APPENDIX A

THE NATURE OF AUDIT PROCEDURES IN AN EC PAYMENT SECURITY AUDIT

INDEX

1 Introduction – Purpose of this Appendix

The audit considerations mentioned in this Appendix are related to an audit in an EC payment security environment and assist the IS auditor in determining the audit procedures and tests to be performed. The nature and extent of the audit procedures are further dependent on the information obtained and the risks in the environment. Due to the complexity of the technology in the EC payment security environment, the considerations covering the nature and extent of the auditing procedures have been included separately from Chapter 6 in this Appendix. This is also due to the level of detail required to provide detailed consideration listings related to the nature and extent of the procedures.

This Appendix shows the audit considerations related to the steps in the audit approach as highlighted in Chapter 6 of this dissertation. Firstly, the considerations related to Background information gathering is provided in Section 2, followed by the considerations related to the controls in Section 3. In Chapter 6, the reference to the detailed considerations was provided with each control area, where applicable. Chapter 6 and this Appendix should therefore be used together to obtain the maximum benefit from the information provided.

2 BACKGROUND INFORMATION GATHERING AUDIT CONSIDERATIONS

2.1 GENERAL IT INFORMATION GATHERING CONSIDERATIONS

The following tables contain guidelines for information that should be gathered by the IS auditor to obtain an understanding of the EC environment in an organisation.

Table A1 IT Information to be Obtained

IT Information			
Outsourced functions (Consider IT operations, systems development, web development, web hosting, ASP, IT Internal Audit):			
Hardware platforms (Consider central IT, localised IT, e Commerce, m Commerce):			
e.g. AS/400, UNIX, OS/390			
External links e.g. routers, firewalls (please detail): Operating systems and other system software (please detail): No. of WANs [ ] No. of LANs [ ]			
Application software that supports key EC business processes (please detail):			
Name	Supplier *(or in house)*	Key business process	Date developed/implemented

Table A2 Hardware Platform Configuration Information to be Obtained

Hardware Platform Configuration (make and model)	Number	Number of Terminals
Mainframe		
UNIX Environment		
Windows NT/W2K Environment		
Other Platforms		
• PC(s)		

Table A3 IT Installation Information to be Collected

IT Installation		
Operating Systems in use	**Version**	
IBM (e.g., OS/390)		
UNIX (e.g., HP-UX, Solaris, AIX)		
Windows NT/W2K		
PC		
Other		
Programming Languages or 4GLs (Powerbuilder, Developer 2000 etc.)	**Version**	**Running on**
Access control software (Safeguard, Intel LanDesk Protect etc)		
Database management system (e.g., DB2, Oracle, Sybase, Adabas, RACF, ACF2)		
Network Scanning and Intrusion Detection tools used (e.g., ITA, Axent/ESM, Netprowler)		
Others		
Disk or tape management systems		
Document Management		
Report Generators		
Audit Software		

Table A4 EC Application System Information

EC Application systems software	Date installed	Computer used	Comments (e.g. in-house or packaged software, EDI, e-commerce, batch,on-line)	WP Ref
Accounting				
Other applications				

Information on significant EC Applications used to support to EC activities

Consider the specific setup of application(s) that are considered significant.

Table A5 General EC Application Information to be Obtained

Name of Application (e.g.. package name):	
Designated Owner:	
Description of the Application:	

Major Modules / Functions of the Application:

....

Table A6 EC Specific Application System Information to be Obtained

• Package or In-house developed:	• Package/software maintenance supplier:
• Installation Date:	• Version of software:
• Source code owned or available: • Program Language:	• Extent of modifications:
• Number of Users:	• User satisfaction ranking (good-5 low-1)
• Is the system documented:	• Interfaces:

Is the system considered to be stable? (Please comment.)

Was there sufficient training on the systems?

2.2 EC SPECIFIC INFORMATION GATHERING AUDIT CONSIDERATIONS

General Information

EC activities to be covered:

- Describe the entity's electronic commerce activities.
- What goods / services are being sold / provided?
- Who is the typical customer?
- What is the typical form of payment?
- What is the Web site URL?
- Who is responsible for controlling these activities
  - What is their organisation reporting relationship to the entity's management?
- How long has the entity been selling such goods and services through this form of electronic commerce?
- If the electronic commerce activities have changed describe the nature of such changes
  - When did each change occur?

- Information Systems Used to Support the Electronic Commerce Activities (if not covered through the IT information gathering as highlighted in 3.1.1.1 above).

Control Environment

Describe the factors in the entity's organisation that contribute to a control environment that is generally conducive to reliable business practice disclosures on its Web site.

Describe the effective controls over electronic commerce transaction integrity and the protection of related private customer information. Such factors might include, but not be limited to:

- Management's strategy for EC;
- Hiring, development, and retention of competent personnel;
- Emphasising the importance and responsibilities for sound business practices and effective control;
- Supervising business activities and control procedures;
- Employing a suitable internal auditing function that periodically audits matters related to the entity's electronic commerce activities;
- Other factors.

Business Practice Disclosures

Describe the entity's business practices related to EC payments. How are such practices disclosed to customers? Consider the following:

- The terms and conditions by which electronic commerce transactions are conducted;
- Payment terms, including customer options, if any;
- Electronic settlement practices and related charges to customers;
- How the customer may cancel recurring charges, if any;
- Other relevant terms and conditions, if any.
- Who is responsible for controlling these activities?
- Has the entity changed its business practices or the related disclosures since the last review? If so, describe the nature of such changes and when each change occurred.

- Describe the entity's process for monitoring customer claims and complaints and for identifying patterns of claims and complaints that are not being satisfactorily addressed. A review of customer complaints may indicate weaknesses in the system.
- Describe the processes management uses to monitor the continuing effectiveness of its disclosure of business practices.

Transaction Integrity Controls

Describe the controls maintained by the entity to ensure the integrity of electronic commerce transactions. The IS auditor should describe the following.
How the entity provides reasonable assurance that:

- Each order is checked for accuracy and completeness;
- Positive acknowledgment is received from the customer before the order is processed.
- Services and information are provided to the customer as agreed to on the order;
- Back order and other exceptions are promptly communicated to the customer.
- Sales prices and all other costs are displayed for the customer before requesting acknowledgment of the order;
- Orders are billed and electronically settled as agreed;
- Billing or settlement errors are promptly corrected.
- The entity maintains controls that allow for subsequent follow-up of orders.
- Responsible has been assigned for controlling these activities.
- If the entity changed its controls over transaction integrity since the last review and if controls over transaction integrity have changed, the nature of such changes and when each change occurred are detailed.
- The processes management uses to monitor the continuing effectiveness of its controls over transaction integrity are adequate.

Information Protection Controls

Private customer information includes personal identification information for the customer or his or her family (name, address, telephone number, social security or other government identification numbers, employer, credit card numbers, etc.), personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records or

similar information. The following should be considered by the IS auditor during the information gathering phase:

- Describe the steps taken to ensure the protection of private customer information.
- Describe the controls maintained by the entity to protect transmissions of private customer information over the Internet from unintended recipients.

- Describe the controls maintained by the entity to protect from outsiders private customer information obtained as a result of electronic commerce and retained in its system.

    - How systems that retain private customer information, obtained as a result of electronic commerce, are protected from outside access.
    - How the entity ensures that customers entering through the Web page can only perform inquiries, execute authorised transactions, and obtain information about their own transactions.
    - How private customer information obtained as a result of electronic commerce is protected from intentional disclosure to parties not related to the entity's business unless:
        - customers are clearly notified prior to their providing such information, or
        - customer permission is obtained after they have provided such information.
    - How the entity ensures that private customer information obtained as a result of electronic commerce is used by employees only in ways associated with the entity's business.

- Describe the controls maintained by the entity to protect against its unauthorised access to customer's computers and its unauthorised modification of customer's computer files:

    - How the entity ensures that customer permission is obtained before storing, altering or copying information in the customer's computer (including the use of "cookies" stored on the customer's computer system), or that the customer is notified with an option to prevent such activities;
    - How the entity ensures that transmission of computer viruses to customers is prevented;

- Who is responsible for controlling these activities?

Has the entity changed its controls over information protection since the last review? If so, describe the nature of such changes and when each change occurred.
Describe the processes management uses to monitor the continuing effectiveness of its controls over information protection.

Describe any other matters that would be relevant in evaluating EC payment security. Examples include:

- Significant changes in the entity's business or its organisational structure;
- Significant processing or controls problems with the entity's electronic commerce systems or supporting infrastructure;
- Instances of fraud and breaches of transaction integrity, security and information protection controls involving:
  - employees with electronic commerce responsibilities;
  - contractors and others who provide services to the entity related to its electronic commerce activities;
  - unauthorised third parties, or
  - systems and supporting infrastructure used for executing electronic commerce transactions.
- Significant changes in management and other key personnel with electronic commerce responsibilities.
- Other relevant information.

3 EC DETAILED AUDIT PROCEDURES AND CONTROL CONSIDERATIONS

3.1 SECURITY POLICY, CORPORATE INFORMATION SECURITY (CIS) AND SECURITY ADMINISTRATION

3.1.1 Security Policy

A security policy, Corporate Information Security Office (CISO), or security administration review would normally be performed as a separate audit. The IS auditor should ensure that aspects related to EC have been included in such previous audits. The IS auditor should therefore ensure that aspects mentioned in

this section have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact the EC payment security audit and assess management actions taken since the last audit/ review.

A security policy needs to lay out, in writing, the security steps followed by an organisation and should outline the issues of who, what, when, how, and why of ongoing actions and procedures. It should be a detailed document that identifies risks, defines steps taken to reduce them to acceptable levels, and outlines the tasks and job-descriptions of those directly involved in the enforcement of security in an organisation.
The auditor needs to determine whether formal security policies and security standards documents are tailored specifically for each networking environment. The auditor must also determine whether periodic assessment of systems, policies, and procedures is performed, (thereby providing an effective augmentation of existing security programs), and the implementation of new security measures and countermeasures.

Audit Procedures
Review documentation, and/or interview appropriate personnel to determine whether the CISO has performed an assessment of the risk and determined the security requirements and operational procedures to be included in the applicable Security Policy, Certificate Policy and/or Certificate Practice Statement (CPS – as used by a Certification Authority (CA)).

Ensure review document includes descriptions of the following controls:

- Primary controls including:
  - Security Policy and Security Organisation
  - Asset Classification and Control
  - Personnel Security
  - Physical and Environmental Security
  - Computer and Network Management
  - System Access Control
  - Systems Development and Maintenance
  - Business Continuity Planning
  - Legal Compliance

- Event Journal

- Key management life cycle controls including:
  - Key Generation, Storage, Backup and Recovery
  - Key Distribution, Escrow, Usage, Destruction, and Archival

- Certificate life cycle controls including:
  - Initial Certificate Registration
  - Subsequent Certificate Renewal and Rekey
  - Certificate Issuance, Distribution, Revocation, and Suspension
  - Certificate Revocation List (CRL) Processing

- Device life cycle controls including:
  - Device Shipment, Receipt, Pre-Use, Storage, Installation, Usage, De-installation, Service and Repair, and Device Retirement

Review documentation, and/or interview appropriate personnel to determine whether documented policies and procedures exist and are followed for making available the CA's Certification Practice Statement (CPS), and applicable public CA Certificate Policies to all End Entities and Relying Parties.

Interview the organization's information security manager, if someone has been appointed to that position, or other employees who have been given information security management responsibilities to determine whether their understanding of their assigned tasks is consistent with the organisation's security policy statement.

3.1.2 Security Organisation

Audit Procedures

The IS auditor should consider performing the following procedures to determine whether the requirements of the information security infrastructure, as stated in the applicable security-related documentation, are being achieved:

- Obtain documentation of the security organisation;
- Obtain and review documentation of the security related roles and responsibilities;

- Match the defined security roles and responsibilities with the names of the personnel performing the specific functions and determine whether the segregation of duties is adequate;
- Review the authorisation process for the IT facilities;
- Interview relevant personnel including the security officer;
- Obtain a copy of any reviews of the security organisation whether Internal audit, External audit, or other third party organisations, and evaluate for discrepancies found.

The IS auditor should consider performing the following procedures to determine whether the requirements for third party access, as stated in the applicable security-related documentation. are being achieved:

- Review documentation and interview appropriate personnel to determine the business need for providing third party access, if such access is allowed.
- Review documentation and interview appropriate personnel to determine the extent of third-party access allowed.
- Obtain documentation of the procedures for granting, controlling and monitoring third-party access.
- Obtain a copy of relevant Service Level agreements and review the security section to identify security considerations in the contract and ensure it has been adequately defined.
- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the requirements for security reviews of IT systems, as stated in the applicable security-related documentation, are being achieved:

- Obtain reports of internal or external reviews of the IT systems against the company security policy and identify any weaknesses related to the EC payment security audit.
- Obtain reports of internal or external reviews of the IT facilities against the security implementation standards and identify any weaknesses related to the EC payment security audit.
- Evaluate the protection of system audit tools
- Interview appropriate auditors.

