, as it defines the information security management system.

Threat and Risk Assessment

The Assets Register is a document that lists everything that is of value to an organization. It is used in the Threat Risk Assessment (TRA) to identify and determine the risk to the enterprise's assets. The TRA is conducted in two parts:

The first component identifies the threats to each of the access channels supporting the service to be secured, the controls selected to mitigate the risks to an acceptable level for each channel, and demonstrates an acceptable residual risk level for each of the channels [9]. The controls applied to each channel are depicted in the Control Catalogue.

The second component, demonstrates a risk rating for each section in the ISO/IEC 27001:2005 standard, and determines a priority for risk treatment. The risk assessment also determines whether the requirements described in the standard are "applicable" to the service being protected [12]. The risk treatment methods are described in the TRA.

A requirement may be "not applicable" because it does not occur, or the cost of mitigation outweighs the risk realization value, or the enterprise deems that the risk is acceptable. All policy within the enterprise is derived from the Threat Risk

Assessment, which is to be reviewed annually. The TRA is documented in Threat Risk Assessment Report.

Statement of Applicability

The Statement of Applicability (SoA) documents the risks derived from each section of the AS/NZS ISO/IEC 27001:2006 standard and demonstrates the applicability of those risks to the services being protected [12]. The SoA describes the enterprise's attitude to risk, its risk appetite, the mitigation strategies (if any) used to treat the identified risk, the controls selected to facilitate the mitigation strategy and the acceptable residual risk level expected after the controls have been implemented.

Administration and Access Management

One of the major issues identified for an enterprise in a federation is that of identity compromise. This issue can be minimised by the use of an Identity based Management system that is implemented in accordance with an agreed framework. The concept of Identity based Management covers both the administration of identities as well as identity based access to resources.

The use of an Identity based Management system offers an enterprise some distinct advantages. The enterprise can identify and reduce the risk of internal identity compromise by documenting, reviewing and updating its identity administration work practices and work flows. The auditing and regular review of identity administration processes allows the enterprise to be certain that its digital identities are all related to a specific entity or service requirement. The use of change control in the Identity based Access Management component also prevent unauthorised, unchecked and unplanned changes occurring in production processes.

Identity based Management also creates a series of security chokepoints that act to allow better verification of identities and their access to the resources of the enterprise.

However, in order to properly implement an Identity based Management solution, an enterprise requires a framework that it can use to map its business needs and requirements against the requirements of the framework.

An *internal enterprise framework* can be defined as one that combines the identity administration of entities and their identities with identity based access management to control access to the resources of an enterprise [2]. The *internal enterprise framework* (Fig. 2) provides an enterprise with the assurance that it has an effective Identity based Management system that controls the creation of digital identities and their access to resources.

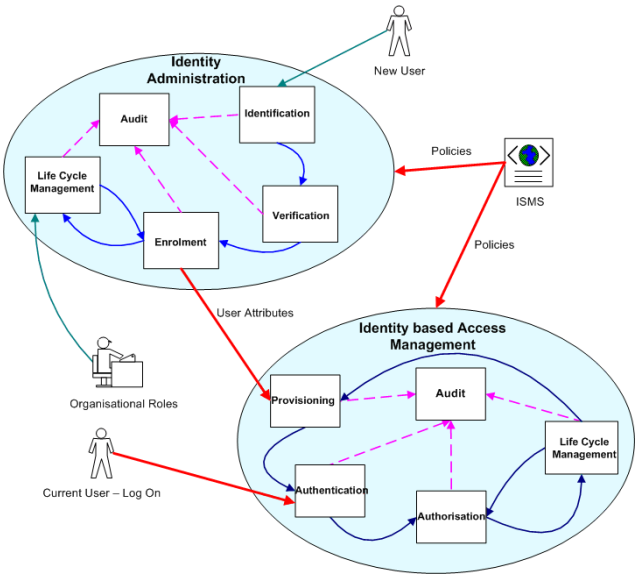

Figure 2: The Internal Enterprise Framework

The internal enterprise framework contains two major components — Identity Administration and Identity based Access Management. These two components each contain a number of processes that currently exist in an enterprise. The internal enterprise framework documents the processes to ensure consistent application and verifies that they are in accordance with the policies laid down in the ISMS. Although the framework is designed for implementation on a technology platform, it is really more concerned with process and process management than any particular technological implementation [2].

Identity Administration

Identity administration is the process of positively identifying an entity, determining the identifiers to be used by a digital identity and issuing credentials for future authentication by that identity. This process contains a number of components: identification, verification, enrolment, life-cycle management and audit.

