TECHNICAL REPORT

ISO/TR 13569

Third edition
2005-11-15

Financial services — Information security guidelines

Services financiers — Lignes directrices pour la sécurité de l'information

Reference number
ISO/TR 13569:2005(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 13569 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This third edition cancels and replaces the second edition (ISO/TR 13569:1997), which has been technically revised. It also incorporates ISO/TR 13569:1997/Amd 1:1998.

Introduction

Financial business practices have changed with the introduction of computer and network-based technologies. Increased reliance on electronic transactions has heightened the need to manage the security of information and communications technology. Huge amounts in funds and securities are transferred daily by electronic communication mechanisms controlled by security practices based on business policies.

The high value and sheer volume of such transactions within an increasingly connected, open environment exposes the financial industry to potentially severe consequences. Interconnected networks and the increased number and sophistication of malicious adversaries compound this risk with the potential to impact banks and their customers. And when financial transactions involve systemically important payment systems, these consequences may adversely affect national and global financial markets.

The necessity to expand business operations into these environments and to manage risk, demands a strong and effective enterprise information security programme. Financial institutions must manage these programmes in a comprehensive manner, just as they manage risk through well-established business practice and agreements, careful outsourcing of functions, insurance and the use of appropriate security controls. Also they must architect their security programmes to address the changing risks and requirements imposed by an expanding national and international legal and regulatory environment.

As the Basle accords warn us, operational, legal and regulatory risks can cause or exacerbate credit and liquidity risks. The management of these risks has become central to the information security programme of a financial institution. Each institution must interpret these risks in terms of its own business activities in order to understand its exposure. Careful consideration must be given to operational risks, including fraud and criminal activities, natural disasters and acts of terrorism. Low probability events, such as the tsunami that struck Asia in December 2004 and the September the eleventh, 2001 terrorist attacks on the financial services in New York City, do happen and must be planned for.

This Technical Report is intended for use by financial institutions of all sizes and types that need to employ a prudent and commercially reasonable information security management programme. It also gives useful guidance to providers of services to financial institutions, and may serve as a source document for educators and publishers serving the financial industry.

The objectives of this Technical Report are:

- to define the information security management programme;
- to present programme policy, organization and necessary structural components;
- to present guidance on the selection of security controls that represent accepted prudent business practice in financial applications;
- to inform financial services management of the need to systematically address legal and regulatory risks in their security information management programme.

This Technical Report is not intended to provide a single generic solution for all financial service institutions. A risk analysis must be performed by each organization and appropriate actions selected. This Technical Report provides guidance for conducting that process, not specific solutions.

Financial services — Information security guidelines

1 Scope

This Technical Report provides guidelines on the development of an information security programme for institutions in the financial services industry. It includes discussion of the policies, organization and the structural, legal and regulatory components of such a programme. Considerations for the selection and implementation of security controls, and the elements required to manage information security risk within a modern financial services institution are discussed. Recommendations are given that are based on consideration of the institutions' business environment, practices and procedures. Included in this guidance is a discussion of legal and regulatory compliance issues, which should be considered in the design and implementation of the programme.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9564 (all parts), *Banking — Personal Identification Number (PIN) management and security*

ISO 10202 (all parts), *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards*

ISO 11568 (all parts), *Banking — Key management (retail)*

ISO/IEC 11770 (All parts), *Information technology — Security techniques — Key management*

ISO 15782 (all parts), *Certificate management for financial services*

ISO 16609:2004, *Banking — Requirements for message authentication using symmetric techniques*

ISO/IEC 17799, *Information technology — Security techniques — Code of practice for Information security management*

ISO/IEC 18028 (All parts), *Information technology — Security techniques — IT network security*

ISO/IEC 18033 (All parts), *Information technology — Security techniques — Encryption algorithms*

ISO 21188, *Public key infrastructure for financial services — Practices and policy framework*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access control
functions that limit access to information or information processing facilities, to those persons or applications authorized such access, including physical access controls, which are based on placing physical barriers between unauthorized persons and the information resources being protected, and logical access controls, which employ other means

3.2
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2; ISO/IEC 13335-1:2004, definition 2.1]

3.3
alarm
indication of a security violation, or unusual or dangerous condition, which may require immediate attention

3.4
asset
anything that has value to the organization

[ISO/IEC 13335-1:2004, definition 2.2]

3.5
audit
function that seeks to validate that controls are in place, adequate for their purposes, and that reports inadequacies to appropriate levels of management

3.6
audit journal
chronological record of system activities which is sufficient to enable the reconstruction, review and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results

[ISO 15782-1:2003, definition 3.3]

3.7
authentication
provision of assurance of the claimed identity of an entity

[ISO/IEC 10181-2; ISO/IEC TR 13335-4:2000, definition 3.1]