3.1.3 System Administration and Access Control

Audit Procedures

The auditor should consider performing the following procedures to determine whether the user access management requirements, as stated in the applicable security-related documentation, are being achieved:

- Review the user access management policy and procedure documentation;
- Interview appropriate personnel;
- Review user registration and de-registration procedures;
- Select a sample of employees who have changed jobs or left the organisation and assess the timeliness of the required changes to their access rights.
- Review privileged use log reports: determine whether the logs are reviewed and follow up actions defined and taken, where required;
- Review password management policies and procedures and determine whether they adhere to generally accepted standards;
- Review documentation to determine whether the assigned permissions and separation of duties for the Root CA systems are appropriate;
- Review documentation of the CA functions, the performance of which requires the concurrent participation of two or more individuals, and the related access lists;
- Select a sample of user accounts and test whether their access privileges are correct;
- Review policies and procedures and interview appropriate personnel to determine whether users' access rights and privileges are periodically reviewed.

The auditor should consider performing the following procedures to determine whether the requirements for user responsibilities, as stated in the applicable security-related documentation, are being achieved:

- Review password management policies and procedures;
- Interview appropriate personnel to determine whether password change requirements are in operation;

- Test the corporate and CA's documented password strength controls through review of operating system security policy criteria for passwords (e.g., format, length, history, etc.);
- Review policies and procedures related to unattended user equipment;
- Observe whether automatic log-off for unattended equipment is in operation;
- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the network access control requirements, as stated in the applicable security-related documentation, are being achieved:

- Obtain a network map to understand the network components and environment;
- Review network access control policies and procedures documentation and ensure it includes descriptions of the following:
  - Limited services
  - Enforced path
  - User authentication
  - Node authentication
  - Remote diagnostic port protection
  - Segregation in networks
  - Network connection control
  - Network routing control
  - Security of network services

- Interview appropriate personnel.
- Perform automated scans of selected servers to ascertain whether known vulnerabilities are present. Review active services on the critical networks and compare it to the requirements specified in the security policy. Obtain justification for active services and evaluate for appropriateness.

The auditor should consider performing the following procedures to determine whether the computer access control requirements, as stated in the applicable security-related documentation, are being achieved:

- Review computer access control policy documentation and ensure it includes descriptions of the following computer access control requirements:

- Automatic terminal identification
- Terminal log-on procedures
- User identifiers
- Password management system
- Duress alarm to safeguard users
- Terminal time-out
- Limitation of connection time.

- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the application access control requirements related to EC payment applications, as stated in the applicable security-related documentation, are being achieved:

- Review the application access control policy and procedures documentation and ensure it includes descriptions of the following application access control requirements:

  - Information access restriction.
  - Use of system utilities.
  - Access control to program source library.
  - Sensitive system isolation.

- Interview appropriate personnel;
- Observe whether sensitive systems are physically and logically isolated;
- Observe whether the equipment in the Root CA or any encryption key generation ceremony room is not connected to any network outside of the room, is password protected and is physically secured inside the locked room.

The auditor should consider performing the following procedures to determine whether the requirements for monitoring system access and use, as stated in the applicable security-related documentation, are being achieved:

- Review the policies and procedures documentation for monitoring system access and use;

- Review configurations of logging hosts and logged clients and determine whether logging information is being produced and archived for review by management;
- Review a sample of system availability reports and determine whether they are produced on a regular basis;
- Interview management to gain an understanding of review and follow-up procedures;
- Review management reports to determine whether appropriate network monitoring information is summarised and reported to management.

Monitoring activities related to intrusion detection is covered under Section 2.11.

3.2 PHYSICAL AND ENVIRONMENTAL SECURITY

A really solid network defense is not complete if someone can physically gain access to equipment or private networks. A physical and environmental security review would normally be performed as a separate audit. The purpose of this section is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that needs to be taken into account and audit procedures that need to be performed by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in previous audit procedures. Where weaknesses were identified during a physical or environmental security audit, the IS auditor should assess whether such weaknesses impact upon the EC payment security audit and assess management actions taken since the last audit/ review.

Audit Procedures

The auditor should perform the following procedures that relate specifically to the physical security of the EC payments security environment:

- Ensure equipment has several layers of physical security. Some examples to be considered:
  - Controlled access to the building;
  - A secure network room;
  - Locked cabinets for the equipment;
  - A screen to prevent wireless communications from leaving the room.

- Ensure E-commerce servers are located in a secured building and were included as part of the previous audit procedures for physical and environmental security. Physical security aspects should be specified in the policies and procedures documentation.

The following apply to secure areas related to CA activities.

- Ensure data centres and computer rooms supporting critical business activities have strong physical security, which includes the following:

    - Root CA operations are conducted in a physically secure environment requiring dual control;
    - Subordinate CA operations are conducted in a secure environment comparable to a data centre requiring dual control;
    - RA operations are conducted in a controlled environment, i.e., restricted or private area.

3.2.1 Asset Classification and Control

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for asset classification and control, as stated in the applicable security-related documentation, are being achieved:

- Review asset accountabilities to determine whether owners have been assigned for all major assets;
- Review the inventory of assets and verify the procedures to ensure completeness and accuracy of these lists:

    - Information assets (e.g., databases, data files, system documentation, business continuity plans, user manuals, training materials, etc.);
    - Software assets (e.g., application software, system software, utilities, etc.);
    - Physical assets (e.g., computer and communications equipment, power supplies, air conditioning units, etc.);
    - Services (e.g., computing and telecommunications services).

- Review asset classifications for reasonableness.

3.3 OPERATING SYSTEM AND WEB SERVER CONSIDERATIONS

An operating system or web server review would normally be performed as a separate audit. The purpose of this section is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account, and audit procedures that need to be performed by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact the EC payment security audit and assess management actions taken since the last audit/ review. The IS auditor should review procedures to ensure the following considerations (that should be performed by the appropriate auditee personnel), have been included in an operating system review.

- Removing default CGI scripts that are not needed - these are typically not meant for commercial use.
- The web server should utilise the minimum privileges to execute CGI scripts (for example, on a UNIX system, a web server should not execute as 'root').
- Automatic directory listing should be turned off. If this is available, the program sources could be downloaded for examination for potential vulnerabilities.
- Disabled acceptance of SSIs (Server-Side Includes). SSIs are codes embedded within HTML documents. If these are uploaded to the web server they will execute under the web server privilege.
- Restrict the directories from where CGI scripts can be executed from the web server. This is because if CGI scripts are placed in user directories, there could be security threats.
- Ensure command processors or interpreters such as Perl or command.com have not been included in CGI directories.
- Allocate sufficient memory for CGI scripts to minimise the likelihood of buffer overflows.
- Ensure CGI scripts activities are recorded in a log.
- Check for proper configuration of cookie distribution. Cookies are sent between a web server and client. This could include authentication information. If the cookies are misconfigured, an unauthorized server might be able to retrieve that

cookie, and in theory, could then try to gain unauthorized access to the original web server. In other words, check whether the "secure" value of the cookie has been set to require the browser to send the cookie only over an encrypted session.

- Check to ensure all deadly defaults for the specific application and supporting operating systems are addressed. In order to find out information on the deadly defaults, one can visit the CERT sites (http://www.cert.org), vendor sites, and other security related sites such as http://www.ntsecurity.net for Windows NT.
- Turn off network services that are not needed. If the server is a mail server, http and ftp may not be needed. Opportunities for attacks increase with the number of enabled network services.
- Keep up with the latest operating system (OS) patches. These typically address potential security related OS bugs and holes that have been discovered.
- Use of strong passwords. Standard controls should apply, such as regular reviews of policies, password length and format, frequent forced change of password (e.g., every 30 days), access rights linked to staff movement, unique identifier, regular audit of the effectiveness of the procedures and applications by staff. This is also discussed in the access control Section 3.3.1.1.3.
- Document what is installed and monitor for any changes.
- Run logging and monitor log files. Actions of users should be logged and reviewed.
- Block the ability to know OS and web server information.
- Limit access to the system. Proper authentication techniques are vital. This can come down to having users log onto the system with their own user IDs (never directly as root or administrator) and care being taken to ensure proper authority levels are granted. Different authentication schemes can be utilised such as Kerberos, Radius or LDAP but it comes down to enforcing logins with proper privileges and enforcing strong password usage. Care should also be taken in how a login is achieved. Remote connections should always be avoided across the Internet through the use of a non-secure medium that could easily be captured and read (such as telnet).
- Keep the system up to date with latest fixes and patches. Keep up to date on Bugtraq or CERT advisories, and apply the necessary patches to ensure there is no exposure to any newly discovered vulnerabilities.
- Image, or back up the system at appropriate stages. Backup is mandatory as more reliance is placed on the electronic audit trail. Organisational requirements

should dictate the backup policy and this should be coordinated closely with a disaster recovery plan.

- Stage and test applications and systems on a staging server prior to implementation of systems, applications or changes in a production environment.
- Change default configurations that can endanger security i.e. customise the operating system to the environment where it is implemented.
- Determine whether the web server has been placed on a network that does not carry confidential traffic. This isolates the less secure systems from the secure. Making it difficult for an attacker to pick up or sniff internal traffic for valuable information. Using a firewall as previously mentioned can do this. Another option is to put all database and file servers providing web support service on a protected subnet. It is also important to disable any source routing that would allow the originator to influence routing decisions.

One component often overlooked in the various security models, methods, and protocols, is the end user's computer. No matter what financial service providers or certificate authorities do in software, hardware, or policies, they have no control over the end user's computer. That computer has stored all the digital certificates, most of the consumer's personal information, and quite often, usernames and passwords. People will use the password cache and auto complete features in their browsers, which store information in some very basic forms, even plain text. This use means the consumer's financial and banking data is only as secure as that computer. To further complicate matters, there are many laptop computers used at home and in business. The theft of a portable computer means that they no longer have any security, and only the thief may have access to their data. Controls that can minimise this risk are physical security, access controls and policies as described in the sections above.

3.4 CHANGE MANAGEMENT

A change management review would normally be performed as a separate audit. The purpose of this section is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account and audit procedures that need to be performed by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in previous audit procedures. Where weaknesses were identified, the

IS auditor should assess whether such weaknesses impact the EC payment security audit and assess management actions taken since the last audit/ review.

The auditor should consider performing the following procedures. [Pieter, format appears awkward / inappropriate - needs to be inset or bulleted and the current bullets set in further.]

- Evaluate procedures that ensure that there are approval processes for upgrades and for the implementation of new systems;
- Evaluate control over the segregation of duties between the development staff and operational staff;
- Ensure separate logical development and production environments.

- Describe the entity's controls over changes to its electronic commerce business practices, its transaction integrity controls, its information protection controls, and its electronic commerce systems and supporting technology, which are designed to provide reasonable assurance that:

    - All such changes are approved by management;
    - Changes in business practices are reflected in modified disclosures of such practices;
    - Changes in the manner in which electronic commerce transactions are executed are reflected in modified business practice disclosures;
    - Controls over transaction integrity and information protection continue to function effectively;
    - The corporate security function is aware of all major changes and specify their requirements for all changes that may affect the security environment.

3.5 BUSINESS CONTINUITY PLANNING (BCP)

Audit Procedures

A BCP review would normally be performed as a separate audit. The purpose of this section is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that needs to be taken into account and audit procedures that needs to be performed by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in

previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact the EC payment security audit and assess management actions taken since the last audit/ review.

The auditor should consider performing the following procedures to determine whether the requirements for business continuity planning, as stated in the applicable security-related documentation, are being achieved:

- Any current BCP should address specific e-commerce needs. Determine whether plans are benchmarked with plans of similar organisations or environments. If information about similar organisations is available compare the BCP with those plans. Identify discrepancies;
- Determine whether backups recovery procedures are tested regularly and stored off-site;
- Review the emergency procedures included in the Information Systems Department's disaster recovery plan for completeness of coverage of all of the emergencies that may occur at a data processing site;
- Review the Information Systems Department's list of critical computer resources and determine if it includes e-commerce resources;
- Review documentation to determine whether business continuity planning includes disaster recovery processes for all critical components of a CA system, including the hardware, software and keys;
- Observe whether cryptographic hardware and other keying material is stored securely in vaults requiring dual access;
- Observe whether a locking cage has been employed around dedicated equipment at the hotsite data centre facility.

The auditor should consider performing the following procedures to determine whether the requirements for key compromise, as stated in the applicable security-related documentation, are being achieved:

- Review the procedures to respond to all known or suspected key or critical security component compromises;
- Ensure that disaster recovery procedures include the revocation and re-issuance of all certificates that were signed with the CA's private key in the event of the compromise or suspected compromise of a CA's private key;

- Ensure that procedures are in place for the secure and authenticated revocation of all certificates issued by the CA in the event that a CA has to replace its private key;
- Review the contingency plan for key compromise and determine whether it includes who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures, encrypted data, etc;
- Interview appropriate personnel.

Note: Key compromise is considered one type of "disaster." CA termination is included under business continuity planning, because in the event the CA terminates, policies and procedures should be in place to ensure the continuity of service to customers.

The auditor should consider performing the following procedures to determine whether the requirements for CA termination, as stated in the applicable security-related documentation, are being achieved:

- Review CA termination policies and procedures to minimise potential disruptions as a result of the cessation of their services.
- Interview appropriate personnel.