Fig. 3 illustrates how the *identity administration* components interact. A new entity presents the formal identification documents required by the enterprise. The enterprise verifies the entity's identity according to its internal processes. When the identity has been verified, the entity's digital identity is created in the enrolment process and the appropriate authentication credentials are issued. The identity may also be assigned to an organisational role at this stage. The processes of identification and verification may well remain manual processes for many enterprises into the foreseeable future, despite the introduction of automated identity verification applications, particularly in the U.K.

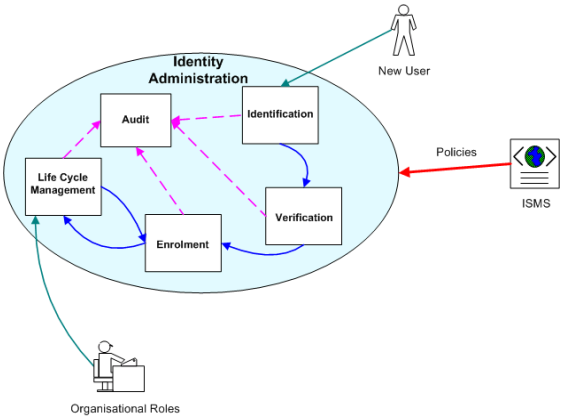

Figure 3: Identity Administration

Identity based Access Management

Identity based access Management is a set of processes that authenticate an identity that is claiming access and authorises access to certain resources while maintaining an audit trail of all authentication, access and use of resources. *Identity based access management* (Fig. 4) has a series of components: provisioning, authentication, authorisation, life-cycle management, change control and auditing.

Fig. 4 shows how the *identity based access management* components interact. A new entity's identity is initially passed to the Provisioning module for provisioning of the account. This includes creating email accounts, database accounts and any other accounts that are required for the entity's role in the enterprise. Provisioning may also include Single Sign On (SSO) arrangements where the entity's authentication credentials are also accepted by some or all enterprise applications.

When an entity attempts to logon to the system, they are initially authenticated through the enterprise's LDAP directory service. The authenticated identity is then authorised to access certain enterprise resources using the enterprise's access control method. However, these procedures must be in accordance with the

enterprise's ISMS (Fig. 4) and must provide an audit trail. Life-cycle management, which also includes change control, allows for any change of role for all entities in the system.

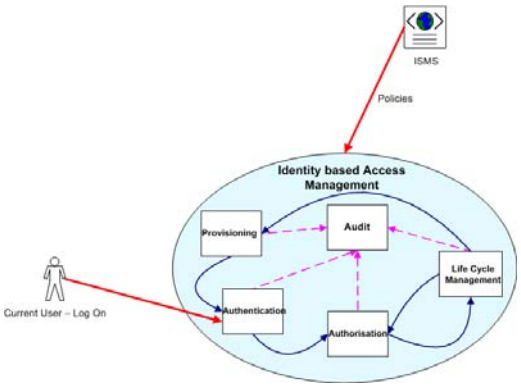

Figure 4: Identity based Access Management

Identity based Management using the Internal Enterprise Framework improves the security of the enterprise by creating a series of security chokepoints. The first chokepoint is created in the Enrolment process where all digital identities are created. This ensures that all employee, contractor and service identities that are created can now be verified. This chokepoint prevents the unauthorised creation of identities and provides an assurance to the business, as well as to external federation partners, that the organisation's identities are both valid and verifiable.

A second chokepoint is created in the Provisioning process where all identities are provisioned into the various systems and databases of the enterprise through this one process. This chokepoint prevents the unauthorised provisioning of identities into systems or databases. This acts to assure the business that only the correctly authorised identities have access to its strategic resources.

The final chokepoint occurs at the Authentication process where all identity claims are processed and authorised or rejected. This removes the requirement for different systems and databases to have their own authentication credentials and procedures. It allows a single, stronger system to be employed for all authentication, and reduces the chances of "back door" access being available in a strategic system [2].

Extending the ISMS

Information Exchange Agreement

Information Exchange Agreements between parties participating in a federation serve to create a trusted and legally binding contractual relationship between the participants. The creation of this contractual framework is critical to the success of the federation and will vary according to the needs of the enterprises. This discussion is not intended to offer any legal advice, inferred or otherwise.

Purpose of a Contractual Framework

It is a requirement of AS/NZS ISO/IEC 27001:2006, that external parties be managed to maintain the security of the enterprise's information assets. One way to achieve this is for all parties that participate in a federation establish a contractual framework that obligates all the parties to abide by certain requirements, rules, and solutions that will govern their ongoing relationship.

