Global Information Assurance Certification Paper

Implementing an Information Security Management System (7799) for an e-Banking Environment

[G7799 Assignment version 1.1]

Suzy Clarke

January 2005

[Course attended: SANS Down Under, Melbourne, July 2004]

Contents

1. Abstract

This paper outlines the steps necessary to implement an Information Security Management System (ISMS) for an e-Banking environment following the standards outlined in ISO 17799. It has been written as part of the SANS GIAC G7799 certification.

2. Part One: Defining the System

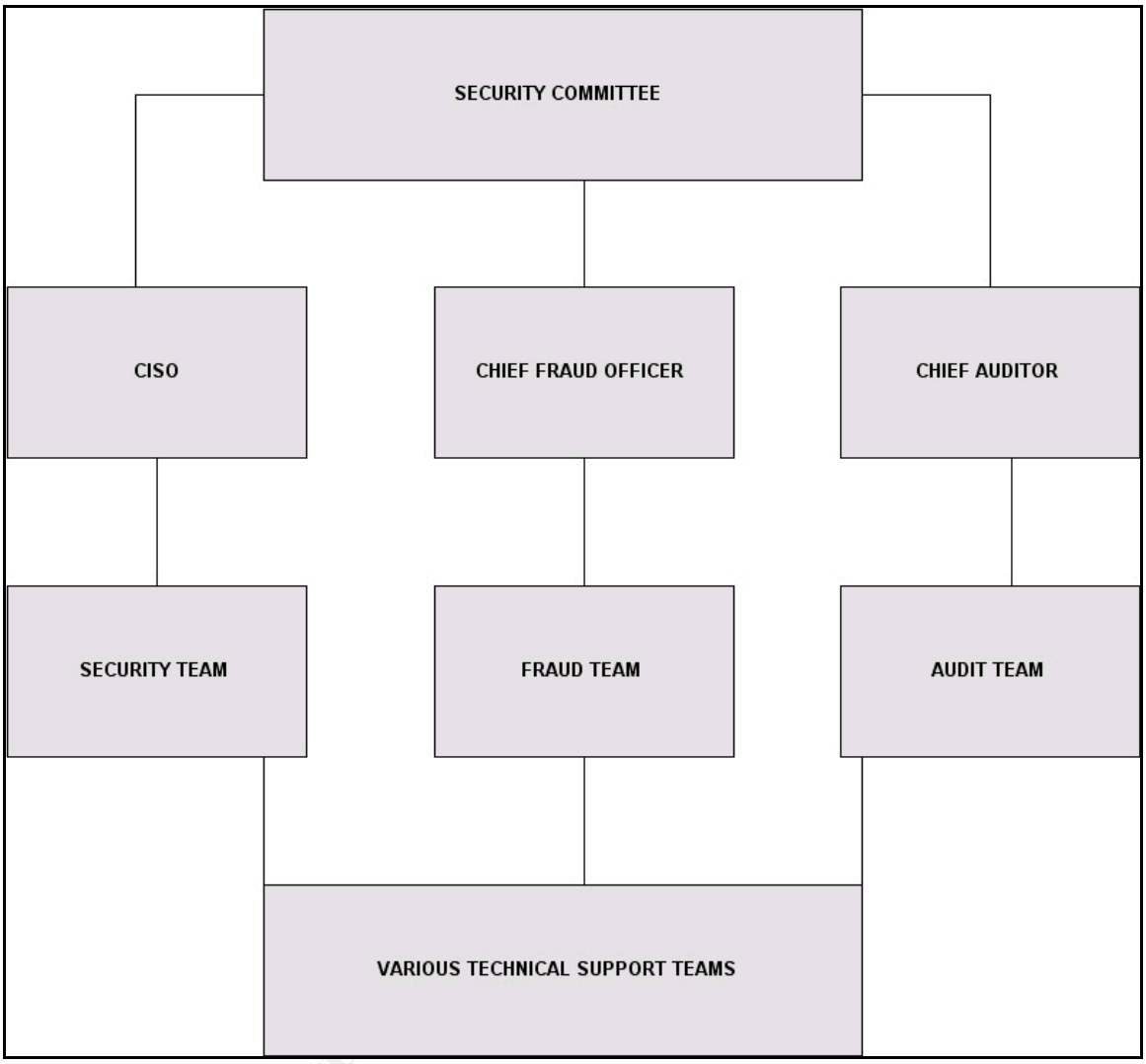
2.1 The Organization

Bank X is a financial services provider that employs approximately 10,000 staff and has nearly a million customers. It operates a number of branches at geographically diverse locations within one country. Operations such as technology, call centers and business support functions are distributed in 3 main locations within the same city.