3.6 ORGANISATIONAL STRUCTURE

Audit Procedures

The auditor should consider performing the following procedures to determine whether the personnel security requirements for job definition, hiring, and training, as stated in the applicable security-related documentation, are being achieved:

- Conduct interviews with human resources management to gain an understanding of the policies and procedures regarding hiring, termination, and related HR processes;
- Examine job descriptions of staff involved in EC payment security activities and assess segregation of duties;

- Review screening reports for staff involved in EC payment security activities and assess adequacy;
- Review confidentiality agreements and ensure they are signed by all staff;
- Review a sample of new hires and the background check log to determine whether background checks have been completed;
- Review a sample of "trusted employees" and confirm whether background checks have been performed;
- Review a sample of recent terminations against the badge access listing and/or network access listing to determine whether access has been cancelled and appropriate exit procedures performed;
- Review training program materials to determine whether key staff receive training related to their functions and cross training is encouraged.

The auditor should consider performing the following procedures to determine whether the security requirements for incident response, as stated in the applicable security-related documentation, are being achieved:

- Review incident reporting and response policies and procedures;
- Review the incident categorisation/classification scheme;
- Review a sample of reported incidents and determine whether incident response policies and procedures were followed;
- Interview personnel responsible for incident reporting and incident response;
- Review logs and reports of disciplinary measures taken;
- Interview personnel responsible for the disciplinary process.

The audit procedures related to intrusion detection are covered in more detail in Section 2.10 below.

3.7 COMPUTER OPERATIONS AND BACKUP

The auditor should consider performing the following procedures to determine whether the requirements for computer operations, as stated in the applicable security-related documentation, are being achieved:

- Review the documented procedures for computer operations to ensure it includes operating procedures and incident management procedures;

- Interview appropriate personnel to determine segregation of duties and separation of development and operational facilities;
- Determine whether any external facilities are used. Evaluate procedures related to this service.

The auditor should consider performing the following procedures to determine whether the requirements for system planning and acceptance, as stated in the applicable security-related documentation, are being achieved:

- Review documentation of the system planning and acceptance process and ensure the following activities are included:
- Capacity planning
- System acceptance
- Fallback planning
- Operational change control (also covered in change control above)
- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the requirements for virus control, as stated in the applicable security-related documentation, are being achieved:

- Review documentation of virus control policies and procedures and ensure it also includes user awareness procedures, regular virus software update and scanning procedures, and virus detection emergency procedures;
- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the requirements for data backup, operator logs and monitoring, as stated in the applicable security-related documentation, are being achieved:

- Review documentation of the processes for data backup, operator logging and monitoring;
- Interview personnel responsible for data backup to gain an understanding of the adequacy of the procedures used to back up the computer system and to maintain and store computer magnetic tapes. Ensure that it includes EC systems;

- Review selected sections of the backup procedures manual and determine whether the procedures are properly documented;
- Select a sample of tape volume serial numbers for EC related backups from the backup tape listing and compare tape serial numbers to the physical tape residing in the tape library to determine whether the tapes are properly accounted for and recorded;
- Obtain and read the contract with the off-site storage vendor, if applicable, to determine whether responsibilities are clearly outlined, and whether a list of authorised personnel is maintained and current;
- Review the backup logs and configuration files for servers (including EC servers such as the web server) to determine whether they are backed up regularly and properly.
- Review documents to determine whether expired and/or defective tapes are destroyed in a controlled manner.

- Ascertain the requirements for network security control, as stated in the applicable security-related documentation, that should at least include descriptions of the following network security control requirements:

    - Ensure there is separation of operational responsibilities for networks from computer operations, where appropriate;
    - Evaluate responsibilities and procedures for the management of remote equipment, including equipment in user areas;
    - Assess controls to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems i.e., ensure encryption, secure protocols and digital certificates are used where applicable;
    - Assess co-ordination of computer and network management activities to optimise system performance and to ensure the consistency of security measures across the IT infrastructure.

3.8 FIREWALL AND ROUTER CONSIDERATIONS

The role of the IS auditor in this respect is to ensure that the firewall/ router review policy covers the following controls and procedures:

- Obtain network diagrams and understand the architecture of the network and the nature and location of network firewalls and routers. The auditor should consider performing the following procedures:

    - Determine the environment in which the firewalls and routers operate. Discuss with management their assessment of the relative hostility of the environment;
    - Obtain an understanding of the role that firewalls and routers play in the network (e.g., Do routers simply provide connectivity or do they also provide control?);
    - Examine the network architecture and identify where firewalls and routers play a role in authentication and authorisation;
    - Understand how changes to the network are initiated and managed and ensure that all changes are approved and monitored.

- Determine whether remote firewall and router administration is avoided, especially over the Internet. The firewall/router also needs to be securely managed to limit the possibility of someone breaking into it. As the protector of the network, the router or firewall is a target for intruders. Managing the firewall/router via the Internet interface is probably the least desirable situation, especially if the management connection is of questionable encryption strength or can be spoofed. Taking care not to allow management ports to be available to the Internet also helps prevent fingerprinting the type of firewall/router used;
- Ensure firewall/router software is upgraded on a regular basis, with patches and upgrades. For software-based firewalls, this applies to the operating system and the firewall software;
- Ensure firewalls/routers are reviewed periodically e.g., through the use of commercial products that can help make this task easier such as the Internet Security Scanner ISS - http://www.iss.net;
- The auditor should consider performing the following procedures related to auditability of routers and firewalls:

    - Through discussion and review of available documentation, determine whether the firewalls and router management and security activity records are being maintained;
    - Ensure that the records are adequate for the needs of the organization;

- Understand the monitoring and review activities performed by network management;
- Ensure that logs are properly configured, monitored, and audited. The firewall product will deny access to unauthorized connections, will show where those attempts originated and what ports they were destined to. There are many types of firewalls that can exist on the host. There are also firewalls that are used to protect networks;
- Determine if information gathered from logs is used to find patterns, misconfigured equipment and break-in attempts. This information can be used to communicate those attempts to the owners of the originating hosts.

- As with most operating systems, firewalls and routers never come out-of-the-box configured to secure any given site, and are only as good as the staff administrating them. Evaluate skills and segregation of duties for staff administering the firewalls. The auditor should consider performing the following procedures:

  - Determine how firewalls and routing tables are created and maintained;
  - Determine how changes to firewalls and routing tables are managed and controlled and whether the control of these changes is limited to a single person at a time;
  - Determine how this person is authenticated;
  - Through discussion with management, understand the types of services and network components to which access is intended to be granted;
  - Review the access tables to determine what access they are providing and the filters used. Document any services which were not intended / authorised;
  - Review the network architecture and the firewalls and routing tables of selected firewalls/routers to determine whether the concept of "least cost path routing" is applied.

- Determine whether filters are as specific as possible. Permissions for inherently dangerous traffic, such as rules that allow remote management, should always be as specific as possible. But less obvious threats are often overlooked;

- If different systems are used for web site and mail, ensure web and mail traffic are not allowed to the entire subnet. Specify mail traffic allowed to the mail server and web traffic to the web server;
- Allowing SMTP traffic to a web server may not seem to be all that large a risk, but it is an unnecessary one: i.e., evaluate whether SMTP traffic is needed;
- The auditor should consider performing the following procedures regarding changes to firewalls and routers:

    - Understand how "read" vs. "read and update" access is granted to the firewalls and router tables;
    - Understand the source of changes to the firewalls, routing, and security tables, whether from a local console only, or from the network as well;
    - If changes can be made from the network, determine how the firewall/router is protected from interference and contamination;
    - If a password is used to control update access, determine who has access to it and how it can be changed;
    - Determine if changes to firewalls and router tables are approved by management and logged;
    - Determine if accountability for changes is maintained to the level of a single individual;
    - Through discussion with management and review of available documentation, understand the population of users that should be granted access by the routers;
    - Review the access tables to determine the definition of the access paths granted and the type of access allowed. Network users should be routed to the specific devices that they are intended to have access to. Document any access which is not intended;
    - Through discussion with management and review of available documentation understand the authentication methods used;
    - Some routers have an alternate access path defined, a dial-in access port. Look at how that is controlled. In particular, if they are using the router as a firewall or some significant security device, determine if a secure id or one-time password is used to access that port, or if the connection is manually controlled.

- The auditor should consider performing the following procedures regarding recoverability of firewalls and routers:

  - Based on our understanding of the network architecture, determine the established firewalls and router redundancy, and the adequacy of the firewall/router configurations to minimize disruption in the event of a problem;
  - Through discussion with management, determine whether a plan has been established for recovery of a single router or multiple routers;
  - Review the recovery plan to ensure it is up-to-date and adequate to address the specific recovery needs of the company;
  - Ensure that the router management techniques and tools provide easy reconfiguration of firewalls and routers in the event they go down.

- The auditor should consider performing the following evaluative procedures on the techniques and tools used for management of the routers and firewalls:

  - Through discussion with management and review of available documentation, determine the techniques and tools used for management of the routers and firewalls;
  - Determine if the procedures are documented;
  - Based on the tools used, ensure that known risks and weaknesses are adequately addressed by the client;
  - Discuss with the network managers the adequacy of the tools to facilitate easy firewall and router configuration;
  - Understand the controls over the password that allows the network manager to control the firewall or router device; ensure that is not easily guessed and is frequently changed to ensure that routers cannot be turned on or off or configurations changed without management approval.

3.9 ENCRYPTION, PRIVACY, AND SECURE PROTOCOLS

One of the objectives of encryption and secure protocols is to ensure information protection, i.e., ensure that private customer information obtained as a result of electronic commerce is protected from uses not related to the entity's business. Primary considerations that should be evaluated by the IS auditor include the following:

- Controls to protect private customer information obtained as a result of electronic commerce and retained in its system from outsiders. For example, customers entering through the Web page can only perform inquiries, execute transactions and obtain information about their own transactions. The auditor can ensure this is controlled by ensuring that all system access from outside the entity, other than for customary electronic commerce transactions through the Web page, (through the Internet, dial up, or other connections) is restricted by one-time passwords and smart cards. This has also been covered in the access control section above.
- Private customer information obtained as a result of electronic commerce is not intentionally disclosed to parties not related to the entity's business unless (1) customers are clearly notified prior to their providing such information or (2) customer permission is obtained after they have provided such information.
  - In some cases, customers may be asked for explicit permission to provide their private information to other parties, and customers have the option to decline. Ensure the entity has a systematic way of identifying those customers who have not granted such permission and ensuring that their private information is not provided to other parties.
  - Determine whether customers are informed when certain requested information is optional and are not required to furnish such information to complete the transaction.
  - Determine whether certain private customer information maintained is encoded to make it extremely difficult, but not impossible, for outsiders to understand it without the appropriate codes and keys.
- Private customer information obtained as a result of electronic commerce is used by employees only in ways associated with the entity's business:
  - Determine whether the entity has strict policies and monitoring procedures to ensure that only certain employees can access private customer information. These policies also set forth ways that customer information should and should not be used.
- The entity maintains controls to protect against its unauthorised access to customer's computers and its unauthorised modification of customer's computer files by ensuring that customer permission is obtained before storing, altering or copying information in the customer's computer or the customer is notified with an option to prevent such activities:

- Evaluate whether the entity requests the customer's permission before it intentionally stores, alters or copies information (such as cookies and other similar files) in the customer's computer;
- Determine whether the entity requests the customer's permission before it performs any diagnostic or inventory on the customer's computer, and evaluate controls related to this process.

The IS auditor should evaluate controls to ensure that:

- Private customer information is protected during transmission by using encryption technology (Secure Sockets Layer (SSL) technology);
- The entity has registered its Domain Name and Internet IP address to protect its Internet identity. The address is unique and no more than one company can have the same address;
- The entity's Web page has a digital certificate which can be checked using features in a standard Web browser. Certificates are covered in detail in the PKI section below;
- The entity's Webmaster updates the site and reviews and tests key Web pages at least daily to ensure that improper content or links have not been added;
- SSL has been configured with the systems software according to the vendor recommendations;
- The entity uses a standard web browser version that supports SSL encryption.

The IS auditor should attempt to obtain a connection to the entity's web site and observe whether SSL is activated when private information and payment information is collected from customers. This would also verify the certificate issuing process.

The aspects related to encryption keys and digital certificates are addressed in the PKI section below.

