Global Information Assurance Certification Paper

Information Security Management System (7799) for an Internet Gateway

Amarottam Shrestha

GIAC Certified ISO-17799 Specialist Practical Assignment (Version 1.0)

24 June 2004

Table of Contents

Information Security Management System (7799) for an Internet Gateway

Amarottam Shrestha

Abstract:

The Internet presence is an important aspect most businesses these days. An Internet gateway provides network security for businesses from the Internet. It is important that the Internet gateway is designed, implemented and operated in a secure manner. The management of any organization would like to have some assurance on how the Internet gateway is operated. This paper develops an Information Security Management System (ISMS) to provide assurance that the Internet gateway meets the required security level to protect the Information resources of an organization's internal network. This paper uses a case study to demonstrate Plan Do Check Act (PDCA) process based on AS/NZS 7799:2:2003 Information Security Management to develop an ISMS.

1. Introduction

An Internet gateway is part of an organization's network, which provides "network border" security to the internal network from the Internet. It is critical to an organization's information security that the Internet gateway is designed and operated in a secure manner. In this paper, an organization with business requirements for an Internet connection is considered. The existing Internet gateway is studied and an ISMS is developed to acquire 7799 certification for the gateway. In the following sub-sections, a brief description of the organization and its network infrastructure is provided.

1.1 XYZ Association

XYZ Association is a membership association for professionals in Australia. The membership is open to individuals or organizations providing Civil Engineering consultancy service. The main objectives of the association is to:

- Promote civil engineering profession to general public.
- Provide networking opportunities to the members.
- Lobby government and other administrative bodies on behalf of the profession.
- Organise promotional conferences and exhibitions.
- Support members in their business endeavours.

The association has about 100 staff in different locations across the country. The head office of the association is located in Sydney and it has branch offices in all state and territory capitals. The association also has a few regional offices. The following table lists the number of staff in different locations and type of the office.

Table 1: XYZ Association office locations

Location	Number of Staff	Type of Office
Sydney	20	Head Office
Melbourne	15	Branch Office

Location	Number of Staff	Type of Office
Canberra	10	Branch Office
Adelaide	7	Branch Office
Brisbane	15	Branch Office
Darwin	7	Branch Office
Perth	10	Branch Office
Hobart	7	Branch Office
Coffs Harbour	3	Regional Office
New Castle	3	Regional Office
Gold Coast	3	Regional Office
Townsville	3	Regional Office

The association has more than 1000 members. The members are geographically spread across the country. The members either physically visit an office or visit the association's website for service. At the moment the association is working on its eBusiness initiative to provide most of the services online.

1.2 XYZ Association Network

There are 12 locations altogether. All of them are connected to each other via an ISP managed "virtual private network" across the ISP's routed network. As far as XYZ Association network is concerned, all of the complexity of the ISP routed network is hidden and the association network is numbered with private IP addresses (not routable in the Internet). Bandwidth between different locations varies depending upon expected demand.

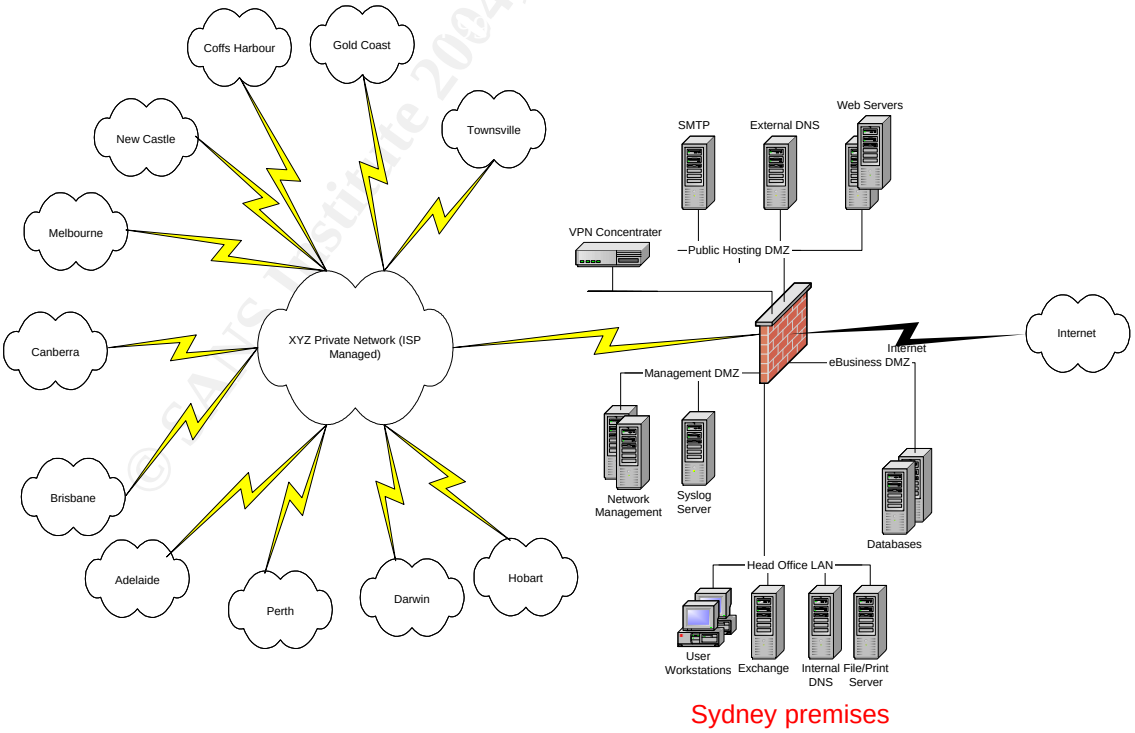

Figure 1: XYZ Association network

The internal network is based upon the Windows networking technology. Every location has its own file and print servers installed locally. All locations with 10 or more users have their own email server. For all other locations, the email server at the head office (Sydney) provides email service.

The office network is connected to the Internet via a gateway managed by the IT Department of the association. The Internet gateway is physically located in Association's Sydney premises. The staff at all locations have Internet browsing services available from their desktops. The staff also have email service available to them, which enables them to send and receive emails to and from the Internet. The association has several web servers hosted in the gateway. The association also provides limited "remote access" service for staff to "work from home" or while travelling.