Bank X not only relies on traditional bricks and mortar branches to attract and maintain customers it also operates within the technical space. It offers its customers the ability to do their banking over the internet, the telephone (landline PSTN) and the mobile (cell) phone.

The bank places a high importance on technology and prefers to perform as many IT functions as possible in house. It has a large team of developers and IT support analysts on staff to ensure continued development and improvement of its IT infrastructure.

Due to the critical priority of minimizing and mitigating risk with all financial transactions there is a strong security culture within the bank. A dedicated information Security Team is established; this is complimented with a separate Audit Team and a Fraud Team. The diagram below gives an overview of the organizational structure:



The Security Committee is comprised of management representatives from key business and technical areas including Fraud, Audit, Security and Legal. The Security Committee reports up to the Executive Board.

The Security Committee Charter outlines the scope, responsibilities, authority, activities and structure of the committee. The main modus operandi for the committee as outlined in the charter is:

"Ensure a cross-organization senior management focus on security, particularly with regard to security initiatives, strategic direction and operational matters such as risk management. The Committee also acts as a forum to facilitate communication and dissemination of security information at the Executive level".

Bank X has a well documented security policy framework which was

developed in conjunction with an external consultancy company. It is based on the policy requirements contained within ISO 17799. At a high level it contains the management and executive commitment to security within the bank; the generic policy statements and guiding security principles; the supporting standards and the explicit procedures.

The policy is owned and maintained by the Security Team under the direction of the Chief Information Security Officer (CISO). It is reviewed periodically by the Audit Team as well as an external consultancy company.

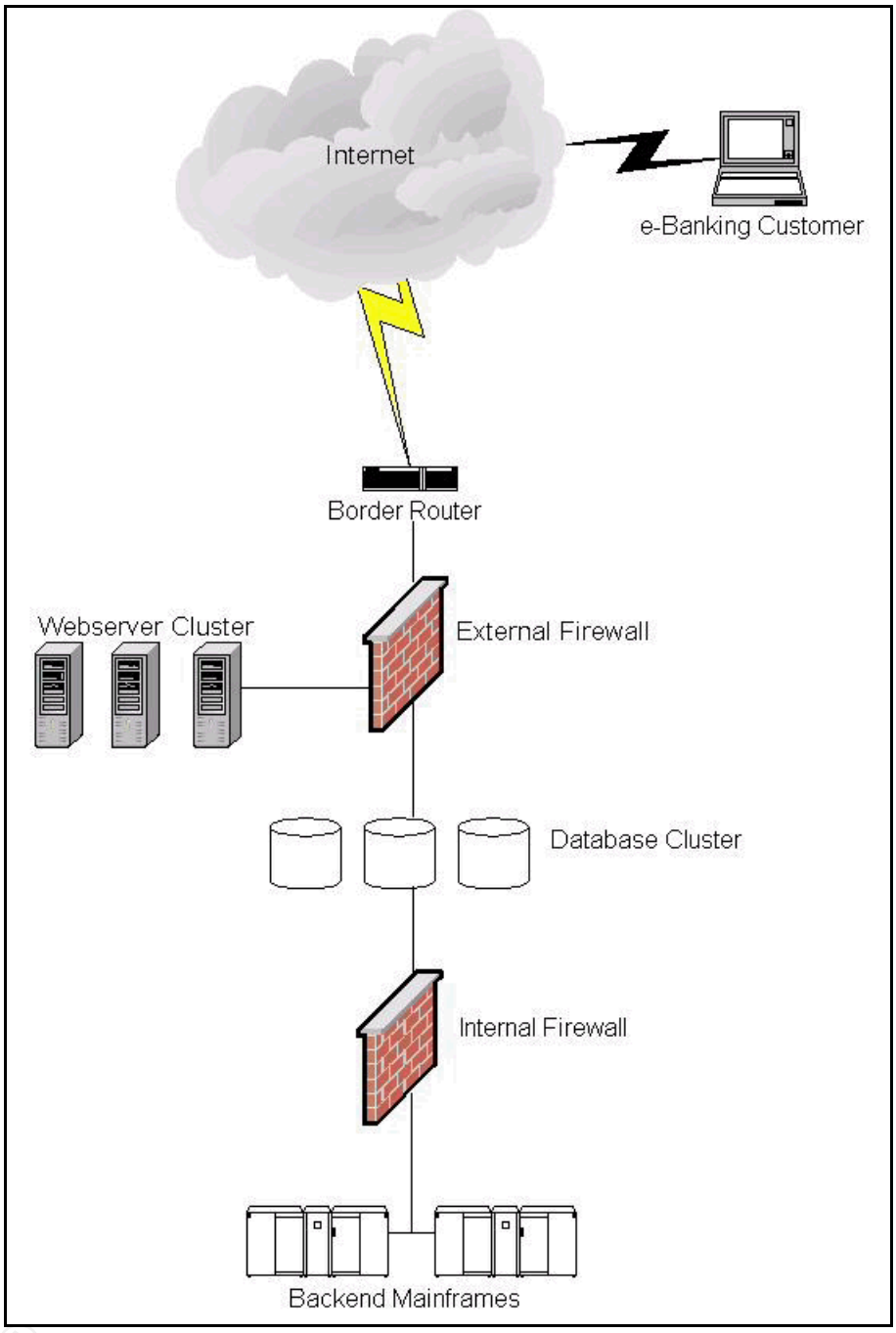
The policy framework is supplemented by a comprehensive security awareness program and various acceptable use policies that were developed in conjunction with the HR and Legal teams.