3.10 PKI AUDIT AND CONTROL CONSIDERATIONS

3.10.1 Key Management Life Cycle Controls

3.10.1.1 Key Generation

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key generation, as stated in the applicable security-related documentation, are being fulfilled:

- Obtain documentation of the cryptographic modules used for key generation;
- If cryptographic modules are internally developed (and internally tested) without external third-party evaluation, consider the functional correctness of the cryptographic module;
- If cryptographic modules are externally tested, obtain a copy of the evaluation report and/or verify the module's FIPS 140-1 certification at the manufacturer's URL i.e.:
  - Root CA key generation occurs within a secure cryptographic device meeting the FIPS 140-1 Level 4 requirements;
  - Sub-CA and RA key generation occurs within a secure cryptographic device meeting the FIPS 140-1 Level 3 requirements;
  - End Entity key generation occurs within a secure cryptographic device meeting the FIPS 140-1 Level 2 requirements;
  - Review the configuration of the cryptographic module and compare it with the configuration specifications provided by the vendor and/or test lab;
  - Observe a key generation ceremony and related event journals (audit trails) produced to ascertain whether key generation ceremony procedures are followed. This may include:
    - Key generation uses a random number generator (RNG) or pseudo random number generator (PRNG) as specified in an ANSI X9 or ISO standard;
    - Key generation uses a prime number generator as specified in an ANSI X9 or ISO standard;
    - Key generation uses a key generation algorithm as specified in an ANSI X9 or ISO standard;
    - Key generation results in key sizes in accordance with the CA's CPS;

- The key generation process takes place in a physically secure environment;
- Key generation takes place with dual control.
- Observe whether cryptographic hardware is tested before key generation;

- Interview appropriate personnel that perform key generation.

3.10.1.2 Key Storage, Backup and Recovery

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key storage, backup and recovery, as stated in the applicable security-related documentation, are being fulfilled:

- Review documentation of the key storage, backup and recovery processes and ensure that:
  - If the CA private key is not exported from a secure cryptographic module and moved to secure storage for purposes of off-lineoff-line processing or backup and recovery, then the CA private key is generated and used within the same cryptographic module and is never exported outside of the cryptographic module.
  - If the CA private key is exported from a secure cryptographic module and moved to secure storage for purposes of off-line processing or backup and recovery, then the private key is exported in a secure key management scheme including:
    - as ciphertext using dual control,
    - as encrypted key fragments using dual control and split ownership, or
    - in another secure cryptographic module such as a key transportation device using dual control.
- For storage in a cryptographic module:
  - If the Root CA private key is stored as cleartext, then the Root CA private key never appears as cleartext outside the secure confines of a cryptographic module meeting at least FIPS 140-1 Level 4 requirements;
  - If the Root CA private key is stored as ciphertext, then the Root CA private key is stored inside the secure confines of a cryptographic module meeting at least FIPS 140-1 Level 3 requirements;

- If the Subordinate CA or RA private key is stored as cleartext, then the Subordinate CA or RA private key never appears as cleartext outside the secure confines of a cryptographic module meeting at least FIPS 140-1 Level 3 requirements;
- If the Subordinate CA or RA private key is stored as ciphertext, then the Subordinate CA or RA private key is stored inside the secure confines of a cryptographic module meeting at least FIPS 140-1 Level 2 requirements.

- Recovery of the CA private key is conducted in the same secure scheme used in the backup process, using dual control;
- The integrity of the CA private key is maintained throughout its life cycle;
- Observe the key storage, backup and recovery process;
- If approved cryptographic modules are used for the storage, backup and recovery of private keys, determine whether test lab documentation is current;
- Interview appropriate personnel who perform key storage, backup and recovery operations.

The auditor should consider performing the following procedures to determine whether the management controls for key storage, backup and recovery, as stated in the applicable security-related documentation, are being adhered to:

- Review documentation of the key storage, backup and recovery process and ensure the following
  - Ensure that the private key is backed up, stored and recovered using dual control in a physically secured environment;
  - Ensure that private key storage and recovery is performed only by authorised personnel;
  - Verify that recovery is to a cryptographic module, in which:
    - The Root CA private key is accessed and imported for purposes of off-line processing or backup and recovery into a cryptographic module meeting the requirements of FIPS 140-1 Level 4 using dual control in a physically secure site;
    - The Subordinate CA private key is accessed and imported for purposes of off-line processing or backup and recovery into a cryptographic module meeting the requirements of FIPS 140-1 Level 3 using dual control in a physically secure site.

- Verify that the backup and recovery period for private and public keys is in accordance with the applicable security-related documentation;
- Verify that backup and recovery procedures are tested on a periodic basis in accordance with the applicable security-related documentation;
- Verify that key storage, backup and recovery actions are recorded in the event journal;
- Observe the key storage, backup and recovery process;
- If approved cryptographic modules are used for the storage, backup and recovery of private keys, determine whether test lab documentation is current;
- Interview appropriate personnel that perform key storage, backup and recovery operations.

3.10.1.3 Key Distribution

This section covers the distribution of the Root CA public key. The distribution of non-Root CA public keys is covered in Certificate Distribution.

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key distribution, as stated in the applicable security-related documentation, are being fulfilled:

- Review documentation of the process for the periodic rekeying of the Root CA and ensure the Root CA public key must be changed (rekeyed) periodically according to the requirements of the applicable CA Certificate Policy and/or CPS.
- Review documentation of the process for the initial distribution of the Root CA public key and ensure the integrity and authenticity of the key and associated parameters are maintained.
- Review documentation of the process for the subsequent distribution of the Root CA public key.
- Review a sample of event journals to determine whether key distribution actions are properly recorded.
- Interview appropriate personnel.

3.10.1.4 Key Escrow

Key escrow refers to the process whereby law enforcement officials can gain access to an escrowed private key.

Audit Procedures

Determine whether the requirements for key escrow, as stated in the applicable security-related documentation, are being fulfilled. The auditor should consider performing the following procedures:

- Review documentation of the storage, backup and recovery controls and procedures of the third party providing escrow services;
- Determine whether digital signature keys are ever subject to key escrow, or any other form of key recovery;
- Review documentation of the CA's key escrow process.
- Review the escrow contract between the involved parties and ensure it outlines the liabilities and remedies between the parties;
- Determine whether key escrow actions by a third party are recorded in the CA's event journal when communicated to the CA;
- Interview appropriate personnel at the CA that perform the key escrow process;
- If possible, interview appropriate personnel of the third party providing escrow services that are involved in the key escrow process.

3.10.1.5 Key Usage

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key usage, as stated in the applicable security-related documentation, are being fulfilled:

- Review key usage documentation and ensure keys are only used for their intended purpose, which is specified during key generation;
- Review policies and procedures relating to key usage and ensure certificate signing is performed by the Root CA using dual control;

- Observe the authentication requirements for the activation and de-activation of the CA private key and ensure the activation of the CA private key is performed using two factor authentication;
- Review a sample of event journals to determine whether key usage actions were properly recorded;
- Interview appropriate personnel.

3.10.1.6 Key Destruction

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key destruction, as stated in the applicable security-related documentation, are adhered to:

- Review documentation of the key destruction process and ensure all copies and fragments of the CA private key are destroyed at the end of the key pair life cycle, using dual control in a physically secure site;
- Review a sample of event journals to determine whether key destruction actions were properly recorded;
- Interview appropriate personnel that perform the destruction process.

3.10.1.7 Key Archival

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key archival, as stated in the applicable security-related documentation, are being achieved:

- Review documentation of the key archiving process, and ensure archived keys are periodically verified to ensure that they are properly destroyed upon expiration;
- Observe the key archiving process and ensure:

- All archived keys are destroyed at the end of the archive period using dual control in a physically secure site, as required by the applicable security-related documentation;
- Keys held in archive meet the requirements for key storage, backup and recovery;
- Mechanisms are in place to ensure that archived keys are never put back into production;
- Mechanisms are in place to ensure that the archived keys are recovered for the shortest time period technically possible;
- Private keys are archived to permit access to data after the certificate expires.
- Interview appropriate personnel that perform key archiving operations;
- Ensure the archival process includes entries into the event journal.

3.10.2 Device Life Cycle Management

For purposes of this section, "device" refers to cryptographic hardware and other hardware used for sensitive CA operations.

Audit Procedures

3.10.2.1 Device Shipment

Determine whether the requirements for device shipment, as stated in the applicable security-related documentation, are adhered to. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to device shipment;
- Observe the receipt of cryptographic hardware from the manufacturer via registered mail with tamper evident envelopes and seals intact;
- If observation is not possible in the two guidelines above, interview appropriate personnel;
- Ascertain the requirements for physical protection of cryptographic hardware as stated in the applicable security-related documentation.

3.10.2.2 Device Receipt

The auditor should consider performing the following procedures to determine whether the requirements for device receipt, as stated in the applicable security-related documentation, are adhered to:

- Review policies and procedures documentation related to device receipt;
- Observe the inspection of the tamper evident packaging upon receipt of cryptographic hardware from the manufacturer;
- Observe the process of acceptance testing and verification of firmware settings;
- Observe for integrity the process of testing devices used for private key storage and recovery and the interfaces to these devices;
- For the guidelines above, if observation is not possible, interview appropriate personnel;
- For a sample of devices that have been received recently, check the event journal for the recording of the device receipt.

3.10.2.3 Device Pre-Use Storage

Determine whether the requirements for device pre-use storage, as stated in the applicable security-related documentation, are being adhered to. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to pre-use storage, and ensure that, to prevent tampering, the device is stored in a secure site, with access limited to authorised personnel. The procedures should have the following characteristics:
  - Inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device;
  - Access control processes and procedures to limit physical access to authorised personnel only;
  - All successful or failed physical access attempts are recorded in an event journal;
  - Incident processes and procedures to handle abnormal events, security breaches, and investigation and reports;
  - Audit processes and procedures to verify the effectiveness of the controls.

- Observe whether cryptographic hardware is stored in tamper resistant envelopes;
- Select a sample of cryptographic hardware tokens from the inventory listing and verify their status and location;
- Interview appropriate personnel;
- For devices entered or removed, determine whether these actions were properly recorded in an event journal;
- Ensure the handling of cryptographic hardware is performed in the presence of no less than two trusted employees.

3.10.2.4 Device Installation and de-installation

Determine whether the requirements for device installation, as stated in the applicable security-related documentation, are complied with. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to device installation and de-installation;
- Observe the process of device installation and ensure the installation of cryptographic hardware is performed in the presence of no less than two trusted employees;
- For the guideline above, if observation is not possible, interview appropriate personnel;
- For a device that has been installed or de-installed, determine whether the device installation / de-installation was properly recorded in an event journal.

3.10.2.5 Device Usage

Determine whether the requirements for device usage, as stated in the applicable security-related documentation, are being achieved. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to device usage and ensure they are followed:
  - to verify correct processing on a periodic basis;
  - to provide diagnostic support during trouble shooting.
- Interview appropriate personnel;

- Select a sample of device usage events and determine whether they were properly recorded in an event journal.

3.10.2.6 Device Service and Repair

Determine whether the requirements for device service and repair, as stated in the applicable security-related documentation, are fulfilled. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to device service and repair and ensure:
- The service or repair site is a secure site with inventory control and access limited to authorised personnel;
- The handling of cryptographic hardware is performed in the presence of no less than two trusted employees;
- The designation of a device for service and repair is recorded in an event journal;
- Upon the receipt of cryptographic hardware that has been serviced or repaired, policies and procedures require acceptance testing and verification of firmware settings.
- Interview appropriate personnel;
- Select a device servicing or repair event and determine whether it was properly recorded in an event journal.
-

3.10.3 Certificate Life Cycle Controls

3.10.3.1 Initial Certificate Registration

Audit Procedures

Determine whether the requirements for the certificate request, as stated in the applicable security-related documentation, are complied with:

- For the Subordinate CA initial certificate registration, the auditor should consider performing the following procedures:

- Review documentation to ascertain that the Root CA (or Superior CA) documents its requirements for the CA certificate request and makes them available to the Sub-CA;
- Interview appropriate personnel.

- For the End Entity initial certificate registration, the auditor should consider performing the following procedures:
  - Review documentation to ascertain whether the End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity submits the required registration information to the RA;
  - Interview appropriate personnel.

- For the initial certificate registration in general, the auditor should consider performing the following procedures:

  - If an on-line application is utilised to collect application information, obtain documentation of the on-line application processing to ascertain that:
    - The online form is adequately protected from unauthorised modification;
    - The on-line form requires completeness of information prior to submission to the registration authority (RA);
    - The submission of the application data is logically secured while in transmission.
  - If an off-line or manual application form is utilised, obtain documentation of application processing to ascertain whether the off-line form collects all relevant information, as required in the Certificate Policy, to perform the validation step;
  - Review documentation of the acceptance process and interview appropriate personnel to determine whether subscribers are required to review and accept the terms and conditions of the Certification Practice Statement and subscriber agreements prior to the submission of a certificate application;
  - If a web-wrap agreement is utilised, ascertain the method utilised to manage the changes of the related on-line subscriber agreement, reviewed and approved by the applicant as follows:
    - Review configuration management controls over online version of agreements;
    - Review event journals (audit trails) of changes to the agreements;
    - Review notifications to existing subscribers.

Determine whether the requirements for the registration (application) process, as stated in the applicable security-related documentation, are complied with. The auditor should consider performing the following procedures:

- For the Subordinate CA registration (application) process, the auditor should consider performing the following procedures:
  - Review documentation to ascertain whether the Sub-CA submits the required certificate request information to the Root CA (or Superior CA);
  - Review documentation to ascertain whether the Sub-CA submits evidence to the Root CA (or Superior CA) that it possesses the private key corresponding to the public key;
  - Interview appropriate personnel.

- For the End Entity registration (application) process, the auditor should consider reviewing documentation to ascertain that:
  - The End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity submits the required credentials to the RA, as well as evidence to the RA that it possesses the private key corresponding to the public key;
  - Interview appropriate personnel.