The purpose of these contractual agreements is to:

- describe the agreed rules, policies, obligations, procedures, risk mitigation, and solutions that will govern the (a) relationship among the participating organisations, (b) the administration of the federation, and (c) technical implementation of the defined and agreed specifications;
- act as a legal structure to the operational rules and technical standards implemented in the federated cluster;
- provide organisations with legally enforceable solutions in the event an organisation does not abide by the agreed upon rules, policies, obligations and procedures, and
- ensure the organisations ISMS meets the requirement s of AS/NZS ISO/IEC 27001:2006 section A.10.8 Exchange of information, section A.6.2 External parties, and section A.11.1 Business requirement for access control.

As part of the process of creating an IEA, an enterprise needs to consider the issues described below in addition to any unique issues that enterprise may have. These issues will have an impact on the TRA as the IEA is negotiated between two enterprises. The list presented below is not definitive and is offered as a starting point to facilitate the drafting of an IEA by identifying issues that stakeholders may need to consider. The list as presented is a combination of many authors' work; however, the major sources only are cited at the end of the list.

The major issues that must be considered in drafting an IEA are:

- **Purpose**. The IEA must state the overall purpose of the agreement. What are the services being offered? What service is offered by which enterprise? What data or information is being exchanged, and who is the recipient?
- **Terminology, Communication & Documentation**. What common terminology will be used to describe the participants, their federation, their relationship, their rights and obligations? How will the technical interface and other standards be established, communicated, and implemented? Who in each organisation has the responsibility for developing, documenting and accepting the security design and plan?
- **Trust, roles and obligations**. What is the behaviour expected by and from each system within the federation? Is each enterprise expected to protect the information belonging to the other through the implementation of an ISMS? What are each enterprise's roles, operational rights and obligations within the federation? Are these based solely on each enterprise's ISMS or do they arise out of a mutually recognized source such as legislation, mutually agreed best practice, etc?
- **Privacy, Security and Incident Reporting**. What are the privacy and security standards that apply to each enterprise and the federation? What are the system technical security services used to secure the federation? What is the procedure for responses and reporting of information security incidents? How will Confidentiality, Integrity, and Availability be assured for each organisation?
- **Confidentiality, Integrity and Availability**. How will Confidentiality, Integrity, and Availability be assured for each organisation? What level of confidentiality obligations should be imposed? What level of availability will be imposed or guaranteed?
- **Governance, Version Control, Change Management and Audit**. Who will be responsible for day-to-day governance of the federation? How will the parties communicate regarding operational issues that arise? How will changes to the rules, policies, and/or main contractual agreements be

approved and implemented? What audit/verification/certification rights should each participant have? What events will be monitored and how will these events be logged by each organisation?

- **Authentication**. How will authentication occur between enterprises? Is there an agreed framework that will be used to control the authentication of identities within each enterprise?
- **Enforcement**. How will the rules and policies be enforced? What dispute resolution mechanism will be used? What options or solutions will be available to the participants in the event that rules and policies are not followed?
- **Participation**. Under what circumstances may:
    - A new enterprise be added to the federation?
    - An existing enterprise terminate its involvement in the federation?
    - May the other enterprise(s) have an enterprise removed from the federation?
- **Service Levels**. What (if any) are the security obligations, responsibilities and liabilities for each enterprise? What are the minimum service levels that will apply? Will they be targets or minimum obligations? [8, 13-16]

The issues presented above would be the minimum that would need to be considered in drafting an IEA for an enterprise considering federation. Other issues, that are specific to the enterprise and the federation, would also need to be included in the IEA. This should also include the details of the authentication framework that is used to underpin connection to the federation. The use of Identity based Management using the Internal Enterprise Framework provides an enterprise with a number of additional security chokepoints. This should assure any federation partners that the enterprise can verify identities and correctly authorise their access to the resources of the federation. The possibility of a chain of trust issue is reduced when both parties to the IEA agree to use the Internal Enterprise Framework.

AS/NZS ISO/IEC 27001:2006 details the functional requirements for an enterprise's information security management system. It also details requirements for an enterprise's interaction with external parties, for third party service delivery and electronic commerce. These requirements must be reviewed as part of the IEA drafting process to ensure that the IEA covers all the requirements that are appropriate in AS/NZS ISO/IEC 27001:2006.

After drafting and reaching agreement on an IEA, it should be included in a new TRA and then incorporated in the enterprise's ISMS. The IEA will now form an integral and important part of the enterprise Security Management Architecture. The IEA, and its implications for the enterprise, must be considered as part of any security management architecture discussions and plans. The enterprise can no longer be considered in isolation, as it is now part of a federation community and it must now plan and act as a member of that community.

Advantages and Issues

The use of an IEA gives an enterprise a measure of certainty and security in its progress to federation. The act of drafting the IEA causes an enterprise to consider the risk implications of federation to their business and allows them to prepare for all

the issues involved in joining a federation. It allows the enterprise to enter the federation fully aware of the risks and opportunities that federation brings.