2.2 Scope of the ISMS

Bank X has selected components of its e-Banking (internet banking) environment to fall within the scope of the 7799 Information Security Management System (ISMS).

The e-Banking architecture is hosted internally within the bank and is fully supported by various teams of technical support personnel. It consists of a tiered network infrastructure with various security controls in place to provide protection against insider and external attacks.

The following diagram gives a simplistic overview:



The External Firewall is dual-homed. One network interface connects to the web DMZ and the other connects to the internal network. The Internal Firewall provides further segmentation and protection of the Backend Mainframes. It does not directly connect to the network perimeter.

For ease of reference a number of items are not shown in this diagram. The out of band (OOB) management network is not depicted; neither is the internal LAN or the QA and development environments which mirror the live

production infrastructure. Each production network segment contains an IPS (Intrusion Prevention) network sensor which connects to a central reporting and alerting console on the OOB management network. Each firewall icon actually represents a pair of firewalls which are set up in a fault tolerant configuration.

Following the principle of separation of duties each component is supported by a different team. The Security Team is responsible for the firewalls, IPS and anti-virus. There are a number of other teams which are responsible for each remaining component:

- Database Team
- Webmasters
- Mainframe Team
- Developers
- QA Team

Strict change control procedures which conform to IT Infrastructure Library (ITIL[1]) recommendations are enforced.

The specific components selected for the 7799 ISMS scope are the Windows 2003 webserver cluster (running IIS 6.0) and the e-Banking application (written in ASP.Net).

The e-Banking application is written by an internal development team within the development environment. It is then migrated to the QA environment where it is tested (under-going both usability and stress testing) by a dedicated team of testers. It is also exposed to rigorous security testing by representatives from the Security Team. Once all necessary sign-off has been given the code is migrated to the production environment by the Webmasters. The Webmasters also support and administer the webservers.

The Security Team has identified a number of additional technical controls that could be implemented to strengthen the security posture of the Bank X e-banking architecture:

i) Introduction of host IPS (Intrusion Prevention) onto the webservers
ii) Introduction of application level firewalls onto the webservers
iii) Introduction of file integrity checkers onto both the webservers and databases
iv) Introduction of database protection measures such as SQL Shield[2] or

[1] http://www.ogc.gov.uk/index.asp?id=2261

[2] http://www.sql-shield.com/

SQL Guard[3]

The merits of introducing these controls will not be discussed as part of the ISMS. Separate projects for each control will be started once the ISMS is put into effect.

[3] http://www.guardium.com/

3. Part Two: Plan

3.1 Preparation Steps

Before the ISMS can be implemented a number of preparation steps need to be taken. In the first instance Bank X will need to appoint a lead Project Manager (PM) who will oversee the implementation of the ISMS and guide all of the associated processes.