- For the registration (application) process in general, the auditor should consider performing the following procedures:

  - Interview appropriate personnel to gain an understanding of certificate request processing;
  - Review procedures manuals;
  - Observe whether online certificate enrolment requests are encrypted during transmission (e.g., using an SSL session);
  - Observe whether online certificate applications require completion of all required fields in order to be processed;
  - Select a sample of issued certificates and review the CA's issuance checklists or procedures to assess the completeness of the subscriber-provided information;
  - Re-perform the authentication process for a sample of issued certificates;

- Observe and determine whether the CA system prevents a certificate from being issued if any of the required fields is incomplete;
- Select a sample of selected certificate files and determine whether they contain appropriate retained documentation with respect to the authentication process;
- Observe and determine whether only authorised individuals are permitted access to CA systems for processing and issuance of certificate enrolment/revocation requests.
- Review a sample of the CA system logs of authentication steps by user ID, date, and time to determine whether these are complete;
- Interview CA system validation personnel and review quality control evaluations to gain an understanding of the quality control reviews of staff related to certificate issuance.

Determine whether the requirements for the registration (application) validation process, as stated in the applicable security-related documentation, are being complied with. The auditor should consider performing the following procedures:

- For the Subordinate CA registration (application) validation process, the auditor should consider reviewing documentation to ascertain that:
  - The Root CA (or Superior CA):
    - authenticates the Sub-CA;
    - authorises the Sub-CA's CA certificate request;
    - verifies the public and private key of the Sub-CA;
    - checks the data accuracy of the Sub-CA's CA certificate request.
    - when the Root CA (or Superior CA) detects duplicate public keys, the certificate request is rejected and the original certificate is revoked;
  - Interview appropriate personnel.

- For the End Entity registration (application) validation process, the auditor should consider reviewing documentation to ascertain that:

  - The RA:
    - authenticates the End Entity;
    - authorises the End Entity's registration request;
    - verifies the public and private key of the End Entity;
    - submits the required certificate request information to the CA;

- submits the required authentication data to the CA.

- The CA authenticates the RA for the registration request;
- The CA checks the data accuracy of the RA's certificate request;
- When the CA detects duplicate public keys, the certificate request is rejected and the original certificate is revoked;
- Interview appropriate personnel.

- For the registration (application) validation process in general, the auditor should consider performing the following procedures:

  - Review documentation of the certificate application validation process.
  - Ascertain whether personnel performing the certificate application validation process are adequately trained, understand their roles and responsibilities and possess the requisite skills, education and trustworthiness in accordance with the CPS as follows:
    - Review the requirements of the CP/CPS;
    - Observe personnel performing certificate application validation processing;
    - Interview appropriate personnel.

  - Ascertain whether procedures controlling the authentication of validation personnel against the certificate management system exist and are followed;
  - Review documentation of the authentication and identification procedure:
    - Interview appropriate personnel;
    - Determine the means of authentication, including digital certificates, passwords, tokens or biometrics;
    - Determine the management process for approving and updating user access lists;
    - Observe the authentication and validation procedure performed by certificate application validation personnel.

  - Review documentation and interview appropriate personnel to ascertain whether quality control procedures over the certificate registration (application) validation process exist and are followed. Specifically ascertain whether:

- An individual independent of the validation process performs periodic review of validation procedures;
- The results of such periodic reviews are summarised and presented to management in a timely manner;
- Quality control trend information is maintained and periodically reviewed to identify negative trends that require management attention or procedural changes;
- Identified errors are corrected in a timely manner;
- The results of each quality assurance review provide input into a continuous improvement process.

- Select a sample of quality control reviews performed by the CA to ascertain whether:
  - The individual performing the quality control review is independent of the validation process;
  - The results were properly summarised and reported to management;
  - Corrective action has been taken on deficiencies noted in quality control reviews.
- If a manual form is used to submit certificate application data, review controls over the integrity of data input into the certificate management system:
  - The auditor should ascertain whether the following procedures are performed:
    - manual review by the subscriber of information entered into the system;
    - secondary review by CA personnel; and/or online edit checks in co-ordination with the validation procedures.
  - The auditor should consider selecting a sample of manual forms submitted by the subscriber and compare the actual information to that entered in the system;
  - Select a sample of certificates issued by the CA and re-perform the validation steps. In doing so, consider the following:
    - validation steps documented in the CPS;
    - related system based controls to validate application data;
    - appropriateness of the source of automated validation data.
- Review documentation of the process for processing incomplete or unvalidated certificate applications;

- Observe personnel processing incomplete or unvalidated certificate applications;
- Interview appropriate personnel;
- Review documentation and interview appropriate personnel to ascertain the controls in place under which the RA validates that the subject of the certificate application has control over the private key corresponding to the public key submitted with the application;
- Review documentation of the event journal (audit trail) updating process for critical validation processing;
- Review documentation to ascertain whether the audit trail contains sufficient information to identify the individual or system responsible for performing the validation steps and approving the issuance of a digital certificate.

3.10.3.2 Subsequent Certificate Renewal

The difference between certificate renewal and the initial certificate application is that the renewed certificate contains essentially the same information and the same public key, with some minor changes (e.g., the issuance date or expiration date will change). Therefore, less information may be required to be submitted by the End Entity or the Subordinate CA.

Audit Procedures

Determine whether the requirements for certificate renewal, as stated in the applicable security-related documentation, are being fulfilled.

- For certificate renewal in general, the auditor should consider performing the following procedures:

  - Obtain documentation of the certificate renewal process and ensure it specifies the following:
    - CA only renews certificates that it previously issued;
    - The CA renews a certificate only after validating the certificate renewal request;
    - The CA or RA, if used, has a procedure for notifying subscribers prior to the expiration of their certificate of the need for renewal.
  - Select a sample of certificate renewal requests and ascertain that

- the CA validated the signature on each Certificate Renewal Data submission,
- verified the existence and validity of the certificate to be renewed; and
- verified that the request meets the specific requirements of the CPS;

- Select a sample of renewal requests and renewed certificates to ascertain that the CA has not renewed an expired certificate;
- Ascertain whether only trusted personnel are allowed to perform certificate renewal functions;
- Ascertain that the Certificate Renewal Data contains:
  - The Distinguished Name of the End Entity;
  - The Serial Number of the certificate; and
  - The requested Validity Period.

Determine whether the requirements for subsequent certificate rekey, as stated in the applicable security-related documentation, are being fulfilled:

- For Subordinate CA certificate renewal, the auditor should consider reviewing documentation to ascertain that:
  - The Root CA (or Superior CA) documents its requirements for the CA certificate renewal request and makes them available to the Sub-CA;
  - The Sub-CA submits the required certificate renewal request information, including the unexpired Sub-CA certificate, to the Root CA (or Superior CA);
  - The Sub-CA signs the CA certificate renewal request using the unexpired Sub-CA private key corresponding to the unexpired Sub-CA certificate;
  - The Root CA (or Superior CA) authenticates the Sub-CA by verifying the signed CA renewal request using the unexpired Sub-CA certificate;
  - The Root CA (or Superior CA) verifies the unexpired Sub-CA certificate;
  - The Root CA (or Superior CA) checks the data accuracy of the Sub-CA's CA certificate renewal request;
  - Interview appropriate personnel.

- For End Entity certificate renewal, the auditor should consider reviewing documentation to ascertain that:

  - The End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity submits the required registration renewal information, including the unexpired End Entity certificate, to the RA

and the End Entity signs the registration renewal request using the unexpired End Entity private key corresponding to the unexpired End Entity certificate;

- The RA authenticates the End Entity by verifying the signed registration renewal request using the unexpired End Entity certificate;
- The RA authorises the End Entity's registration renewal request;
- The RA verifies the unexpired End Entity certificate;
- The RA submits the required certificate renewal request information, including the unexpired End Entity certificate, to the RA;
- The RA submits the required authentication data to the CA;
- The CA checks the data accuracy of the RA's certificate renewal request;
- Interview appropriate personnel.

3.10.3.3 Subsequent Certificate Rekey

The difference between certificate rekey and the initial certificate application is that the certificate contains the same information, with some minor changes (e.g., the issuance date or expiration date will change); however the public key is different. Therefore, less information may be required to be submitted by the End Entity or the Subordinate CA.

Audit Procedures

Determine whether the requirements for subsequent certificate rekey, as stated in the applicable security-related documentation, are achieved:

- For the Subordinate CA, the auditor should consider reviewing documentation to ascertain that:

  - The Root CA (or Superior CA) documents its requirements for the CA certificate rekey request and makes them available to the Sub-CA;
  - The Sub-CA submits the required certificate rekey request information, including the unexpired Sub-CA certificate, to the Root CA (or Superior CA);
  - The Sub-CA submits evidence to the Root CA (or Superior CA) that it possesses the new private key corresponding to the new public key;
  - The Root CA (or Superior CA):
    - Authenticates the Sub-CA by verifying the signed CA rekey request using the unexpired Sub-CA certificate;
    - Authorises the Sub-CA's CA certificate rekey request;

- Verifies the unexpired Sub-CA certificate;
- Verifies the new public and private key of the Sub-CA;
- Checks the data accuracy of the Sub-CA's CA certificate rekey request;
- Detects possible duplicate public keys, and if found rejects the certificate rekey request and revokes the original certificate.

- Interview appropriate personnel.

- For the End Entity, the auditor should consider reviewing documentation to ascertain that:

  - The End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity submits the required registration rekey information, including the unexpired End Entity certificate, to the RA and the End Entity signs the registration rekey request using the End Entity private key corresponding to the unexpired End Entity certificate;
  - The RA:
    - Authenticates the End Entity by verifying the signed rekey renewal request using the unexpired End Entity certificate;
    - Verifies the unexpired End Entity certificate;
    - Verifies the new public and private key of the End Entity;
    - Submits the required certificate rekey request information, including the unexpired End Entity certificate, to the CA;
    - Submits the required authentication data to the CA.
  - The CA authenticates the RA for the registration rekey request;
  - The CA checks the data accuracy of the RA's certificate rekey request;
  - When the CA detects duplicate public keys, the certificate rekey request is rejected and the original certificate is revoked;
  - Interview appropriate personnel.

- For subsequent certificate rekey in general, the auditor should consider reviewing documentation to ascertain that:

  - The CA only rekeys certificates that it previously issued;
  - The CA rekeys a certificate only after validating the certificate rekey request;
  - Certificate rekey is allowed only after performing all three of the following:
    - The CA validates the signature on the Certificate Rekey Data submission;

- The CA verifies the existence and validity of the certificate to be rekeyed;
- The CA verifies that the request, including the extension of the validity period, meets the requirements defined in the CPS.

- The CA or RA, if used, has a procedure for notifying subscribers prior to the expiration of their certificate of the need for rekey;
- Interview appropriate personnel.

3.10.3.4 Certificate Issuance

Audit Procedures

Determine whether the requirements for certificate issuance, as stated in the applicable security-related documentation, are complied with. For Subordinate CA and End Entity certificate issuance, the auditor should consider performing the following procedures:

- Review documentation of the certificate issuance process;
- Review documentation of the procedures used by the CA to ensure uniqueness of distinguished name and to determine that the public key is unique;
- Review documentation to determine whether the CA generates X.509 version 3 certificates with key usage fields, validity periods and extension fields in accordance with the proper X.509 version 3 syntax;
- Review documentation to determine whether the issuing CA verifies its own digital signature for the certificate;
- Interview appropriate personnel.

Determine whether the requirements for certificate distribution upon subscriber acceptance, as stated in the applicable security-related documentation, are complied with. For Subordinate CA and End Entity certificate issuance, the auditor should consider performing the following procedures:

- Review documentation of the certificate distribution process (e.g., process for updating the certificate repository);
- Review documentation to determine whether certificates are distributed only upon subscriber acceptance;

- Determine the means of subscriber acceptance and develop tests of controls or substantive tests as appropriate;
- Interview appropriate personnel.

Determine whether the requirements for certificate receipt and verification by the subscriber, as stated in the applicable security-related documentation, are fulfilled.

- For Subordinate CA certificate issuance, the auditor should consider reviewing documentation to determine whether:

    - The Root CA sends the required certificate response data to the Sub-CA;
    - The Sub-CA authenticates the Root CA (or Superior CA);
    - The Sub-CA checks the data accuracy of the certificate;
    - The Sub-CA verifies the certificate;
    - Interview appropriate personnel.

- For End Entity CA certificate issuance, the auditor should consider reviewing documentation to determine whether:

    - The CA sends the required certificate response data to the RA;
    - The RA authenticates the CA;
    - The RA matches the certificate response to the original registration request;
    - The RA sends the required registration response data to the End Entity;
    - The End Entity checks the data accuracy of the certificate;
    - The End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity verifies the certificate;
    - Interview appropriate personnel.

If required by the applicable CA Certificate Policy, determine whether the requirement for the CA to notify the subscriber of the issuance of a certificate in an out-of-band communication, as stated in the applicable security-related documentation, is complied with.