3.8
authenticity
property, as applied to entities such as users, processes, systems and information, that ensures that the identity of a subject or resource is the one claimed

3.9
availability
property of being accessible and usable upon demand by an authorized entity

[ISO 7498-2; ISO/IEC 13335-1:2004, definition 2.4]

3.10
back-up
saving of business information to assure business continuity in case of loss of information resources

3.11
biometric
measurable biological or behavioural characteristic that reliably distinguishes one person from another, used to recognize the identity, or verify the claimed identity, of an individual

[ANSI X9.84:2003]

3.12
biometrics
automated methods used to recognize the identity, or verify the claimed identity, of an individual, based on physiological or behavioural characteristics

3.13
card authentication method
CAM
concept that allows unique machine-readable identification of a financial transaction card, and that prevents copying of cards

3.14
classification
scheme that separates information into categories, such as fraud potential, sensitivity or information criticality, so that appropriate controls may be applied

3.15
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO 7498-2; ISO/IEC 13335-1:2004, definition 2.6; ISO 15782-1:2003, definition 3.19]

3.16
contingency plan
procedure that, when followed, allows an organization to resume operations after natural or other disasters

3.17
control
see safeguard

3.18
corporate information security policy
Policy
general statement of the intentions and goals of establishing an information security programme

3.19
credit risk
risk that a party within the system will be unable to fully meet its financial obligations within the system either when due or at any time in the future

[CPSS, Core Principles for Systemically Important Payment Systems]

3.20
criticality
requirements that certain information or information processing facilities be available to conduct business

3.21
cryptography
mathematical process used for encryption or authentication of information

3.22
cryptographic authentication
authentication based on a digital signature, message authentication code as generated under ISO 16609 with a cryptographic key distributed under ISO 11568, or inferred through successful decryption of a message encrypted under ISO 18033 (coupled with ISO/TR 19038 or ANSI X9.52) with a key distributed under ISO/IEC 11770

3.23
cryptographic key
value that is used to control a cryptographic process, such as encryption or authentication

NOTE Knowledge of an appropriate key allows correct decryption or validation of the integrity of a message.

3.24
destruction of information
any condition which renders information unusable regardless of cause

3.25
digital signature
cryptographic transformation that, when associated with a data unit, provides the services of origin authentication, data integrity and signer non-repudiation

[ANSI X9.79]

3.26
disclosure of information
unauthorized viewing or potential viewing of information

3.27
dual control
process of utilizing two or more separate entities (usually persons), who are operating in concert, to protect sensitive functions or information

NOTE 1 Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is able to access or to utilize the materials (e.g. cryptographic key).

NOTE 2 For manual key and certificate generation, conveyance, loading, storage and retrieval, dual control requires split knowledge of key among the entities.

NOTE 3 Whenever dual control is required, care should be taken to assure that individuals are independent of each other. See also split knowledge.

[ISO 15782-1:2003, definition 3.31]

3.28
encryption
process of converting information to render it as a form unintelligible to all except holders of a specific cryptographic key

NOTE Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

3.29
firewall
collection of components placed between two networks that collectively have the properties that

- all network traffic from inside to outside, and vice-versa, must pass through the firewall;
- only authorized network traffic, as defined by local security policy, is allowed to pass;
- that it is itself immune to penetration

3.30
identification
process of uniquely determining the unique identity of an entity

[ISO/IEC TR 13335-4:2000, definition 3.2]

3.31
image
digital representation of a document for manipulation or storage within an information processing system

3.32
incident
any unexpected or unwanted event that might cause a compromise of business activities or information security, such as

- loss of service, equipment or facilities;
- system malfunctions or overloads;
- human errors;
- non-compliances with policies or guidelines;
- breaches of physical security arrangements;
- uncontrolled system changes;
- malfunctions of software or hardware;
- access violations

[ISO/IEC 13335-1:2004, definition 2.10]

3.33
information processing facility
any information processing system, service or infrastructure, or the physical locations housing them

[ISO/IEC 13335-1:2004, definition 2.13]

3.34
information
any data, whether in an electronic form, written on paper, spoken at a meeting, or on any other medium which is used by a financial organization to make decisions, move funds, set rates, make loans, process transactions and the like, including software components of the processing system

3.35
information asset
information or information processing resources of an organization

3.36
information security
all aspects related to defining, achieving and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information or information processing facilities

[ISO/IEC 13335-1:2004, definition 2.14]

3.37
information security officer
ISO
person responsible for implementing and maintaining the information security programme

3.38
information resource
equipment used to manipulate, communicate or store information, such as telephones, facsimiles, and computers, whether these are inside or outside the organization

3.39
integrity
the property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004, definition 2.15]

3.40
key
see cryptographic key

3.41
kiting
using a bad cheque to get credit or money

3.42
legal risk
risk of loss because of the unexpected application of a law or regulation or because a contract cannot be enforced

[CPSS, Core Principles for Systemically Important Payment Systems]

3.43
letter of assurance
document setting forth the information security controls which are in place for the protection of information held on behalf of the recipient of the letter

3.44
liquidity risk
risk that a party within the system will have insufficient funds to meet financial obligations within the system as and when expected, although it may be able to do so at some time in the future

[CPSS, Core Principles for Systemically Important Payment Systems]

3.45
message authentication code
MAC
code appended to a message by the originator, which is the result of processing the message through a cryptographic process

NOTE If the receiver can generate the same code, confidence is gained that the message was not modified and that it originated with the holder of the appropriate cryptographic key.