During this initial planning stage the PM will be primarily responsible for:

- Identifying the primary stakeholders and sponsors of the project (in conjunction with the Bank X Security Committee)
- Identifying the individuals who should participate in the ISMS Steering Committee
- Selecting an appropriate project management methodology
- Drafting the first project plan that outlines the expected start and end dates as well as any key milestones and dependencies
- Scoping the amount of resource (both in terms of cost and hours of effort) required
- Identifying any major project risks that are initially evident
- Keeping the Security Committee informed of the overall project progress and any problems that are encountered

The Bank X Security Committee has charged the manager of the Technical Solutions Division with selecting the appropriate individual for the job. The decision has been made to appoint an internal employee as it was felt that an external PM would not have the same appreciation of the Bank's processes and culture.

The Bank has not standardized on any one particular project management methodology. The Security Committee expects the PM to select the most relevant framework for this type of project. All PMs within the Technical Solutions Division have experience with a range of methodologies such as Microsoft Solutions Framework[4], Prince[5] and PMI[6].

One of the most important factors when selecting a methodology is to ensure

[4] http://msdn.microsoft.com/vstudio/enterprise/msf/

[5] http://www.ogc.gov.uk/prince/

[6] http://www.pmi.org/info/default.asp

it encourages proactive risk management. At a high level Bank X follows the risk management lifecycle outlined in AS/NZS ISO/IEC 17799:2001. This involves establishing a context, identifying risks, analyzing, evaluating and treating risks and constantly monitoring and reviewing the whole process.

Examples of project risks associated with implementing an ISMS include but are not limited to:

- limited in-house of knowledge of 7799 and the ISMS framework
- resource constraints due to other high priority projects being run simultaneously
- complexity of project communications due to the large number of teams and individuals involved

Another important step during the preparation phase is to identify and document all assets that fall within the scope of the ISMS. These include all types of assets such as physical, electronic, IP (intellectual property) and personnel.

Bank X is currently in the process of implementing a centralized asset management system that replaces manual documentation and processes.

Finally the relevant areas of security policy that need to be referenced during the implementation of the ISMS are:

i) Backup Policy
ii) Logging and Data Retention Policy
iii) Encryption Policy
iv) Incident Handling Policy
v) Information Classification Policy
vi) System Administrator Appropriate Use Policy
vii) Systems Development Policy
viii) Web Application Technical Standards
ix) Webserver Build Standards

The majority of these policies already exist within the Bank X security policy framework. However many of these require further development to be considered SMART (Specific, Measurable, Achievable, Realistic, Time-based).

3.2 ISMS Management Structure

As previously noted Bank X already has a well established Security Committee that meets on a monthly basis. It has been decided that implementing an ISMS requires a dedicated 7799 Steering Committee.

This committee will be comprised of a slightly different set of individuals and will meet on a 2 weekly basis. It will report back to the Security Committee and will be guided by the CISO. A separate charter that incorporates the major milestones and deliverables identified by the PM will be drawn up.

3.3 Policies and Standards

Of the 8 policies outlined in section 3.1 three require further development as part of the ISMS:

Policy name: System Administrator Appropriate Use Policy

Purpose: The purpose of the policy is to ensure that system administrator privileges are not abused and are only used for legitimate, authorized business purposes.

Audience: The individuals who manage the systems, which within the scope of the Bank X ISMS is the Webmasters team.

Areas of 7799 standard that will be addressed: 9.3 “User Responsibilities”; 12.1.5 “Prevention of Misuse of Information Processing Facilities”

Policy name: Web Application Technical Standards

Purpose: The purpose of the policy is to ensure that web applications such as the e-Banking application are developed to a defined, secure standard. The document includes best practice guidelines such as those outlined by the Open Web Application Security Project[7].

Audience: The individuals who develop and maintain the e-Banking application and its underlying components. Within the scope of the Bank X ISMS this is the Developers and the Webmasters.

Areas of 7799 standard that will be addressed: 10 “Systems Development and Maintenance”; 10.2 “Security in Application Systems”

Policy name: Webserver Build Standards

[7] http://www.owasp.org

Purpose: The purpose of the policy is to ensure that all webservers, regardless of operating system, are built to a minimum, secure standard.

Audience: The individuals who build and manage the systems, which within the scope of the ISMS are the Webmasters team.