- For Subordinate CA certificate issuance, the auditor should consider performing the following procedures:

    - Review documentation of the out-of-band communication process;
    - Assess the strength of the out-of-band communication process;

- Select a sample of certificates issued and review the out-of-band communication for each certificate;
- Review documentation to ascertain whether the Sub-CA system (hardware, software, etc.) operates according to specifications such that the Sub-CA handles the out-of-band notification from the Root CA;
- Interview appropriate personnel.

- For End Entity certificate issuance, the auditor should consider performing the following procedures:

  - Review documentation of the out-of-band communication process;
  - Assess the strength of the out-of-band communication process;
  - Select a sample of certificates issued and review the out-of-band communication for each certificate;
  - Review documentation to ascertain whether the End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity handles the out-of-band notification from the CA;
  - Interview appropriate personnel.

3.10.3.5 Certificate Distribution

This section covers the distribution of non-Root CA public keys.

Audit Procedures

Determine whether the requirements for certificate distribution, as stated in the applicable security-related documentation, are achieved. The auditor should consider performing the following procedures:

- Review certificate distribution documentation and ensure that certificates are distributed to relying parties in accordance with business requirements;
- Interview appropriate personnel.

3.10.3.6 Certificate Revocation

Audit Procedures

Ascertain the requirements for certificate revocation as stated in the applicable security-related documentation. The applicable security-related documentation should at least address the following:

- The applicable CA Certificate Policy and/or CPS specifies:
  - Who may request a certificate revocation;
  - Under what circumstances a certificate revocation request may be made;
  - Under what circumstances a certificate must be revoked.
- The RA authenticates the entity requesting revocation of a certificate;
- The RA verifies the authority of the entity requesting revocation of a certificate;
- The RA submits certificate revocation requests to the CA in an authenticated manner;
- The RA receives and verifies the confirmation that the CA has received the revocation request;
- The CA provides an authenticated acknowledgement of the revocation to the requesting entity;
- Certificate revocation requests are processed and validated in accordance with the requirements of the CPS;
- The CA updates the CRL upon certificate revocation;
- The CA provides an authenticated acknowledgement of the revocation to the entity whose certificate has been revoked.

Determine whether the requirements for certificate revocation, as stated in the applicable security-related documentation, are fulfilled. The auditor should consider performing the following procedures:

- Review documentation of the certificate revocation process;
- If revocation is allowed by individuals other than the subscriber, review documentation to ascertain whether notices of revocation are transmitted in an out-of-band fashion to the subscriber;
- Select a sample of revocations and ascertain whether an out-of-band communication occurred;

- Review documentation to gain an understanding of the event journals (audit trails) related to certificate revocations that are maintained;
- Test the accuracy of the event journals (audit trails) when testing the certificate revocation process;
- Select a sample of revocation requests and ascertain that the revocation request was properly validated prior to updating the certificate status and that the CRL or other status mechanism was updated appropriately;
- Reconcile the status of a selection of certificates within the repository to those in the CRL;
- Review documentation to determine whether only trusted personnel are allowed to perform certificate revocation functions;
- Review a sample of revocation transactions (e.g., revocation requests, including revocation/regeneration records) and assess the completeness and accuracy of certificate status records in the CA system;
- Review a sample of certificate revocations and determine whether a valid revocation/regeneration request has been received for certificates that have been revoked and/or regenerated;
- Interview appropriate personnel.

3.10.3.7 Certificate Suspension

Audit Procedures

Determine whether the requirements for certificate suspension, as stated in the applicable security-related documentation, are achieved. The auditor should consider performing the following procedures:

- Review documentation of the certificate suspension process and ensure it specifies who may request a suspension, under what circumstances a certificate suspension request may be made, and under what circumstances a certificate must be suspended;
- If suspension is allowed by individuals other than the subscriber, review documentation to ascertain whether notices of suspension are transmitted in an out-of-band fashion to the subscriber;
- Select a sample of suspensions and ascertain whether an out-of-band communication occurred;

- Review documentation to gain an understanding of the event journals (audit trails) that are maintained related to certificate revocations;
- Test the accuracy of the event journals (audit trails) when testing the certificate revocation process;
- Select a sample of suspension requests and ascertain whether the suspension request was properly validated prior to updating the certificate status, and that the CRL or other status mechanism was updated appropriately;
- Reconcile the status of a selection of certificates within the repository to those in the CRL;
- Review documentation to determine whether only trusted personnel are allowed to perform certificate suspension functions;
- Review a sample of suspension transactions (e.g., revocation requests) and assess the completeness and accuracy of certificate status records in the CA system;
- Review a sample of certificate revocations and determine whether a valid suspension request has been received for certificates that have been suspended;
- Review documentation that specifies under what circumstances a request may be made to lift a certificate suspension;
- Review a sample of requests to lift suspensions and ascertain whether they were properly validated;
- Interview appropriate personnel.

3.10.3.8 Certificate Revocation List (CRL) Processing

Audit Procedures

Determine whether the requirements for CRL processing, as stated in the applicable security-related documentation, are complied with. The auditor should consider performing the following procedures:

- Review documentation to gain an understanding of the process to generate CRLs and ensure that appropriate controls exist to ensure completeness of each generation of the CRL;
- Review documentation of the CA's CRL management process and perform the following procedures:

- Obtain documentation of the CRL management process and ensure only trusted personnel are allowed to perform CRL management functions;
- Review backup procedures for the archival of CRLs;
- Review personnel security policies and procedures related to the roles and responsibilities of trusted personnel.

- Review procedures to ensure that the CA makes the CRL available to the appropriate relying parties and evaluate for appropriateness;
- Review controls to ensure that a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period. Test check through a sample of revoked certificates;
- Select a sample of days that a CRL was to be published, archived, and checked and ascertain that the CRL actions were performed in accordance with the policies within the CPS;
- Review the processes in place to identify when the distribution of a CRL to a relevant party fails;
- Review documentation to ascertain that the CRL has been digitally signed by the appropriate CA digital certificate prior to issuance;
- If required by the CPS or other service level agreements, review controls over the distribution of the CRLs to ensure timely and correct distribution to all relevant parties;
- Test the accuracy of the event journals (audit trails) when testing the CRL management process;
- Interview appropriate personnel.

3.11 INTRUSION DETECTION

Audit procedures and considerations

This section contains considerations for the IS auditor. Some of these considerations were covered in an operating system/server vulnerability or a firewall review. Where applicable, this is indicated for each consideration mentioned below. The IS auditor needs to ensure that these aspects were covered in the appropriate review. This can be done by evaluating the results of such review and evaluating the impact of negative findings on the risks in the intrusion detection area.

The implementation of the aspects mentioned below, will serve as preventative as well as detective controls for intrusion. The role of the IS auditor is to determine whether the following actions are performed by the organisation. (The areas impacted are also noted for each point, where applicable).

- Establish and maintain regular backup schedules and policies, particularly for important configuration information - *operating system and server vulnerabilities.*
- Establish and maintain appropriate password policies, especially access to highly privileged accounts - *operating system, server vulnerabilities, and access control*
- Implement properly designed firewalls - these can track all traffic in and out of the site, logging and inspecting every packet of information to ensure its legitimacy – *firewalls.*
- Keep all software up-to-date: implementing all security fixes and patches as they are released will go a long way to reducing vulnerability to these attacks. As available, install patches to guard against TCP SYN flooding – *firewalls and operating system.*
- Disable any unused or unneeded network services - *firewalls and operating system/ server vulnerabilities.*
- Enable quota systems on operating system if available i.e., limit users and programs to a certain amount of resources only – *operating system and server vulnerabilities*;
- If the operating system supports partitions or volumes, partition the file system so as to separate critical functions from other activities – *operating system and server vulnerabilities.*
- Establish system performance baselines and observe daily activity for aberrations - *server vulnerabilities.*
- Routinely examine the physical security environment with respect to current needs - *server vulnerabilities and physical security.*
- Use tools (e.g., Tripwire) to detect changes in configuration information or other files - *server vulnerabilities.*
- Invest in surplus and fault-tolerant network configurations.
- Switch on audit logs for all key servers: when efficiently and effectively configured and monitored, these logs will provide adequate information to identify and investigate any problems.

- Install intrusion detection software: if properly configured, this software will quickly identify known patterns of attack and immediately shut out only the attacker, while sounding the appropriate alarms.
- Hire the right people: make sure your technical personnel completely understand the issues, the technologies and the solutions.
- Test defenses regularly: the rapid rate of change in both the technology area and the hacking community means defenses must be tested on a regular basis.
- Design the network to isolate attacks: if the worst happens and the hacker gets inside, appropriate network configuration, firewalls and other tools will ensure any damage the hacker could cause is isolated to a small area – *firewalls*;
- Have an incident response plan: identifying, reacting to and resolving the problem immediately is the real business dilemma. Identify who should respond and test the plan. Establish procedures for determining the seriousness of the breach.
- Focus on preventative measures: swift, large volume, automated attacks require sophisticated, automated defense mechanisms. Identifying a problem an hour later and then trying to trace and resolve it is not an option.
- Gather evidence: understanding how to identify, gather and manage legal evidence to ensure the appropriate legal action can be taken against a hacker should be a key element of defense system design.
- Educate: constant awareness and updating of knowledge is the best defense to any attack - *server vulnerabilities.*
- Use network or file scanning tools to detect Distributed Denial of Service (DdoS) attacks and keep these up to date with new developments and types of attacks.
- Determine whether the system was designed to avoid allocating system resources for a potential user session before authentication is complete. Doing this would reduce denial of service attacks based on initiating many log-on attempts.
- Use a real-time system that can detect known attack signatures and patterns, as well as suspicious activity, including probes of the network or critical systems and unauthorized attempts to modify access control mechanisms. The system should be configurable to provide for immediate and automated alerts to such activity, and provide for configurable actions such as logging and automatically terminating the session.
- Immediate and tactful response is necessary in the event of a threat, attack, system compromise, or misuse of network resources. An Incident Response

Team should be formed and trained to respond to an identified security event. Automated response capabilities should be incorporated whenever possible.

- Tools for intrusion management therefore will include: use of monitoring software, the results of which are checked within a specific time-frame; automatic time-out; trend analysis; benchmarking; survey of markets for latest detection tools; patches and anti-virus software, as well as a system wide audit program.
- A system-wide audit program should be implemented to provide for immediate and full logging of activity to provide for user accountability. A central repository for the audit logs will provide immediate and historical reference in response to an investigation or management request for information. The program should also include security and statistical analysis tools to evaluate the audit logs. The audit program should include procedures to verify the integrity of individual systems and for compliance with existing system and security policies and procedures.

Determine whether the security requirements for incident response as stated in the applicable security-related documentation are achieved. The auditor should consider performing the following procedures:

- Review incident reporting and response policies and procedures;
- Review the incident categorisation/classification scheme;
- Review a sample of incident reports;
- Review a sample of reported incidents and determine whether incident response policies and procedures were followed;
- Interview personnel responsible for incident reporting and incident response;
- Review logs and reports of disciplinary measures taken;
- Interview personnel responsible for the disciplinary process.

APPENDIX B

GLOSSARY OF TERMS

The definitions of terms in this glossary are defined below in the context in which they were used in throughout this dissertation. These definitions were obtained from various Internet Online dictionaries and glossaries at the following Internet addresses:

http://whatis.com
http://www.onelook.com
http://www.pcwebopaedia.com
http://whatis.techtarget.com/
http://www.webopedia.com

Term	Definition
ANSI (X9)	*ANSI* (American National Standards Institute) is the primary organisation for fostering the development of technology standards in the United States. *ANSI* works with industry groups and is the U.S. member of the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). Long-established computer standards from *ANSI* include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI). The X9 standard refers to standards for financial/banking.
Authentication	The process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), *authentication* is commonly done through the use of log-on passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The action of verifying information such as identity, ownership, or authorisation.
Backbone	A *backbone* is a larger transmission line that carries data gathered from smaller lines that interconnect with it. 1) At the local level, a *backbone* is a line or set of lines that local area networks connect to for a wide area network connection or within a local area network to span distances efficiently (for example, between buildings). 2) On the Internet or other wide area network, a *backbone* is a set of paths that local or regional networks connect to for long-distance interconnection. The connection points are known as network nodes.
Biometric authentication	A security measure for checking a network user's identity through the use of certain characteristics unique to the user such as a user's retina,

Bits	A *bit* (short for *binary digit*) is the smallest unit of data in a computer. A *bit* has a single binary value, either 0 or 1. Although computers usually provide instructions that can test and manipulate *bits*, they generally are designed to store data and execute instructions in *bit* multiples called bytes. In most computer systems, there are eight *bits* in a byte. The value of a *bit* is usually stored as either above or below a designated level of electrical charge in a single capacitor within a memory device.
Buffer overflow	A *buffer overflow* occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, *buffer overflow* is an increasingly common type of security attack on data integrity. In *buffer overflow* attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. *Buffer overflow* attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
Certification authorities (CA)	A *CA* is a person or organisation that creates and manages issues around digital certificates.
Certificates	A *certificate* is an electronic document binding some pieces of information together such as a user's identity and public key – which is the key known to all in encryption and used to verify signatures.
Cgi-scripts	In computer programming, a *script* is a program or sequence of instructions that is interpreted or carried out by another program rather than by the computer processor (as a compiler program is). Some languages have been conceived expressly as *script* languages. In the context of the World Wide Web, Perl, VBScript, and similar *script* languages are often written to handle forms input or other services for a Web site and are processed on the Web server. In general, *script* languages are easier and faster to code in than the more structured and compiled languages such as C and C++ and are ideal for programs of very limited capability or that can reuse and tie together existing compiled programs. However, a *script* takes longer to run than a compiled program since each instruction is being handled by another program first (requiring additional instructions) rather than directly by the basic instruction processor.
Command processors	A program that accepts commands from the keyboard and causes the commands to be executed.
Console	(1) The combination of display monitor and keyboard (or other device that allows input). Another term for *console* is terminal. The term *console* usually refers to a terminal attached to a minicomputer or mainframe and used to monitor the status of the system. (2) Another term for monitor or display screen.