The IEA leverages off the existing ISMS of the enterprise. It allows the enterprise to consider the business needs that are the drivers for the federation in addition to the inherent risks involved in participating in a federation.

The proposed IEA will allow for clear understanding between all parties as it details the rights and obligations of each party. This includes: Trust, roles and obligations; Privacy and security; Incident reporting; Governance; Authentication; Change management; Enforcement; Participation, and Service Levels.

The IEA also provides an additional driver towards increased security as it has to consider the question of authentication. The IEA should specify an authentication framework that is acceptable to both parties. It is proposed that the *Internal Enterprise Framework* be used as the authentication framework. The internal enterprise framework is technology agnostic and will work with the existing enterprise authentication and access control system to assure federation partners that it has an identity based management system that can be verified and audited. It will reduce the possibility of chains of trust being created among federation partners. This will act to increase the level of trust between federation partners.

Not every enterprise may be happy to enter into an IEA for a federation. There may be issues with entering legal arrangements and/or with the maintenance of those arrangements. Some enterprises may not be willing to accept and implement an internal Identity based Management system, even though they may have a business need to join a federation. There is always the risk that a party to an IEA may not fulfil their obligations under the IEA therefore opening the other enterprise to risk.

Conclusion

A federation is created when an enterprise publishes some internal resources externally and allows other remote enterprises to consume those resources, using their individual internal authentication.

The use of Identity based Management and the Internal Enterprise Framework will enhance the internal security of an enterprise. The enterprise that intends to join a federation to further enhance its business objectives, will find that it needs to enter into a contractual agreement with the proposed federation partners. This agreement, an Information Exchange Agreement, should include agreed rules, policies, obligations, procedures, risk mitigation, and solutions. It should also include details of the authentication framework that will be used in the federation and any underlying framework. The Internal Enterprise Framework is recommended for inclusion in an IEA as a technology agnostic framework that will provide assurance that all identities and authentication can be verified and audited.

The IEA will now form an integral and important part of the enterprise Security Management Architecture. The IEA, and its implications for the enterprise, must be considered as part of any security management architecture discussions and plans. The enterprise can no longer be considered in isolation, as it is now part of a federation community and it must now plan and act as a member of that community.

Reference List

1 Casassa Mont M, Pearson S, Bramhall P. Towards Accountable Management of Privacy and Identity Information. *Lecture Notes in Computer Science*. 2003;2808:146-161.

2 White P, Altas I, Howarth J, Weckert J. An Internal Enterprise Framework for Identity based Management. Wagga Wagga, Australia: Charles Sturt University 2007.

3 Woodhouse S, Howarth J, Tien D. A management approach to securing geospatial information systems. In: Guangfan. S, Guanran. W, Tien. D, editors. Fourth International Conference on Information Technology and Applications ITCITA 2007; 2007; Harbin, China; 2007. p. 100-105.

4 Hawker A. Security and control in information systems: a guide for business and accounting. London: Routledge 2000.

5 Day K. Inside the Security Mind. Making the tough decisions. Upper Saddle River, NJ.: Prentice Hall 2003.

6 Wood P. Implementing identity management security - an ethical hackers view. Network Security. 2005:12-15.

7 Devargas. The total quality management approach to IT security. Oxford, UK: NCC Blackwell 1995.

8 McCumber. Assessing and managing security risk in IT systems: A structured methodology. USA: CRC Press LLC 2005.

9 Peltier TR, Peltier J, Blackley JA. Information security fundamentals: Auerbach 2003.

10 Calder A. A business guide to information security: how to protect your company's IT assets, reduce risks and understand the law London: Kogan Page Ltd 2005.

11 Proctor P, Byrnes FC. The secured enterprise: protecting your information assets Upper Saddle River, NJ, USA.: Prentice Hall 2002.

12 Calder A, Watkins S. IT governance: Data Security and BS 7799/ISO 17799 - A Manager's Guide to Effective Information Security. London: Kogan Page Ltd 2003.

13 Joint Standards Australia/Standards New Zealand Committee It ISSaIT, Standards New Zealand, Standards Australia. Information security risk management guidelines: HB 231:2000. 2000.

14 Sherwood J, Clark A, Lynas D. Enterprise Security Architecture: A business-Driven Approach. San Francisco, CA, USA: CMP Books 2005.

15 U. S. Customs. How Interconnection Security Agreements are used at the US Customs. Washington DC 2000.

16 Sheckler V. Liberty Alliance Contractual Framework Outline for Circles of Trust. Piscataway. NJ: Liberty Alliance Project 2007.