Areas of 7799 standard that will be addressed*:* 9.5 “Operating System Access Control”; 9.7 “Monitoring System Access and Use”; 10.5.2 “Technical Review of Operating System Changes”

An overview the 5 remaining policies is shown in the table below:

Policy	Purpose	Audience	7799 Reference
Backup	To ensure that a minimum level of backups are taken on a regular basis which can be used in the event of a disaster or media failure	Webmasters	8.4.1 Information Backup
Logging and Data Retention	To ensure that a minimum level audit trail is maintained. Plus to protect important records (such as those related to tax) from loss or destruction	Webmasters Developers	8.4.2 Operator Logs 8.4.3 Fault Logging 12.1.3 Safeguarding of Organizational Records
Encryption	To ensure that appropriate encryption controls are utilized to protect the confidentiality and integrity of sensitive information	Webmasters Developers	10.3 Cryptographic Controls
Incident Handling	To ensure efficient and orderly recovery from security incidents	Webmasters Security Team	6.3 Responding to Security Incidents and Malfunctions 8.1.3 Incident Management Procedures
Information Classification	To ensure that information is appropriately classified and so has the most appropriate protection level applied	Webmasters Developers Security Team	5.2 Information Classification
Systems Development	To ensure that security is built into all applications	Developers	10 Systems Development and Maintenance

3.4 Risks and Controls

The three main risks to the Bank X e-banking environment, from a qualitative perspective, as agreed by the Security Committee are:

1) Human Failure*:* Unauthorized use of administrator rights

2) Technical Failure: Outage of webserver due to hardware failure

3) Deliberate Act*:* Denial of Service

The risk management methodology that has been loosely adopted to identify these risks was AS/NZS 4360:2004[8]. The process that this standard advocates is shown in the following diagram:

Taken from http://www.risksociety.org.nz/dealing.html

The process of mitigating these 3 risks is discussed in the following sections.

3.4.1 Unauthorized use of administrator rights

Nature of the threat

[8] http://shop.standards.co.nz/productdetail.jsp?sku=4360%3A2004%28AS%2FNZS%29

The threat exists that a webserver administrator could abuse their access rights to install Trojan software onto the Bank X webservers in order to compromise customer accounts and commit fraudulent transactions for personal gain.

Vulnerability

Although the practice of segregation of duties is followed within Bank X job rotation and minimum leave are not enforced. Furthermore the logging capabilities in place are limited and could easily be manipulated by an administrator to cover up suspicious activity. The potential for collusion between technical team employees also exists

Likelihood of Occurrence:	**HIGH**
Impact	**HIGH**
Risk Level	**HIGH**

Description of the 7799 controls selected:

i) Section 6: Personnel Security (including Security in Job Definition and Resourcing, User Training, Responding to Security Incidents and Malfunctions).

NB - refer to Section 5 of this document for more information on the controls listed in this section of 7799.

ii) 8.1.2 Operational Change Control and 10.5.1 Change Control Procedures

iii) 8.1.4 Segregation of Duties

iv) 8.3.1 Controls Against Malicious Software

v) 8.4.2 Operator Logs

vi) 9.1.1 Access Control Policy

vii) 9.2.2 Privilege Management

viii) 9.2.4 Review of User Access Rights

ix) 9.5.3 User Identification and Authentication

x) 9.6.1 Information Access Restriction

xi) 9.7 Monitoring System Access and Use

xii) 10.4.1 Control of Operational Software

xiii) 10.4.3 Access Control to Program Source Library

xiv) 10.5.2 Technical Review of Operating System Changes

xv) 12.3.1 System Audit Controls

Reason for selecting controls

These controls ensure that thorough independent audit trails are kept of all activity on the webservers. Fraudulent actions would be recorded and detected by auditors.

Risk level after implementing control **LOW**

3.4.2 Outage of webserver due to hardware failure

Nature of the threat

The threat exists that the Bank X e-banking application might be unavailable if a hardware malfunction or failure occurs with the webservers. An outage of the e-banking application would cause loss of revenue and brand damage[9].

Vulnerability

At present the Bank X webservers have been installed and configured with little attention to power supply resiliency.

Likelihood of Occurrence	**MEDIUM**
Impact	**HIGH**
Risk Level	**MEDIUM**

Description of the 7799 controls selected

i) 5.1.1 Inventory of Assets

ii) 7.2.1 Equipment Siting and Protection

iii) 7.2.2 Power Supplies

[9] Recent events demonstrate that this is a very real threat which can and does occur in the real world. Reference “Major Computer Crash Hits HSBC Customers” http://hardware.silicon.com/servers/0,39024647,39126821,00.htm

iv) 7.2.3 Cabling Security

v) 7.2.4 Equipment Maintenance

vi) 8.2.1 Capacity Planning

vii) 9.7.2 Monitoring System Use (particularly part d – system alerts or failures)

viii) 11.1 Business Continuity Management

In addition to these controls it is important that the webservers are configured in a web cluster; that comprehensive hardware maintenance contracts are in place (ensuring that the considerations in section 4.3.1 “Security Requirements in Outsourcing Contracts” are included) and that a DR environment is in place and is regularly tested.