	(3) A bank of meters and lights indicating a computer's status, and switches that allow an operator to control the computer in some way.
Cookies	A *cookie* is information that a Web site puts on your har disk so that it can remember something about you at a later time. (More technically, it is information for future use that is stored by the server on the client side of a client/server communication.) Typically, a *cookie* records your preferences when using a particular site. Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user previously or anything about your previous visits. A *cookie* is a mechanism that allows the server to store its own information about a user on the user's own computer. You can view the *cookies* that have been stored on your hard disk (although the content stored in each *cookie* may not make much sense to you). The location of the *cookies* depends on the browser. Internet Explorer stores each *cookie* as a separate file under a Windows subdirectory. Netscape stores all *cookies* in a single cookies.txt fle. Opera stores them in a single cookies.dat file. *Cookies* are commonly used to rotate the banner ads that a site sends so that it doesn't keep sending the same ad as it sends you a succession of requested pages. They can also be used to customise pages for you based on your browser type or other information you may have provided the Web site. Web users must agree to let *cookies* be saved for them, but, in general, it helps Web sites to serve users better.
Certificate Practice Statement	A *Certificate Practice Statement* (CPS) is a statement of the practices which a Certification authority employs in issuing and managing certificates.
Cryptographic module	Hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes or both.
Cryptograhic techniques	Techniques used to encrypt (cipher or code) a message in a way that the resulting coded message can be decrypted (deciphered or decoded) only by holders of the appropriate "key"
Deadly defaults	A deadly default is simply a pre-set configuration that is by default insecure.
Dial-up server	A *dial-up server* is a host computer on a network that answers requests for information from it. The server can be accessed by dialling up with a modem from a remote location. The term *server* is also used to refer to the software that makes the process of serving information possible.
Digital cash	Digital cash is an electronic payment system. It provides the consumer and merchant with a list of eligible banks with which to open electronic accounts – also a collection of bits recorded on a magnetic stripe.
Digital signatures	The electronic equivalent of traditional hand-written signatures. *Digital signatures* are performed in a more complex manner through the use of encryption.
Directory	A listing of directories (i.e., files that contains other files or directories).

listing	
Domain name	A *domain name* locates an organisation or other entity on the Internet. For example, the *domain name* : www.totalbaseball.com locates an Internet address for "totalbaseball.com" at Internet point 199.0.0.2 and a particular host server named "www". The "com" part of the *domain name* reflects the purpose of the organisation or entity (in this example, "commercial") and is called the top-level *domain name*. The "totalbaseball" part of the *domain name* defines the organisation or entity and together with the top-level is called the second-level *domain name.* The second-level *domain name* maps to and can be thought of as the "readable" version of the Internet address. A third level can be defined to identify a particular host server at the Internet address. In our example, "www" is the name of the server that handles Internet requests. (A second server might be called "www2".) A third level of *domain name* is not required. For example, the fully-qualified *domain name* could have been "totalbaseball.com" and the server assumed. Subdomain levels can be used. For example, you could have "www.nyyankees.totalbaseball.com". Together, "www.totalbaseball.com" constitutes a fully-qualified *domain name*. Second-level *domain names* must be unique on the Internet and registered with one of the ICANN-accredited registrars for the COM, NET, and ORG top-level domains. Where appropriate, a top-level *domain name* can be geographic. (Currently, most non-U.S. domain names use a top-level *domain name* based on the country the server is in.) To register a U. S. geographic *domain name* or a *domain name* under a country code, see an appropriate registrar. On the Web, the *domain name* is that part of the Uniform Resource Locator (URL) that tells a *domain name* server using the domain name system (DNS) whether and where to forward a request for a Web page. The *domain name* is mapped to an IP address (which represents a physical point on the Internet). More than one *domain name* can be mapped to the same Internet address. This allows multiple individuals, businesses, and organisations to have separate Internet identities while sharing the same Internet server. It may be worth noting that the *domain name* system contains an even higher level of domain than the top-level domain. The highest level is the root domain, which would be represented by a single dot (just as in many hierarchical file systems, a root directory is represented by a "/") if it were ever used. If the dot for the root domain were shown in the URL, it would be to the right of the top-level *domain name*. However, the dot is assumed to be there, but never shown.
Electronic bulletin boards	Provides a central clearing-house for information and correspondence about an almost infinite number of subjects. A shared file where users can enter information for other users to read or download. Many *bulletin boards* are set up according to general topics and are accessible throughout a network.
Electronic	An EC system where a Customer at a PC keys in information regarding

checks	a payment to a third party and signs the check with a digital signature.
Electronic currency	Electronic mathematical representation of money.
Electronic Data Interchange (EDI)	The electronic transfer of information from one organisation's application to another organisation's application using a standardised electronic form.
Electronic Funds Transfer (EFT)	The transfer of funds electronically by using magnetic tape, diskette, or systems designed for such purposes.
E-mail	A store and forward mail service that allows you to communicate throughout the network
Encryption	*Encryption* is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorised people. It relies upon cryptographic techniques.
Escrowed	A written agreement (or property or money) delivered to a third party or put in trust by one party to a contract to be returned after fulfillment of some condition
Extranet	The secured extensions of internal business processes to known external business partners using Internet derived applications and technology.
Fiber-optic cable	Cable that uses discrete light signals that are transmitted through a core of thin glass or plastic fibers.
Fingerprinting	When tracking the amount of traffic on a Web site, it refers to a person who visits a Web site more than once within a specified period of time. Software that tracks and counts Web site traffic can distinguish between visitors who only visit the site once and unique visitors who return to the site. Different from a site's hits or page views -- which are measured by the number of files that are requested from a site -- unique visitors are measured according to their unique IP addresses, which are like online *fingerprints*, and unique visitors are counted only once no matter how many times they visit the site. There are some ISPs that use Dynamic Host Configuration Protocol, such as AOL and cable modem providers, which use different IPs for every file requested, making one visitor look like many. In this case, a single IP address does not indicate a unique visitor. A UNIX program that takes an e-mail address as input and returns information about the user who owns that e-mail address. On some systems, *finger* only reports whether the user is currently logged on. Other systems return additional information, such as the user's full name, address, and telephone number. Of course, the user must first enter this information into the system. Many e-mail programs now have a *finger* utility built into them.
FIPS 140-1	*FIPS* (Federal Information Processing Standards) are a set of standards that describe document processing, provide standard algorithms for

	searching, and provide other information processing standards for use within government agencies. *FIPS 140-1* defines the structure of cryptographic modules you must adhere to in computer and telecommunications systems. *FIPS 140-1* specifies security requirements that must be met by a cryptographic module used inside a security system that protects unclassified information that needs to be safeguarded during transmission and storage.
Firewall	A *firewall* is a set of related programs, located at a network server that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. Basically, a *firewall*, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A *firewall* also includes or works with a server that makes network requests on behalf of workstation users. A *firewall* is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.
Firmware	*Firmware* is programming that is inserted into programmable read-only memory (programmable ROM), thus becoming a permanent part of a computing device. *Firmware* is created and tested like software (using microcode simulation). When ready, it can be distributed like other software and, using a special user interface, installed in the programmable read-only memory by the user. *Firmware* is sometimes distributed for printers, modems, and other computer devices. IBM prefers the term microcode.
FTP	*File Transfer Protocol* (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, *FTP* is an application protocol that uses the Internet's TCP/IP protocols. *FTP* is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.
Hacker	*Hacker* is a term used by some to mean "a clever programmer" and by others, especially journalists or their editors, to mean "someone who tries to break into computer systems." Journalists or their editors almost universally use *hacker* to mean someone who attempts to break into computer systems. Typically, this kind of *hacker* would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system.
Hacking	The art of seeking network and specific system access, promote levels of privileges in a target environment, and then use the promoted privilege to further expand access. Usually this access goes without

	authorisation.
HTTP	The *Hypertext Transfer Protocol (HTTP)* is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), *HTTP* is an application Protocol. Essential concepts that are part of *HTTP* include (as its name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. Any Web server machine contains, in addition to the HTML and other files it can serve, an *HTTP* daemon, a program that is designed to wait for *HTTP* requests and handle them when they arrive. Your Web browser is an *HTTP* client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator) or clicking on a hypertext link, the browser builds an *HTTP* request and sends it to the Internet Protocol address indicated by the URL. The *HTTP* daemon in the destination server machine receives the request and, after any necessary processing, the requested file is returned.
HTML	*HTML (Hypertext Markup Language)* is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user. Each individual markup code is referred to as an element (but many people also refer to it as a tag). Some elements come in pairs that indicate when some display effect is to begin and when it is to end. *HTML* is a formal Recommendation by the World Wide Web Consortium (W3C) and is generally adhered to by the major browsers, Microsoft's Internet Explorer and Netscape's Navigator, which also provide some additional non-standard codes
Internet	A global "network of networks" operating on a co-operative basis and owned by no one entity or organisation. The series of interconnected networks that include local area, regional, and national backbone networks. Networks in the *Internet* use the same telecommunications protocol (TCP/IP) and provide electronic mail, remote login, and file transfer services.
Interpreters	A command *interpreter* is the part of a computer operating system that understands and executes commands that are entered interactively by a human being or from a program. In some operating systems, the command *interpreter* is called the shell.
Intranet	A network connecting an affiliated set of clients using standard Internet protocols.
IP address	In the most widely installed level of the Internet Protocol (IP) today, an *IP address* is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your *IP address* in the message (actually, in each of the packets if more than one is required) and sends it to the *IP address* that is obtained by looking up the domain-name in the URL you requested or

in the e-mail address you're sending a note to. At the other end, the recipient can see the *IP address* of the Web page requestor or the e-mail sender and can respond by sending another message using the *IP address* it received.

An *IP address* has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. On the Internet itself - that is, between the router that move packets from one point to another along the route - only the network part of the address is looked at.

The Network Part of the *IP Address*

The Internet Protocol (IP) is basically the set of rules for one network communicating with any other (or occasionally, for broadcast messages, all other networks). Each network must know its own address on the Internet and that of any other networks with which it communicates. To be part of the Internet, an organisation needs an Internet network number, which it can request from the Network Information Center (NIC). This unique network number is included in any packet sent out of the network onto the Internet.

The Local or Host Part of the *IP Address*

In addition to the network address or number, information is needed about which specific machine or host in a network is sending or receiving a message. So the *IP address* needs both the unique network number and a host number (which is unique within the network). (The host number is sometimes called a local or machine address.)

Part of the local address can identify a subnetwork or subnet address, which makes it easier for a network that is divided into several physical subnetworks (for example, several different local area networks) to handle many devices.

IP Address Classes and Their Formats

Since networks vary in size, there are four different address formats or classes to consider when applying to NIC for a network number:

Class A addresses are for large networks with many devices.

Class B addresses are for medium-sized networks.

Class C addresses are for small networks (fewer than 256 devices).

Class D addresses are multicast addresses.

The first few bits of each *IP address* indicate which of the address class formats it is using. The address structures look like this:

The *IP address* is usually expressed as four decimal numbers, each representing eight bits, separated by periods. This is sometimes known as the dot address and, more technically, as dotted quad notation. For Class A *IP addresses*, the numbers would represent "network.local.local.local"; for a Class C *IP address*, they would represent "network.network.network.local". The number version of the IP address can (and usually is) represented by a name or series of names called the domain name.