The Internet gateway consists of a firewall and a number of DMZs (network security domains). The following is the DMZs and a brief description of their purpose (refer to figure 1):

1. *Internet* – The interface of the firewall is connected to the Internet.
2. *eBusiness DMZ* – databases for eBusiness applications are hosted in this DMZ. No direct connection from the Internet is permitted to this DMZ. Usually, the Internet facing web servers act as an intermediary between this DMZ and the Internet.
3. *Head office LAN* – this network interface is connected to the internal network at the head office. No access from the Internet is permitted to this segment. Limited access to the email servers or file sharing is permitted from other locations of the network.
4. *Management DMZ* – this DMZ hosts network and system management workstations including the central syslog server. Firewall logs are logged real time to the syslog server in this DMZ.
5. *XYZ association private network DMZ* – this network segment is connected to the ISP managed private network.
6. *Remote Access DMZ* – this segment has a VPN concentrator installed. The remote access VPNs from the Internet are terminated here.
7. *Public Hosting DMZ* – the public web servers accessible from the Internet are installed in this DMZ.

1.3 Scope for ISMS

The Internet gateway of the association is selected as the Information System for development of the ISMS. The Internet gateway is expected to provide security to the association's information resources in the internal network from the Internet. The Internet gateway is expected to provide security to the following services:

- Internet browsing from the association's internal network
- Internet email service
- Web hosting – this includes
  a. Public web servers with general information about the association,
  b. Member services, e.g. membership renewals,
  c. Members' hosting – eBusiness service for members, etc.
- Remote access service for staff from Internet based VPN

In strict terms, the following are **in scope** for this ISMS:

- IT & T infrastructure to provide Internet Gateway services to the XYZ Association. This includes, firewall, all servers hosted in the DMZs (except *Head office LAN,* and *XYZ association private network DMZ*), telecommunications link to the Internet, etc.
- Security of data on any system of XYZ Association from the Internet initiated network connections.
- Physical facility to host the Internet Gateway, for example, rooms, equipment racks, etc.
- IT Department staff directly or indirectly involved in the support the Internet Gateway.

The ISMS excludes other aspects of the network security of the internal network of the association from the scope. A separate ISMS should be developed for other aspects of the overall security of the XYZ network. Specifically, the following are **excluded** from the scope of this ISMS:

- *Head office LAN* and *XYZ association private network DMZs* of the firewall.
- Overall information security of the XYZ Association.
- Application level vulnerabilities in the systems used by XYZ Association.

1.4 Current state of security

The technical design and the security architecture of the Internet gateway under consideration seem to be reasonably well designed and documented. However, XYZ association does not have a formal (written) security policy for the organization. This includes the Internet gateway of the organization.

System administrators maintain and operate the Internet gateway in an ad-hoc basis. There are hardly any written plans and procedures for the operation of the gateway.

There are two written policies for acceptable use of the Internet browsing and the Internet email for the staff.

2. Plan Phase

This part of the paper discusses the plan for developing the ISMS. It starts with the steps (methodology) required for ISMS development and further goes on to assess the risk, develop an ISMS management structure and security policy for the Internet gateway.

2.1 Steps used for the ISMS development

The ISMS development process is driven by a risk assessment. The risk assessment will identify the main risks involved in operating the gateway in a secure manner. Once the risks are identified, controls to mitigate the risks can be selected. Based upon the outcome of the risk assessment, a security policy and management structure for the ISMS will be developed.

The following are the main steps used to develop the ISMS for the Internet gateway.

- Project Plan
- Risk Assessment
- ISMS Management Structure based upon risk assessment
- Security policy, plans and procedure development based upon risk assessment

In the following sub sections each of these steps are elaborated.

2.1.1 Step 1: Project plan

A project plan for development of an ISMS for the Internet Gateway of XYZ Association should be prepared before the project initiates. This process shall involve identification of the stakeholders, approval from the sponsors and support from the management of the Association. The project plan should consists, at least, the following details:

- Work Breakdown Structure (WBS) of the project
- Stakeholders or the resources required to conduct the work identified in the WBS
- Expected start and end dates (i.e. proposed timeline) for each of the items identified in the WBS
- Project risks
- Approval of the project plan from the XYZ Association Management

2.1.2 Step 2: Risk assessment and management

"Risk is the possibility of something damaging happening (Harris, p. 72)."
The Risk Assessment is a process to identify the risks and assess the damage it could cause. The end result of a risk assessment is justification of any control or safeguards that need to be implemented to mitigate the risk to an acceptable level. The process of selecting controls or countermeasures will complete the Risk Management process. For the development of the ISMS, the risk management methodology used is based upon the Australian and New Zealand Standard (AS/NZS 4360). The following diagram (Figure 2) shows the risk management overview and is directly quoted from the standard (AS/NZS 4360:1999).