Reason for selecting controls

Implementing these controls will minimize the likelihood and impact of a webserver hardware failure occurring. They will help maintain a high fault tolerance level and reduce the recovery time if a failure does happen.

Risk level after implementing control **LOW**

3.4.3 Denial of Service

Nature of the threat:

The threat exists of a malicious e-banking user or external third party launching a denial of service (DoS) attack against the Bank X e-banking environment. This would have both a negative financial and brand impact. The individual(s) who initiated the attack may be acting out of malice or may be attempting to extort money from Bank X.

A recent Information Security Magazine article discusses just these scenarios and suggests that they are likely to increase in 2005[10].

Vulnerability

Bank X does not have an external IPS with denial of service protection capabilities on its internet link. It also does not have a secondary internet link for redundancy/failover. Finally there are no official reciprocal agreements in place with other banks or ISPs which would come into effect if a DoS was launched.

Likelihood of Occurrence	**LOW**
Impact	**HIGH**
Risk Level	**MEDIUM**

Description of the 7799 controls selected

i) 4.1.2 Information Security Co-Ordination

ii) 4.1.6 Co-Operation Between Organizations

iii) 6.3 Responding to Security Incidents and Malfunctions

iv) 8.1.3 Incident Management Procedures

v) 9.4.7 Network Connection Control

vi) 9.7.1 Event Logging

vii) 11.1 Business Continuity Management

In addition to these controls it also recommended that Bank X configure

[10] Refer to section "DoS Floodwaters on the Rise"
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss526_art1079,00.html

appropriate access control lists on their external routers[11] and deploy an IPS with anti-DoS capability.

With regard to control ii) it is particularly important to establish and maintain liaison with the Bank X upstream Internet Service Provider (ISP).

Reason for selecting controls

Whilst implementing these controls does not lower the likelihood of a DoS occurring they do improve the mitigation techniques and will help to keep the recovery time low should Bank X be the target of a DoS.

Risk level after implementing controls **LOW to MEDIUM**

[11] http://www.cisco.com/warp/public/707/newsflash.html

4. Part Three: Do

4.1 Implementing the Improvements

Problem A: Bank X does not have appropriately documented Appropriate User Policies for System Administrators.

Action: To address this, AUPs will need to be developed and implemented.

Steps:

1) CISO to draft System Administrator AUP based on existing policies
2) Security Committee to review draft AUP
3) AUP to ratified by Legal, HR and Audit
4) AUP to be re-reviewed by Security Committee and signed off
5) AUP to be circulated and publicized internally
6) Individuals with System Administrator access to sign the AUPs
7) HR to hold signed AUPs on file for each relevant employee

Problem B: The Bank X e-banking environment does not have appropriately documented webserver build standards or web technical standards.

Action: To address this, the appropriate standards will need to be developed and implemented.

Steps:

1) CISO to draft standards in conjunction with best practice
2) Standards to be reviewed by relevant technical teams and external consultancy
3) Security Committee to review standards
4) Standards to be circulated and publicized internally
5) Existing web systems to be audited against the standards by the Security Team. Deviations from the standards to be corrected by the relevant technical teams such as the webmasters or developers

Problem C: The Bank X e-banking system is not protected by comprehensive logging and audit trails.

Action: To address this, the appropriate processes and monitoring will need to be developed and implemented.

Steps:

1) The Bank X Security Team under the direction of the CISO to develop logging criteria that contains all necessary parameters such as user IDs, dates and times, privileged operations
2) CISO to sign off on logging criteria
3) Technical teams to implement the criteria
4) Audit Team to assess the logging
5) Report following the audit to be submitted to the Security Committee

Problem D: Bank X has not set up official co-operative agreements between organizations such as fellow banks and upstream ISPs.

Action: To address this, the necessary agreements will need to be developed and implemented.