The Internet's explosive growth makes it likely that, without some new architecture, the number of possible network addresses using the scheme above would soon be used up (at least, for Class C network addresses). However, a new IP version, IPv6, expands the size of the *IP address* to 128 bits, which will accommodate a large growth in the number of network addresses. For hosts still using IPv4, the use of subnets in the host or local part of the IP address will help reduce new applications for network numbers. In addition, most sites on today's mostly IPv4 Internet have gotten around the Class C network address

	limitation by using the Classless Inter-Domain Routing (CIDR) scheme for address notation. Relationship of the *IP Address* to the Physical Address The machine or physical address used within an organisation's local area networks may be different than the Internet's *IP address.* The most typical example is the 48-bit Ethernet address. TCP/IP includes a facility called the Address Resolution Protocol (ARP) that lets the administrator create a table that maps IP addresses to physical addresses. The table is known as the ARP cache. Static versus Dynamic *IP Addresses* The discussion above assumes that *IP addresses* are assigned on a static basis. In fact, many IP addresses are assigned dynamically from a pool. Many corporate networks and online services economise on the number of IP addresses they use by sharing a pool of *IP addresses* among a large number of users. If you're an America Online user, for example, your *IP address* will vary from one logon session to the next because AOL is assigning it to you from a pool that is much smaller than AOL's base of subscribers.
ISO	*ISO* (International Organisation for Standardisation), founded in 1947, is a worldwide federation of national standards bodies from some 100 countries, one from each country. Among the standards it fosters is Open Systems Interconnection (OSI), a universal reference model for communication protocols. Many countries have national standards organisations such as the American National Standards Institute (ANSI) that participate in and contribute to *ISO* standards making. "ISO" is not an abbreviation. It is a word, derived from the Greek *isos*, meaning "equal", which is the root for the prefix "iso-" that occurs in a host of terms, such as "isometric" (of equal measure or dimensions) and "isonomy" (equality of laws, or of people before the law). The name *ISO* is used around the world to denote the organisation, thus avoiding the assortment of abbreviations that would result from the translation of "International Organisation for Standardisation" into the different national languages of members. Whatever the country, the short form of the Organisation's name is always *ISO.*
Java-Beans	Enterprise *JavaBeans (EJB)* is a Java Application Program Interface developed by Sun Microsystems that defines a component architecture for multi-tier client/server systems. *EJB* systems allow developers to focus on the actual business architecture of the model, rather than worry about endless amounts of programming and coding needed to connect all the working parts. This task is left to *EJB* server vendors. Developers just design (or purchase) the needed *EJB* components and arrange them on the server. Because *EJB* systems are written in Java, they are platform independent. Being object oriented, they can be implemented into existed systems with little or no recompiling and configuring.
Key Escrow	If you store data in an encrypted fashion and lose the digital encryption key, you probably have no way of ever reading that data again unless somebody else happens to be holding the key for you (*key escrow*).
Modem	A device for translating the digital data of computers into analogue signals. Two or more computers connected together over phone lines

	are therefore able to exchange files, and generally communicate with each other.
Network	A collection of two or more interconnected computers, for the purpose of sharing and transferring data via telecommunications.
Node	In a network, a *node* is a connection point, either a redistribution point or an end point for data transmissions. In general, a *node* has programmed or engineered capability to recognize and process or forward transmissions to other nodes
Operating System	An *operating system* (sometimes abbreviated as "OS") is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs are called applications.
OSI ISO	*OSI (Open Systems Interconnection)* is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although *OSI* is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the *OSI* model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion. *OSI* was officially adopted as an international standard by the International Organisation of Standards (ISO).
Out of bound	*Out of band* implies the use of methods independent of the primary communications means e.g. *out of band* signaling is telecommunication signaling (exchange of information in order to control a telephone call) that is done on a channel that is dedicated for the purpose and separate from the channels used for the telephone call.
Packet Sniffer	A tool that can capture conversations between two or more systems or devices. It captures network traffic and decodes (interprets) it.
Patches	A *patch* (sometimes called a "fix") is a quick-repair job for a piece of programming. During a software product's beta test distribution or try-out period and later after the product is formally released, problems (called bug) will almost invariably be found. A *patch* is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's Web site. The *patch* is not necessarily the best solution for the problem and the product developers often find a better solution to provide when they package the product for its next release. A *patch* is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and keep track of the installation of *patches*.
Portal/ Gateway	*Portal* is a new term for a World Wide Web site that is or proposes to be a major starting site for users when they get connected to the Web or

	that users tend to visit as an anchor site. There are general portals and specialized or niche portals. Some major general portals include Yahoo, Excite, Netscape, Lycos, CNET, Microsoft Network, and America Online's AOL.com. Examples of niche portals include Garden.com (for gardeners), Fool.com (for investors), and SearchNT.com (for Windows NT administrators). Typical services offered by portal sites include a directory of Web sites, a facility to search for other sites, news, weather information, e-mail, stock quotes, phone and map information, and sometimes a community forum.
Protocol	A *Protocol* is a set of rules that defines how computers transmit information to each other, which allows different types of computer and software programs to communicate. Protocols exist at several levels in a telecommunication connection. There are hardware telephone protocols. There are protocols between each of several functional layers and the corresponding layers at the other end of a communication. Both end points must recognize and observe a protocol. Protocols are often described in an industry or international standard.
Registration Authority (RA)	A *registration authority* (RA) is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. *RA*s are part of a public key infrastructure (PKI), a networked system that enables companies and users to exchange information and money safely and securely. The digital certificate contains a public key that is used to encrypt and decrypt messages and digital signatures.
Random number generator (RNG)	A pseudo-*random number generator* (PRNG) is a program written for, and used in, probability and statistics applications when large quantities of random digits are needed. Most of these programs produce endless strings of single-digit numbers, usually in base 10, known as the decimal system. When large samples of pseudo-random numbers are taken, each of the 10 digits in the set {0,1,2,3,4,5,6,7,8,9} occurs with equal frequency, even though they are not evenly distributed in the sequence. Many algorithms have been developed in an attempt to produce truly random sequences of numbers, endless strings of digits in which it is theoretically impossible to predict the next digit in the sequence based on the digits up to a given point. But the very existence of the algorithm, no matter how sophisticated, means that the next digit can be predicted. This has given rise to the term pseudo-random for such machine-generated strings of digits. They are equivalent to random-number sequences for most applications, but they are not truly random according to the rigorous definition. The digits in the decimal expansions of irrational numbers such as pi (the ratio of a circle's circumference to its diameter in a Euclidean plane), *e* (the natural-logarithm base), or the square roots of numbers that are not perfect squares (such as $2^{1/2}$ or $10^{1/2}$) are believed by some mathematicians to be truly random. But computers can be programmed to expand such numbers to thousands, millions, billions, or trillions of decimal places; sequences can be selected that begin with digits far to the right of the decimal (radix) point, or that use every second, third, fourth, or *n*th digit. However, again, the existence of an algorithm to determine the digits in such numbers is used by some theoreticians to argue that even these single-digit number sequences are pseudo-random, and not truly random. The question then becomes, Is the

	algorithm accurate (that is, random) to infinity, or not? - and because no one can answer such a question definitively because it is impossible to travel to infinity and find out, the matter becomes philosophical.
Routers	On the Internet, a *router* is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The *router* is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A *router* is located at any gateway (where one network meets another), including each Internet point-of-presence. A *router* is often included as part of a network switch.
Router tables	A router table is used by routers to determine the address of the next device in the communication path.
Server	1) In general, a *server* is a computer program that provides services to other computer programs in the same or other computers. 2) The computer that a *server* program runs in is also frequently referred to as a server (though it may contain a number of server and client programs). 3) In the client/*server* programming model, a *server* is a program that awaits and fulfills requests from client programs in the same or other computers. A given application in a computer may function as a client with requests for services from other programs and also as a *server* of requests from other programs.
Smart Card	A *smart card* is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use. A *smart card* contains more information than a magnetic stripe card and it can be programmed for different applications. Some cards can contain programming and data to support multiple applications and some can be updated to add new applications after they are issued. *Smart cards* can be designed to be inserted into a slot and read by a special reader or to be read at a distance, such as at a toll booth. Cards can be disposable (as at a trade-show) or reloadable (for most applications).
SMTP traffic	*SMTP (Simple Mail Transfer Protocol)* is a TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or Internet Message Access Protocol that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses *SMTP* for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server. Most mail programs such as Eudora let you specify both an *SMTP* server and a POP server. On UNIX-based systems, sendmail is the most widely-used *SMTP* server for e-mail. A commercial package, Sendmail, includes a POP3 server and also comes in a version for Windows NT.
Sniffer	A *sniffer* is a program that monitors and analyzes network traffic, detecting bottlenecks and problems. Using this information, a network manager can keep traffic flowing efficiently.

	A *sniffer* can also be used legitimately or illegitimately to capture data being transmitted on a network. A network router reads every packet of data passed to it, determining whether it is intended for a destination within the router's own network or whether it should be passed further along the Internet. A router with a *sniffer*, however, may be able to read the data in the packet as well as the source and destination addresses. *Sniffers* are often used on academic networks to prevent traffic bottlenecks caused by file-sharing applications such as Napster or Gnutella.
Spoofing	On the Internet, "to *spoof*" can mean: 1) To deceive for the purpose of gaining access to someone else's resources (for example, to fake an Internet address so that one looks like a certain kind of Internet user) 2) To simulate a communications protocol by a program that is interjected into a normal sequence of processes for the purpose of adding some useful function 3) To playfully satirise a Web site.
Subnets	A *subnet* (short for "subnetwork") is an identifiably separate part of an organisation's network. Typically, a *subnet* may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organisation's network divided into *subnets* allows it to be connected to the Internet with a single shared network address. Without *subnets*, an organisation could get multiple connections to the Internet, one for each of its physically separate subnetworks, but this would require an unnecessary use of the limited number of network numbers the Internet has to assign. It would also require that Internet routing tables on gateways outside the organisation would need to know about and have to manage routing that could and should be handled within an organisation.
Switches	In telecommunications, a *switch* is a network device that selects a path or circuit for sending a unit of data to its next destination. A *switch* may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to. In general, a *switch* is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.
Tamper evident envelopes	Tamper evident security envelopes are an excellent way to ensure that valuable documents or objects remain safe when mailed The security envelopes are sealed with tamper evident tape that shows a "VOID/OPENED" message when peeled away, clearly showing the recipient that the contents have more than likely been tampered with if the message is showing. These tamper evident security envelopes are preprinted with consecutive numbers, address, and return address lines, and a numbered receipt, so using these security envelopes to protect your mailings is a simple process. When sending valuable documents or personal belongings via mail or courier, a durable security envelope that incorporates a theft deterrent like a tamper evident tape, is the best choice. If the tamper evident

	security envelope arrives with the words "VOIDS/OPENED" showing on the face of the tape, the recipient need only refuse the shipment. In this way, you can be sure that the recipient will not be receiving an empty envelope or an envelope filled with worthless materials.
Two factor authentication	*Two-factor authentication* is a security process that confirms user identities using two distinctive factors – something you know, such as a Personal Identification Number (PIN), and something you have, such as a smart card or token.
TCP/IP	*TCP/IP (Transmission Control Protocol/Internet Protocol)* is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the *TCP/IP* program just as every other computer that you may send messages to or get information from also has a copy of *TCP/IP*. *TCP/IP* is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.
Telnet	A terminal emulation program for TCP/IP networks such as the Internet. The *Telnet* program runs on your computer and connects your PC to a server on the network. You can then enter commands through the *Telnet* program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a *Telnet* session, you must log in to a server by entering a valid username and password. *Telnet* is a common way to remotely control Web servers.
Time stamping	A record mathematically linking a document to a time and date.
URL	*Universal Resource Locator* - (URL) An address that identifies the location of any type of Internet resource.
VAN (value added network)	A private network provider (sometimes called a turnkey communications line) that is hired by a company to facilitate electronic data interchange (EDI) or provides other network services. Before the arrival of the World Wide Web, some companies hired *value-added networks* to move data from their company to other companies. With the arrival of the World Wide Web, many companies found it more cost-efficient to move their data over the Internet instead of paying the minimum monthly fees and per-character charges found in typical *VAN* contracts.
Virtual private network (VPN)	A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A *virtual private network* can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the *VPN* is to give the company the same

	capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A *virtual private network* makes it possible to have the same secure sharing of public resources for data. Using a *virtual private network* involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses.
Web browser	A program, which sends requests for information across the Internet and displays the information when it is received and uses a graphical approach to finding and displaying the information on the Internet.
Web server	A *Web server* is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests). Every computer on the Internet that contains a Web site must have a *Web server* program. Two leading *Web servers* are Apache, the most widely-installed Web server, and Microsoft's Internet Information Server (IIS). Other *Web servers* include Novell's *Web Server* for users of its NetWare operating system and IBM's family of Lotus Domino servers, primarily for IBM's OS/390 and AS/400 customers. *Web servers* often come as part of a larger package of Internet- and intranet-related programs for serving e-mail, downloading requests for File Transfer Protocol (FTP) files, and building and publishing Web pages. Considerations in choosing a *Web server* include how well it works with the operating system and other servers, its ability to handle server-side programming, security characteristics, and publishing, search engine, and site building tools that may come with it.
Web-wrap	A Web Wrap agreement sets forth contractual terms in an on-line environment and is a form of Standard Form Agreement since one party drafts the terms of the agreement without consultation or negotiation of such terms with the other party or parties. A web wrap agreement usually appears as a dialogue box on a customer's screen when the customer attempts to download software or order goods or services on-line. The dialogue box contains the terms and conditions of the license or sale which the customer is instructed to review before assenting thereto by clicking a button at the bottom of the dialogue box.
World wide Web (WWW)	A graphical environment that provides easy access to information stored on systems connected to the Internet. The *WWW* allows users to retrieve software and text on to their own computers for future use.
X.509	The most widely used standard for defining digital certificates. *X.509* is actually an International Telecommunications Union (ITU) Recommendation, which means that has not yet been officially defined or approved. As a result, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use *X.509* certificates to implement SSL in their Web servers and browsers. But an *X.509* Certificate generated by Netscape may not be readable by Microsoft products, and vice versa.