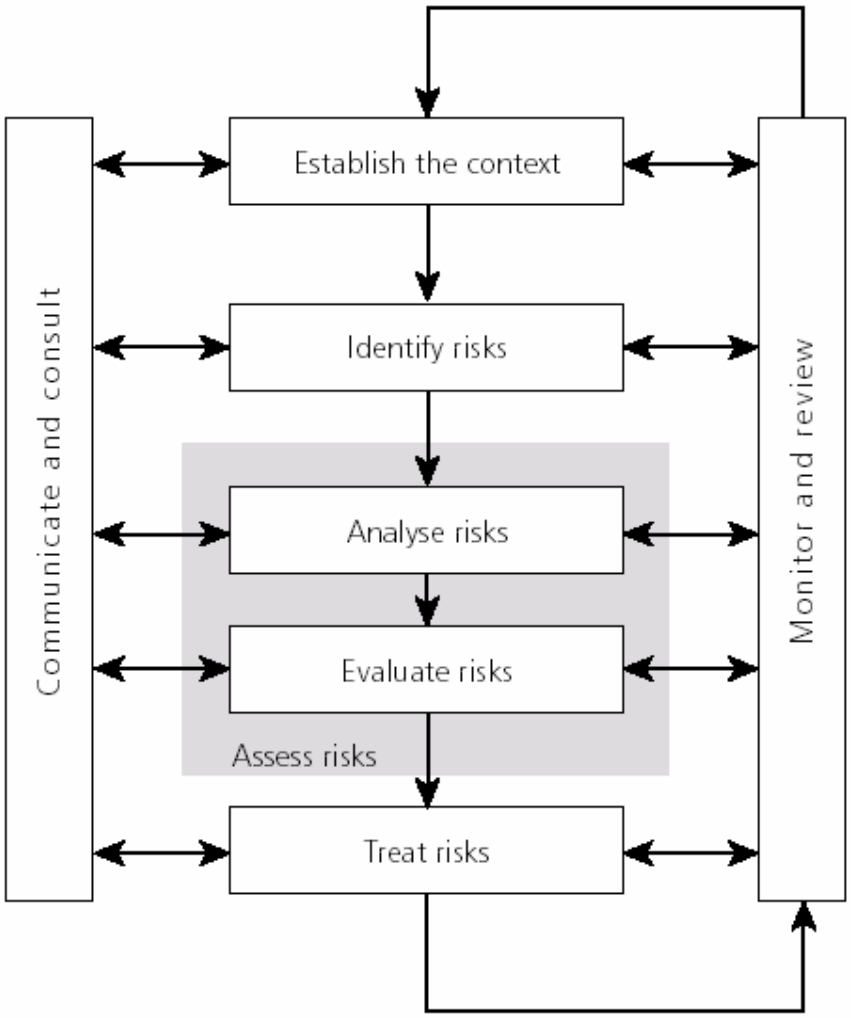

Figure 2: Risk Management Overview (AS/NZS 4360:1999)

The steps for the risk assessment is adapted from the AS/NZS 4360:1999 and are described below:

2.1.2.1 Establish context (Identify asset)

Establishing the context of the risk assessment includes determining the relationship and setting assessment criteria. This section provides the background information required to conduct the assessment.

Assets are integral to the risk assessment process. Security risk assessments are based on protecting an asset or a multitude of assets. When determining the assets, the organization must detail the criticality or value of an asset. For a physical asset (e.g. server) the value of the asset could be determined at the replacement cost, but there are a variety of other factors that need to be considered including, cost of unavailability of service provided and loss of reputation or goodwill, etc. It is important that all costs / values are considered.

Setting the risk evaluation criteria is integral to the process. The criteria should be set to ensure that it meets XYZ Association's expectations. Risk management

practitioners generally suggest that risks assessed as “Low” do not require immediate attention; therefore if the criteria are not set correctly the risk results will be skewed. The XYZ Association Management should determine what is an acceptable level of risk. For IT&T systems identified as an asset, further reference to Confidentiality, Integrity and Availability of the assets are considered while identifying risks against the assets.

For the purpose of this risk assessment, risk level of “Low” is considered acceptable to the XYZ Association and any risk level “Medium” or higher will require treatment to mitigate it to an acceptable level.

2.1.2.2 Risk Identification

Risk identification is the determination of threats and vulnerabilities that could lead to an adverse event. The focus is on the nature and source of the risk such as:

- What could happen or go wrong?
- How could it happen?
- Why can it happen?
- Who or what can be harmed?

The risks identified during this assessment are given in the risk register (section 2.2).

2.1.2.3 Risk Analysis

Once the risk against any asset is identified, the risk is analysed based upon two factors, namely, likelihood of risk materializing and the Consequence of risk materialization to the XYZ Association. The following tables detail the criteria used during this assessment.

Table 2: Likelihood Criteria (Qualitative Measure)

Level	Description
Negligible	Unlikely to occur.
Very Low	Likely to occur two/three times every five years
Low	Likely to occur once every year or less
Medium	Likely to occur once every six months or less
High	Likely to occur once every month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times per day

Table 3: Consequence Criteria (Qualitative Measure)

Level	Description
Insignificant	Will have almost no impact if threat is realised
Minor	Will have some minor effect on the asset value. Will not require any extra effort to repair or reconfigure gateway.
Significant	Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals. May result in compromise of limited amount of hosted data. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of the association, and/or notable loss of confidence in the gateway resources or services. Will require expenditure of significant resources to repair.

Serious	May cause extended gateway outage, and/or loss of business confidence by partners/members. May result in compromise of large amounts of hosted data.
Grave	Compromise of Association's sensitive data in the internal network causing permanent damage to Association's reputation. May cause permanent closure of Association's eBusiness initiative.

The risk evaluation criteria are used as a guide to enable decisions to be made on risk treatment options. The table below defines the risk evaluation criteria used in this assessment.

Table 4: Risk Evaluation Criteria

Threat Likelihood	Consequence					
	Insignificant	**Minor**	**Significant**	**Damaging**	**Serious**	**Grave**
Negligible	Nil	Nil	Nil	Nil	Nil	Nil
Very Low	Nil	Low	Low	Low	Medium	Medium
Low	Nil	Low	Medium	Medium	High	High
Medium	Nil	Low	Medium	High	High	Critical
High	Nil	Medium	High	High	Critical	Extreme
Very High	Nil	Medium	High	Critical	Extreme	Extreme
Extreme	Nil	Medium	High	Critical	Extreme	Extreme

2.1.2.4 Risk Evaluation and Treatment

Results from the risk analysis will be a list of security risks to the Association's gateway. The risk will range from *Nil* to *Extreme*. This should be compared against the acceptable risk determined by the XYZ Association Management in the establish context and scoping phase of the assessment. Only the risks that are identified as unacceptable should be assessed in the next phase.

Determining the priority that risks should be treated are based on the formula:

Risk Level Rating - ***Acceptable Risk Level Rating*** = ***Priority rating***

The following numerical values are applied for risk rating:

Table 5: Risk Rating

Level	Numerical Value
Nil	0
Low	1
Medium	2
High	3
Critical	4
Extreme	5

Once the priority rating is determined, the next step is to implement controls identified in the risk assessment to mitigate (treat) the risk to an acceptable level.