Steps:

1) CISO to contact relevant organizations to determine who the most appropriate security contact is
2) CISO in conjunction with Legal to draft reciprocal agreements
3) Agreements to be reviewed by Security Committee and signed off
4) Agreements to be circulated to relevant external parties and signed as necessary. Bank X Legal to store signed copies
5) CISO to maintain regular contact with the organizations to discuss current security issues and ways to address them

4.2 Statement of Applicability

A Statement of Applicability (SoA) outlines how 7799 has been implemented through the ISMS. It details each relevant 7799 control and how it has been put into place. Concomitant to that it also details the exclusions and justifies why each of the excluded controls has been omitted as not relevant.

Following is an SoA for two of the controls considered for the Bank X e-banking application. One of them is included on the list of exclusions.

Problem C – *8.4.2 Operator Logs and 9.7.1 Event Logging*

This control will be implemented as part of the ISMS as it was listed as a countermeasure for all four risks discussed in section 3 of this document.

Problem D – *4.1.6 Co-operations between Organizations*

Although this control is relevant to the Bank X e-banking environment the Security Committee has decided that the existing ad-hoc informal business relationships that have already been established are sufficient to meet this audit criteria. This control will be excluded. Non-disclosure agreements (NDAs) will be drawn up as necessary if matters need to be discussed with organizations that do not have an existing agreement with Bank X.

5. Part Four: Check

The following checklist outlines the steps that need to be taken to audit the Bank X environment against Section 6 of 7799 which focuses on Personnel Security. The main objective of this section of 7799 is "To reduce the risks of human error, theft, fraud or misuse of facilities".

Introducing controls related to personnel security is of critical importance. A recent article on CNET by Dan Llet[12] references an FSA (Financial Services Authority UK) report[13] which claims that criminals are "planting" insiders in enterprises such as banks to specifically commit fraud, steal data and launch cyber attacks.

Along the same lines a 2002 News.com special report entitled "Cracking the Nest Egg"[14] states "security experts note that a bank insider more often than not plays a role in security breaches" and also goes on to note that often a "current or former employee in the bank's technology department" is involved in such incidents.

Introducing the controls outlined in 7799 Section 6 will help to minimize the likelihood of such "planting" attempts being successful.

[12] http://news.com.com/Cybercriminals+infiltrating+U.K+companies/2100-7355_3-5450117.html

[13] Refer to References Appendix in this document for more information

[14] http://www.go-online.gr/files/document/04-07-2002/banking_risks.pdf

5.1 7799 Audit Checklist

Control Objective	Reason	Check
6.1 Security in job definition and resourcing	"To reduce the risks of human error, theft, fraud or misuse of facilities"	Liaise with Human Resources (HR) and Security team to ensure: Security Policy documents exist Acceptable Use Policy (AUP) templates exist AUPs signed by staff are filed Standard employment contracts exist which reference security responsibilities Also speak with members of staff to ascertain whether they are aware of the security requirements in their employment contracts
6.1.1 Including security in job responsibilities	To ensure all employees are held responsible for security	Liaise with Human Resources (HR) and Security team to ensure: Position description templates exist for teams such as Webmasters and Developers Confirm that security is referenced as a responsibility within these templates

6.1.2 Personnel screening and policy	To ensure the integrity of all employees and to prove the authenticity of their work and academic history	Confirm with HR the process followed to screen potential job candidates. Ensure that: At least 2 character references are obtained (personal and professional) Proof of academic qualifications is obtained Identity checks are performed (for example copies of passport are retained plus any necessary work permits) Credit checks are performed For an existing member of both the Webmasters and Developers team ask to see each piece of information referenced above.
6.1.3 Confidentiality agreements	To ensure that employees do not circulate or leak information that is confidential or business sensitive	Liaise with HR to ensure that confidentiality (non-disclosure) clauses are incorporated into standard employment contracts.
6.1.4 Terms and conditions of employment	To ensure all employees are held responsible for security as well as outlining the employee's legal responsibilities and rights	Liaise with HR to confirm that the standard employment terms and conditions state that security is an employee responsibility.