2.1.3 Step 3: Management structure development and approvals

The Management structure for the ISMS shall be driven by the risk assessment. The objectives for defining a management structure for XYZ Association's Internet Gateway ISMS are the following:

- To demonstrate management commitment to the ISMS.
- To demonstrate that the management structure enforces the principle of "separation of duties" in the gateway operations.

For development of ISMS for XYZ Association's Internet gateway, a management structure is required which demonstrates upper management's commitment to Security in general and specifically the security of the Internet gateway. It is also important that "separation of duties" is implemented to ensure that a single individual or a team is not able to compromise the security of the gateway without another person or team becoming aware of the compromise. This, in itself, will act as a control for secure operation of the gateway. The management structure developed for XYZ Association's Internet Gateway is presented in section 2.3, below.

2.1.4 Step 4: Security Policy, Standards and procedures development

Again, risk assessment should drive the Security Policy development for the XYZ Association's Internet Gateway. Security Policy should address the following areas:

- Gateway access policy
- Physical security policy
- Personnel security policy
- System access policy
- Configuration control policy
- Change management policy
- Incident detection and response policy
- Contingency policy
- Acceptable user policy

The security policy should address only the high level principles that need to be followed for secure operation of the gateway. However, most of the areas identified above shall be supported by lower level procedure and plan documents. Details on these are given in section 2.4, below.

2.2 Risk Assessment and Management

The assessment methodology used for this ISMS development is adapted from AS/NZS 4360, as described in section 2.1.2, above. This section discusses the actual risk assessment process for the Internet Gateway of XYZ Association and lists the important risks in a risk register.

The main assets for the Internet Gateway are identified as follows:

- **XYZ Association's Internet services** – Availability, confidentiality and Integrity of Internet browsing, Internet email, web hosting and remote access services.
- **Internet Gateway Infrastructure** – Availability, Integrity and Confidentiality of the computer systems, the network and server infrastructure, the management network, the physical facility, etc.
- **XYZ Association's Data** – Confidentiality, Integrity and Availability of data in the internal network.

The risk register in Table 6 lists some important risks against the assets identified above. The risk register is presented as an example and does not include all possible risks.

In the risk register, "Resultant Risk" is calculated with the assumption that there is no "control" or "countermeasure" implemented. The "required risk" is the level of risk that the XYZ Association is willing to accept. The countermeasure recommendation column in the risk register lists the "controls" that need to be implemented to bring the risk to the acceptable level. The controls are taken from the standard (AS/NZS 7799.2:2003). It's possible that some the controls are already implemented.

Table 6: Risk Register

Risk ID	Asset Identification	Threat to the Asset	Threat Likelihood Estimate	Consequence, if the threat is realised	Resultant Risk Level	Required Threat Likelihood	Required Consequence, if threat is realised	Required Risk	Countermeasure(s) Priority	Countermeasure(s) Recommendation based on AS/NZS 7799.2
1	XYZ Association's Internet services -- Availability	Critical network device (e.g. router, firewall, etc.) failure	Low	Significant	Medium	Very Low	Significant	Low	1	A.7.2.1 Equipment siting and protection A.7.2.2 Power supplies A.7.2.4 Equipment maintenance A.8.1.3 Incident management procedures A.8.2.1 Capacity planning A.8.2.2 System acceptance A.8.5.1 Network controls A.11.1.1 Business continuity management process A.11.1.2 Business continuity and impact analysis A.11.1.3 Writing and implementing continuity plans A.11.1.4 Business continuity planning framework A.11.1.5 Testing, maintaining and re-assessing business continuity plans
2	XYZ Association's Internet services -- Availability	Denial of Service attack from Internet	Very High	Significant	High	Very Low	Minor	Low	2	A.6.3.1 Reporting security incidents A.6.3.2 Reporting security weaknesses A.6.3.3 Reporting software malfunctions A.6.3.4 Learning from incidents A.8.1.3 Incident management procedures A.8.3.1 Controls against malicious software A.8.5.1 Network controls A.9.7.1 Event logging A.9.7.2 Monitoring system use A.9.7.3 Clock synchronization A.11.1.1 Business continuity management process A.11.1.2 Business continuity and impact analysis A.11.1.3 Writing and implementing continuity plans A.11.1.4 Business continuity planning framework A.11.1.5 Testing, maintaining and re-assessing business continuity plans
3	XYZ Association's Data - Integrity	Compromised network security by hackers from the Internet	Low	Serious	High	Negligible	Damaging	Nil	3	A.6.3.1 Reporting security incidents A.6.3.2 Reporting security weaknesses A.6.3.3 Reporting software malfunctions A.6.3.4 Learning from incidents A.8.1.3 Incident management procedures A.8.3.1 Controls against malicious software A.8.5.1 Network controls A.9.7.1 Event logging A.9.7.2 Monitoring system use

Risk ID	Asset Identification	Threat to the Asset	Threat Likelihood Estimate	Consequence, if the threat is realised	Resultant Risk Level	Required Threat Likelihood	Required Consequence, if threat is realised	Required Risk	Countermeasure(s) Priority	Countermeasure(s) Recommendation based on AS/NZS 7799.2
										A.9.7.3 Clock synchronization
4	XYZ Association's Data - Confidentiality	Compromised network security by hackers from the Internet	**Medium**	**Damaging**	**High**	**Negligible**	**Significant**	**Nil**	3	A.6.3.1 Reporting security incidents A.6.3.2 Reporting security weaknesses A.6.3.3 Reporting software malfunctions A.6.3.4 Learning from incidents A.8.1.3 Incident management procedures A.8.3.1 Controls against malicious software A.8.5.1 Network controls A.9.7.1 Event logging A.9.7.2 Monitoring system use A.9.7.3 Clock synchronization
5	Internet Gateway Infrastructure - Integrity	Accidental misconfiguration of the security enforcing device	**Low**	**Damaging**	**Medium**	**Negligible**	**Significant**	**Nil**	2	A.6.3.1 Reporting security incidents A.6.3.2 Reporting security weaknesses A.6.3.3 Reporting software malfunctions A.6.3.4 Learning from incidents A.8.1.2 Operational change controls A.8.1.3 Incident management procedures A.8.1.5 Separation of development and operational facilities A.8.4.1 Information back-up A.8.4.2 Operator logs A.8.4.3 Fault logging A.9.7.1 Event logging A.9.7.2 Monitoring system use A.9.7.3 Clock synchronization

2.3 ISMS Management Structure

The following organizational structure (Figure 3) represents the ISMS Management Structure for the Internet Gateway of XYZ Association. The Chief Executive Officer (CEO) of the Association is ultimately responsible for secure operation of the Internet Gateway. Therefore, it is most appropriate for the CEO to head the ISMS Management Committee to demonstrate senior management's commitment to the security of the system. As XYZ Association is a small organization with around 100 staff, it is justifiable for the CEO to get directly involved in this process.

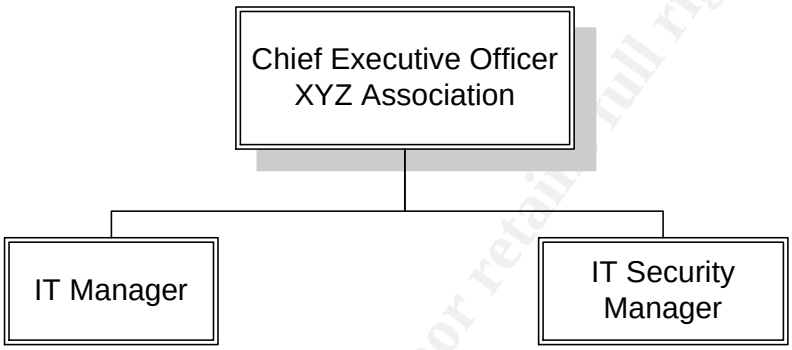

Figure 3: ISMS Management Structure

The IT Manager of the Association is responsible for secure operation of the Internet Gateway. All of the operational staff, for example, System Administrators, report directly to the IT Manager. The IT Security Manger is responsible for enforcing security policy, compliance, auditing and incident response activities. This structure ensures that operational staff will not easily be able to circumvent security for convenience in operations or additional functionality against the security policy.

2.4 Security Policy

In the following sub sections, a short descriptions of the policies identified in the section 2.1.4 are presented. The description is provided in the following format:

a. Purpose of the policy
b. Intended Audience of the policy
c. Areas of the standard (AS/NZS 7799.2) covered by the policy

2.4.1 Gateway access policy

Purpose: The purpose of the policy is to ensure that uncontrolled access to the XYZ Association internal network and the DMZs from the Internet is prevented. It also ensures that only controlled access from the association's internal network to the Internet and DMZs is permitted. This policy should detail at a high level the type of service (protocol) permitted by the gateway.

Intended Audience: The policy is intended for the staff managing the gateway. Certain relevant extracts from this policy should be included in the general staff awareness program.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.9.1.1 Access control policy
- A.9.4.1 Policy on use of network Services

2.4.2 Physical security policy

Purpose: Physical security is an integral part of the overall security of the Internet Gateway and the internal network protected by the gateway. The purpose of this policy is to ensure that the physical security meets industry standards and is maintained during operation. This policy shall cover areas of physical access control, environment control, locks, equipment rack, etc.

Intended Audience: This policy is intended for all staff of the Association and shall be enforced to visitors as well.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.7.1 Secure areas

2.4.3 Personnel security policy

Purpose: The objective of the personnel security policy is "to reduce the risks of human error, theft, fraud or misuse of facilities" (AS/NZS 7799.2:2003, p.18). This policy should cover personnel vetting, training, security incident response, etc.

Intended Audience: This policy is intended for all the staff of the Association who will be served by the Internet Gateway.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.6 Personnel security

2.4.4 System access policy

Purpose: The intention of this policy is to ensure that only authorized personnel have access to systems based upon "need to know" and "least privilege" principle.

Need to know principle ensures that only people who have a need to access information or resource are authorised to do so. Authorisation could be for a limited time period and the need is based upon business requirement, not because someone desires so.

Least privilege principle ensures that minimum required access is granted. For example, system operator can read the logs but cannot change or delete.

Intended Audience: The policy is intended for the staff managing the gateway.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.9.1 Business requirement for access control

- A.9.2 User access management

2.4.5 Change and Configuration control policy

Purpose: The intention of these policies is to prevent errors in configurations of critical devices in the gateway by implementing proper configuration control procedure and ensure that all changes to the infrastructure is approved by all stakeholders. It is also important that all changes are appropriately documented.

Intended Audience: The policy is intended for the staff managing the gateway.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.8.1.2 Operational change controls

2.4.6 Incident detection and response policy

Purpose: Information security systems do not work perfectly all the time. Sometimes there are positive and negative events. It is necessary to document and analyse those events to determine the impact and what changes or corrective actions may be necessary.

Incident management responsibilities and procedures must be established and tested to ensure a quick, effective and orderly response to security incidents. A security incident is a situation where evidence of unauthorised access, modification, or destruction of the Internet Gateway IT resource is detected. This policy is invoked when any security incident is discovered.

Intended Audience: The policy is intended for the staff managing the gateway.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.8.1.3 Incident management procedures
- A.6.3 Responding to security incidents and malfunctions

2.4.7 Contingency policy

Purpose: An incident is any event (either internal, external, deliberate or accidental) that could adversely affect the confidentiality, integrity or availability of the Internet Gateway and the internal network protected by the gateway. Some of the incidents can lead to outage. Events like power failure, Denial of Service attack, hardware or software failure, communications link failure, natural calamities, etc. are examples of such incidents.

The purpose of this policy is to investigate and mitigate the affects of these types of incidents. Other security incidents are dealt with in “Incident Detection and Response Policy”.

Intended Audience: The policy is intended for the staff managing the gateway.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.11.1 Aspects of business continuity management

- A.6.3 Responding to security incidents and malfunctions

2.4.8 Acceptable use policy

Purpose: The objective of this policy is to ensure that users of the Internet Gateway are aware of their responsibilities.

Intended Audience: This policy is intended for all staff of the XYZ Association who will need access to Internet.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.6.2 User training
- A.9.3 User responsibilities
- A.6.3 Responding to security incidents and malfunctions

3. Do Phase

In this section, implementation of the ISMS is discussed. In section 2, requirements for an ISMS are developed. A gap analysis is conducted with the current state of the Internet Gateway and the requirements developed. Outcome of this process is a list of gaps that need to be bridged to arrive at the stage where the Internet Gateway is ready to achieve a 7799 certification. In the following paragraph, each "gap" is presented as a "Problem" in current implementation of the Internet Gateway. Then "action" required to remedy the problem and "steps" required to implement the action are discussed.