6.2 User training *6.2.1 Information security education and training*	"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"	Liaise with Human Resources (HR) and Security team to confirm the formal Induction process. Obtain copies of Induction course material if appropriate and verify that they contain references to security. Confirm that an on-going security awareness program exists and is documented. Read and save any related material such as intranet pages or memos to staff.
6.3 Responding to security incidents and malfunctions *6.3.1 Reporting security incidents*	"To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents"	Liaise with the Security team to confirm that a formal incident reporting procedure exists. Obtain all relevant incident report templates. Confirm the escalation path in the event of an incident. Ascertain the locations of the incident forms. Ask a member of the technical team to describe the process that they would follow if they discovered an incident.
6.3.2 Reporting security weaknesses	To ensure security weaknesses are reported to management in a timely and co-ordinated manner	Liaise with the Security team and Helpdesk Determine if a central mailbox or intranet web form for contacting the security team exists

6.3.3 Reporting software malfunctions	To ensure software malfunctions are reported in a timely and co-ordinated manner	Liaise with the Security team and Helpdesk Determine if a central mailbox or intranet web form for contacting the security team exists Determine if the Helpdesk uses a call management system. View a sample of software malfunction jobs that have been recorded in the last quarter
6.3.4 Learning from incidents	To ensure that steps are taken to correct mistakes which lead or contributed to previous security incidents	Liaise with the Security team Ask to view incident reports – ensure they contain a comprehensive lessons learned section Ask to view Security Committee agenda minutes and ensure that discussion of security incidents has occurred
6.3.5 Disciplinary process	To ensure that a formal disciplinary process exists for security policy violations	Liaise with Human Resources (HR) and Security team Discuss the disciplinary process

6. Part Five: Act

6.1 Maintaining the ISMS

Once the ISMS is implemented a process of continual improvement needs to be instigated. This will be heavily founded on regular monitoring activities that aim to improve all areas of the ISMS framework and keep it current.

Within Bank X this monitoring cycle will take the form of

A) regular risk reviews which highlight new vulnerabilities or threats that change the risk profile of the system
B) an audit program which aims to determine whether the ISMS is still effective and whether the scope is still relevant

The frequency of these tasks will need to be agreed by Bank X management. As a guideline the risk reviews would ideally be run every quarter or twice yearly on an on-going basis and after any major incident on an ad hoc basis. The official ISMS audit program should be run yearly. A decision will need to be made on whether external auditors are engaged to perform this audit.

One of the most important responsibilities within the act phase is to maintain communication with the ISMS stakeholders. An efficient way of achieving this would be to ensure that discussion of the ISMS remains an agenda point at the Security Committee meetings.

The results of the risk reviews and the audit program could then be discussed at this forum and any necessary corrective action agreed and assigned to the relevant internal teams. Furthermore examination of external factors that may affect the ISMS such as

- legislation changes (for example the recent introduction of SOX[15])
- internal incidents
- significant changes in business processes or technology

could also be undertaken.

All reviews, associated findings and follow up actions, such as areas of non-compliance and how to remedy them, will need to be thoroughly documented. The responsibility for ensuring this should ultimately reside with the CISO.

Following this maintenance cycle will also help to highlight the benefits that have been delivered by implementing a best practice ISMS.

[15] http://news.findlaw.com/hdocs/ docs/gwbush/sarbanes**oxley**072302.pdf

Appendix A: References

BEST PRACTICE for SECURITY MANAGEMENT [ITIL] – Cazemier et al – OGC [Office of Government Commerce] – 2003 – ISBN:9780113300143

CISA REVIEW MANUAL – ISACA – 2003 – ISBN: 1-893209-42-3

CISSP All-in-One EXAM GUIDE [Second Edition] – Harris – Osborne – 2003 – ISBN:0072229667

CODE OF PRACTICE for INFORMATION SECURITY MANAGEMENT [AS/NZS ISO/IEC 17799:2001] – Standards Australia/New Zealand – 2001 – ISBN: 0733738761

Countering financial crime risks in information security [Financial Crime Sector Report] -http://www.fsa.gov.uk/pubs/other/fcrime_sector.pdf
FSA [Financial Services Authority] UK – 2004

Implementing BS7799: A Blueprint
http://www.iso17799world.com/ - 2004

ISO 17799 CHECKLIST - Thiagarajan, Valliappan - SANS Institute – 2003
http://www.sans.org/score/checklists/ISO_17799_checklist.doc

IT BASELINE PROTECTION MANUAL [English version] – BSI [Bundesamt für Sicherheit in der Informationstechnik] -
http://www.bsi.de/gshb/english/etc/index.htm
2003 - ISBN:3-88784-915-9

SECURITY STANDARDS: STANDARD PRACTICE -
http://infosecuritymag.techtarget.com/2002/mar/iso17799.shtml
TechTarget - 2002