3.1 Problem – no ISMS Management structure

The XYZ Association Internet Gateway does not currently have an ISMS Management structure in place. The impact of this is the ISMS development process cannot formally progress.

3.1.1 Action

To remedy this problem, an ISMS Management structure shall be formally formed and brought into action to progress with the ISMS development.

3.1.2 Steps

1. The ISMS Management structure proposed above (section 2.3) should be presented to the XYZ Association CEO.
2. Achieve approval of the ISMS Management structure from the CEO.
3. Inform committee members and formalize ISMS Management structure.

3.2 Problem –Security policy not documented

The XYZ Association Internet Gateway does not have a documented policy, procedure and guidelines. The gateway operation is based upon ad-hoc processes, which vary from person to person.

3.2.1 Action

The policies identified in the planning phase (section 2.4) shall be developed and implemented.

3.2.2 Steps

1. For every identified policy, write policy statements.
2. For every identified policy, write explanations on the intent of these policy statements.
3. For every identified policy, write relevant reference documents on which the policy is based, this could include risk assessment, industry standards, etc. The purpose is to explain the link between the policy and why the policy is implemented.
4. For every policy documented, identify need for lower level procedure, plan or guideline documents.
5. Write all identified procedure, plan or guideline documents.

3.3 Problem – Network intrusion monitoring not implemented

The risk assessment has identified a need for a control to monitor network intrusions. In the current state, there is no network intrusion monitoring taking place in the Internet Gateway of XYZ Association.

3.3.1 Action

To address the problem, a Network Intrusion Detection System (NIDS) shall be implemented and processes for monitoring should be developed and implemented.

3.3.2 Steps

1. Engage designers to develop a NIDS solution for the Internet Gateway.
2. Purchase required equipment (hardware and software).
3. Install the NIDS.
4. Develop a procedure for operation and monitoring of the NIDS and document it.
5. Train monitoring staff.
6. Include inputs from NIDS to the “Incident Detection and Response Plan”.

3.4 Problem – Formal configuration management plan does not exist

The Internet Gateway of XYZ Association does not have a formal Configuration Management Plan. Impact of this could be accidental misconfigurations of the devices including the security enforcing devices like firewalls. This could contribute to a serious security breach.

3.4.1 Action

Develop and implement a Configuration Management Plan.

3.4.2 Steps

1. Write the Configuration Management Plan for XYZ Association Internet Gateway operations.
2. Identify required infrastructure (hardware and software) to implement the Configuration Management Plan.
3. Purchase/acquire required infrastructure and install them.
4. Train all support staff on procedure of configuration control.
5. Implement the Configuration Management Plan.

3.5 Problem –Formal change management plan does not exist

The Internet Gateway of XYZ Association does not have a formal Change Management Plan. Impact of this could be undocumented change not compliant with the security architecture due to lack of proper review process for infrastructure changes. This could contribute to serious security breaches.

3.5.1 Action

Develop and implement a Change Management Plan.

3.5.2 Steps

1. Write the Change Management Plan for XYZ Association Internet Gateway operations.
2. Identify required infrastructure (hardware and software) to implement the Change Management Plan.
3. Purchase/acquire required infrastructure and install them.
4. Train all support staff involved in infrastructure change on procedure of change control.
5. Implement the Change Management Plan.

3.6 Problem –Backup and Restore system not implemented

The Internet Gateway of XYZ Association does not have a Backup and Restore system. Lack of a backup system could result in data loss. It will impact on recovery time if a device failure forces the rebuild of a device from scratch. It will also have an impact on the configuration management of devices, in case any planned change needs to be rolled back due to unforeseen technical issues.

3.6.1 Action

Develop a backup and restore plan and implement it.

3.6.2 Steps

1. Develop a Backup and Restore Plan.
2. Complete a technical design for a back and restore system.
3. Acquire infrastructure (hardware and software) required to implement the technical solution.
4. Implement technical solution.
5. Train support staff involved in the backup and restore procedure
6. Backup the systems as per plan.
7. Conduct periodic tests to confirm that backup media is not corrupted or damaged.

3.7 Statement of applicability

The “Statement of Applicability” is the “document describing the control objectives and controls that are relevant and applicable to the organization’s ISMS, based on the results and conclusions of the risk assessment and risk treatment processes” (AS/NZS 7799.2:2003, p. 4). This document also records exclusion of any control objectives and controls listed in Annex A of the standard and reason for their exclusion.

In this section, as examples, two controls are selected from the Annex A of the standard and example "Statement of Applicability" is prepared for these two controls. For demonstration purpose, one of the selected controls is not applicable to the current ISMS implementation.

A.8.2 System planning and acceptance			
Control objective: To minimize the risk of systems failure.			
Controls			
A.8.2.1	Capacity planning	Capacity demands shall be monitored and projections of future capacity requirements made to enable adequate processing power and storage to be made available.	**Applicable**
Explanation: This control is implemented for the ISMS as it was a recommended "countermeasure" for Risk No. 1 & 2 in the risk register (section 2.2). Threats to "Availability of XYZ Association's Internet services" are noted as a failure of critical device or overloading of a critical device due to deliberate Denial of Service (DoS) attack from the Internet. This control will ensure that the capacity of the device is considered during initial design phase and continuously monitored for its resource utilization. This control, once implemented, will reduce the chance of device failure due to overloading of the devices.			

A.9.5 Operating system access control			
Control objective: To prevent unauthorized computer access.			
Controls			
A.9.5.1	Automatic terminal identification	Automatic terminal identification shall be considered to authenticate connections to specific locations and to portable equipment.	**Not Applicable**
Explanation: This control is not applicable to the Internet Gateway. By definition, any connections from the Internet are untrusted and only specific connections are permitted. Therefore, "automatic terminal identification" is against the overall objective of the Internet Gateway's requirement of filtering every connection and allowing only specific connections.			

4. Check Phase

"The Check activity is designed to ensure that the controls are working effectively and as intended, and that the ISMS remains effective" (AS/NZS 7799.2:2003, p. 35). For an effective check or audit activity, a relevant checklist with sufficient details should be prepared. In this section, an audit checklist for the XYZ Association's Internet Gateway is prepared. In the following section 4.1, relevant audit items for the Internet Gateway are identified. For each audit, control objective of the countermeasure that is being audited and its importance to XYZ Association is discussed. Further, steps taken for carrying out audit and frequency of audit is also listed.

4.1 Audit Checklist

No	Audit Description	Control Objective (as per AS/NZS 7799.2:2003)	Reason for Audit	Steps for Audit	Frequency
1	"Inventory of Assets" audit.	(A.5.1) To maintain appropriate protection of organizational assets.	It is necessary to ensure that software licence and hardware appliance versions are up to date to maintain "patches" to a secure level. Therefore, the Inventory of assets shall always be current.	1. Get "Inventory List" from the IT Manger. 2. Randomly select some devices (around 10% of the list). 3. Verify currency of the list by physically sighting the device.	Bi-annual
2	Personnel security audit	(A.6.1) To reduce the risks of human error, theft, fraud or misuse of facilities.	The Internet Gateway operations involve "sensitive" information such as firewall rules, emails in transit, etc. It is important that all support staffs are properly screened and confidentiality agreement is signed.	1. Get the list of support staff. 2. Verify staff screening results are filed for all relevant staff. 3. Sight executed "Confidentiality Agreement" between the staff and XYZ Association.	Annual
		(A.6.2) To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work. (A.6.3) To minimize the damage from security incidents and malfunctions, and to such incidents.	The support personnel should be aware of sensitivity of information, steps to be taken when an incident takes place, etc.	1. Sight staff's signed acknowledgement of receiving the "security brief" and annual refresher.	Annual
3	Physical security audit	(A.7.1) To prevent unauthorized physical access, damage and	The Internet Gateway is housed in a secure room and the security enforcing devices are installed in	1. Access logs of Electronic Access Control System (EACS).	Every quarter

No	Audit Description	Control Objective (as per AS/NZS 7799.2:2003)	Reason for Audit	Steps for Audit	Frequency
		interference to business premises and information. (A.7.2) To prevent loss, damage or compromise of assets and interruption to business activities.	locked up racks. It is important that implemented physical security mechanism is enforced all the time.	2. Verify percentage of failed access is not unusual (more than 10% of overall accesses). 3. Audit physical visitors logbook is up to date by random entry checking. 4. Audit equipment rack access physical log is up to date by random entry checking.	
4	Operational Procedures audit – change management plan, incident management plan	(A.8.1) To ensure the correct and secure operation of information processing facilities.	It is important for the Internet Gateway to have documented operational procedures. It is even more important to make sure that those procedures are followed.	1. Acquire change control records. Verify they are recorded as per plan. 2. Acquire incident response records and verify they are filled up as per plan.	Bi-annual
5	Anti virus application log and signature file audit	(A.8.3) To protect the integrity of software and information from damage by malicious software.	The threat of malicious software is real. It is very relevant to the gateway operations. There are virus scanning solutions implemented to detect malicious code. It is important to verify that they are working properly and when an event of malicious software is detected, it does not go unnoticed.	1. Execute command to check the virus signature version. 2. Verify that the version is up to date. 3. Access virus scanner logs and verify detected viruses are cleaned or appropriately quarantined and alert sent to monitors.	Daily
6	Backup and Restore audit	(A.8.4) To maintain the integrity and availability of information processing and communication services.	Backup system is integral to secure operation of the Internet Gateway. It is important and necessary that backup system operates regularly and backed up media is usable.	1. Access backup system logs and verify that backup takes place regularly and successfully. 2. Verify backup tapes are labelled properly by random checking. 3. Verify tapes are usable by executing a restore function	Bi-annual

No	Audit Description	Control Objective (as per AS/NZS 7799.2:2003)	Reason for Audit	Steps for Audit	Frequency
				in a “test system”.	
7	User system access audit	(A.9.2) To ensure that access rights to information systems are appropriately authorized, allocated and maintained.	It is important for the secure operations of the Internet Gateway that access to any system is controlled. A formal authorisation process should be in place. Many times user accounts of former employees remain in the system.	1. Acquire list of authorised users from the formal record of authorisation process. 2. Verify users in the system and their access levels are as per documentation. 3. This test shall be repeated for all multi-user systems in the gateway environment.	Bi-annual
8	Firewall rule audit	(A.9.4) Protection of networked services.	Firewall rules play vital role in controlling access to and from the Internet to different DMZs of the XYZ Association firewall. It is important that the rules match the approved business requirement of the association.	1. Acquired list of business requirement for network access. 2. Download firewall rules from the live system. 3. Verify that firewall rules match the documented business requirement.	Every quarter
9	Intrusion Detection System (IDS) log audit	(A.9.7) To detect unauthorized activities.	Network IDS is the key monitoring tool implemented in the Internet Gateway. It is important that the logs are analysed on a regular basis.	1. Access online IDS log. 2. Check for interesting events, successful or unsuccessful intrusions.	Daily
10	Firewall log audit		Firewall is the main network traffic filtering device in the Internet Gateway. It is important to check the logs regularly to find out about permitted or blocked traffic to ensure that the gateway access policy is enforced.	1. Access online firewall log. 2. Check for blocked traffic and analyse the traffic pattern. 3. Check for permitted traffic and randomly verify that they are as per documented access policy.	Daily
11	System Logs audit		System logs (syslogs) from all the servers are collected in a central syslog server. It is important to analyse system logs to detect any unusual activity in the network.	1. Access logs in central syslog server. 2. Execute scripts from the log analysis tool to detect anomalies.	Daily

No	Audit Description	Control Objective (as per AS/NZS 7799.2:2003)	Reason for Audit	Steps for Audit	Frequency
12	Network Management System Alerts	(A.8.5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.	Network Management Systems are used to continuously poll network devices and servers for their availability and performance measurements (e.g. memory and CPU utilization). It is important that alerts for this system is dealt with appropriately to ensure good health of the Internet Gateway.	1. Access management console 2. Look for alerts.	Daily, continuos monitoring
13	Operating System (OS) and Application Patch level audit	(A.8.3) To protect the integrity of software and information from damage by malicious software.	OS and application vulnerability is one of the most used exploitation by the hackers. Maintaining the patches of these systems to a secure level is essential for secure operation of the Internet Gateway.	1. Access the documented secure patch level for every system. 2. Verify patch level of all the system by accessing system and typing appropriate commands.	Bi-annual

5. Act Phase

This section of the paper describes how the ISMS for XYZ Association's Internet Gateway should be maintained and improved. In the Check phase of the ISMS development, a number of audit requirements were identified for the ISMS. These audits will be used to detect nonconformity in the ISMS. Nonconformity, according to the standard (AS/NZS 7799.2:2003, p. 37), means

a. the absence of, or the failure to implement and maintain one or more ISMS requirements; or
b. a situation which would, on the basis of available objective evidence, raise significant doubt as to the capability of the ISMS to fulfil the information security policy and security objectives of the organization.

Once a nonconformity is detected, corrective or preventive actions should be taken to eliminate the cause of the nonconformity, resulting in an improved ISMS. In the following sub section, possible nonconformities that could be detected by the designed audits and possible corrective or preventive actions required to eliminate the nonconformity is presented.

5.1 Nonconformity detection and corrective/preventive actions

In section 4.1, checklists for 13 audits are listed. These audits shall be carried out at the frequency recommended in the list. These audits are designed to detect the nonconformities in the ISMS. The following table lists possible nonconformities that the audits could detect and possible corrective or preventive actions to eliminate the nonconformity. The recommendations given here should be taken as guidelines only, actual action should be decided after careful study of the detected nonconformity.

No	*Audit Description*	*Possible Nonconformity*	*Possible Corrective / Preventive action*
1	"Inventory of Assets" audit.	Inventory list is incomplete or erroneous.	a. Correct the list. b. Train staff to ensure inventory control procedure is followed.
2	Personnel security audit	Insufficient evidence of staff screening.	a. Complete staff screening. b. Train staff to ensure screening process is followed while recruiting.
		"Confidentiality Agreement" not signed.	a. Sign "Confidentiality Agreement". b. Ensure the process is followed properly in future.
		Security Brief not completed.	a. Complete the security brief. b. Ensure the process is followed in future.
3	Physical security audit	Inconsistent visitor logs.	Train the staff on access process.
		Inconsistent rack access logs.	Train the staff on rack access process.
		Anomalies in EACS logs.	Investigate and decide corrective or preventive action.

No	Audit Description	Possible Nonconformity	Possible Corrective / Preventive action
4	Operational Procedures audit – change management plan, incident management plan	Change management process not properly followed.	Train the staffs on the process.
		Incident management plan not followed.	Train the staffs on the process.
5	Anti virus application log and signature file audit	Virus signature file not up to date.	a. Update virus signature database. b. Review update process.
		Virus detected but could not be cleaned.	a. Manually delete the infected file(s) and inform end user(s). b. Develop process for manually deleting infected file(s). c. Train staff on process.
6	Backup and Restore audit	Backup tape restore fail.	Investigate the problem and rectify so that it does not repeat in future.
		Tapes not labelled according to standard.	a. Label the tape properly. b. Train the staff on labelling.
7	User system access audit	Paper list and system list inconsistent.	a. Correct the system user to match paper list. b. Review the process and re-train the system administrators.
8	Firewall rule audit	Firewall rules not consistent with the approved business requirements.	Re-configure firewall rules to match approved business rules.
9	Intrusion Detection System (IDS) log audit	Successful Intrusion detected.	Investigate the intrusion and take corrective actions, like, terminate connections, close firewall rule, etc.
		Unsuccessful Intrusion attempt detected.	Investigate the intrusion attempt and decide on possible preventive action.
10	Firewall log audit	"Pattern" detected on unsuccessful traffic.	Investigate the traffic and decide on possible preventive action.
11	System Logs audit	Anomaly on logs suggesting improper use of the system.	Investigate the anomaly further and decide on possible corrective or preventive action.
12	Network Management System Alerts	Device failed.	Replace failed device with spare.
		Device utilization almost more than 80% for long period of time.	Plan upgrade of hardware with higher capacity.
13	Operating System (OS) and Application Patch level audit	Patch level not up to date.	a. Patch the system to required level. b. Review update process.

6. Conclusion

The ISMS development is a time consuming, but necessary task for secure operations of any Information System. This paper demonstrated an AS/NZS 7799.2:2003 based process for development of an ISMS. Though the example organization used in this paper is imaginary and relatively small, the process can be extended to any type and size of organization. This process could be used for just a small part of an organization or the whole organization.

Appendix A: Terms and Acronyms used

AS	Australian Standard
CEO	Chief Executive Officer
DMZ	De-Militarized Zone
DoS	Denial of Service
EACS	Electronic Access Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
IT&T	Information Technology and Telecommunications
LAN	Local Area Network
NIDS	Network Intrusion Detection System
NZS	New Zealand Standard
OS	Operating System
PDCA	Plan Do Check Act (AS/NZS 7799:2:2003 based process)
VPN	Virtual Private Network
WBS	Work Breakdown Structure

Appendix B: Reference

Unknown Authors. AS/NZS 4360:1999 Risk Management, Sydney: Standards Association of Australia, April 1999.

Unknown Authors. HB 231:2000 Information Security risk management guidelines, Sydney: Standards Australia International Ltd, 2000.

Unknown Authors. AS/NZS ISO/IEC 17799:2001 Information technology – Code of practice for information security management, Sydney: Standards Australia International Ltd, June 2001.

Unknown Authors. AS/NZS 7799.2:2003 Information security management Part 2: Specification for information security management systems, Sydney: Standards Australia International Ltd, February 2003.

Harris, Shon. All in one CISSP Certification Exam Guide, Berkeley: McGraw-Hill/Osborne, 2002.

Unknown Authors. Australian Government Information Technology Security Manual ACSI 33, Canberra: Defence Signals Directorate, February 2004.