3.46
modification of information
unauthorized or accidental change in information, whether detected or undetected

3.47
need to know
security concept that limits access to information and information processing resources to that which is required to perform one's duties

3.48
network
collection of communication and information processing systems that may be shared among several users

3.49
non-repudiation
ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

[ISO/IEC 13888-1; ISO 7498-2; ISO/IEC 13335-1:2004, definition 2.16]

3.50
operational risk
risk that operational factors such as technical malfunctions or operational mistakes will cause or exacerbate credit or liquidity risks

[CPSS, Core Principles for Systemically Important Payment Systems]

3.51
owner of information
person or function responsible for the collection and maintenance of a given set of information

3.52
password
string of characters which serves as an authenticator of the user

3.53
prudent business practice
set of practices which have been generally accepted as necessary

3.54
reliability
property of consistent intended behaviour and results

[ISO/IEC 13335-1:2004, definition 2.17]

3.55
residual risk
risk that remains after risk treatment

[ISO/IEC 13335-1:2004, definition 2.18]

3.56
risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

NOTE It is measured in terms of a combination of the probability of an event and its consequence.

[ISO/IEC 13335-1:2004, definition 3.19]

3.57
risk acceptance
approved risk associated with an exception to the Policy

3.58
risk analysis
systematic process of estimating the magnitude of risks

[ISO/IEC 13335-1:2004, definition 2.20]

3.59
risk assessment
process of combining risk identification, risk analysis and risk evaluation

[ISO/IEC 13335-1:2004, definition 2.21]

3.60
risk evaluation
process of comparing analysed levels of risk against pre-established criteria and identifying areas needing risk treatment

3.61
risk identification
process of identifying risks considering business objectives, threats and vulnerabilities as the basis for further analysis

3.62
risk management
total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect information and communications technology system resources

[ISO/IEC 13335-1:2004, definition 3.22]

3.63
risk treatment
process of selection and implementation of measures to modify risks

3.64
safeguard
practice, procedure or mechanism that treats risk

NOTE The term “safeguard" may be considered synonymous with the term “control".

[ISO/IEC 13335-1:2004, definition 2.24]

3.65
security
quality or state of being protected from unauthorized access or uncontrolled losses or effects

NOTE 1 Absolute security is impossible to achieve in practice, and the quality of a given security system is relative.

NOTE 2 Within a state-model security system, security is a specific “state" to be preserved under various operations.

3.66
server
computer that acts as a provider of some service to other computers, such as processing communications, file storage interface or printing facility

3.67
sign-on
completion of identification and authentication of a user

3.68
split knowledge
division of critical information into multiple parts in such a way as to require a minimum number of parts to be present before an action can take place

NOTE Split knowledge is often used to enforce dual control.

3.69
stored value card
token that is capable of storing and transferring electronic money

3.70
systemic risk
risk that the inability of one of the participants to meet its obligations, or a disruption of the system itself, could result in the inability of other system participants or of other financial institutions in other parts of the financial system to meet their obligations as they become due

NOTE Such a failure could cause widespread liquidity or credit problems and, as a result, could threaten the stability of the system or of financial markets.

[CPSS, Core Principles for Systemically Important Payment Systems]

3.71
threat
potential cause of an incident that may result in harm to a system or organization

[ISO/IEC 13335-1:2004, definition 2.25]

3.72
token
user-controlled device (e.g., disk, smart card, computer file) that contains information that can be used in electronic commerce for authentication or for access control

3.73
user ID
character string that is used to uniquely identify each user of a system

3.74
vulnerability
weakness of an asset or group of assets that can be exploited by one or more threats

[ISO/IEC 13335-1:200, definition 2.26]

4 Symbols and abbreviated terms

ATM	Automated Teller Machine
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Corporate Information Security Officer
COO	Chief Operating Officer
CPSS	Committee on Payment and Settlement Systems
CTO	Chief Technology Officer
DMZ	De-Militarized Zone
EFT	Electronic Funds Transfer
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IPSEC	IP Security Protocol
IT	Information Technology
LAN	Local Area Network
LEAP	Lightweight Extensible Agent Platform
MAC	Message Authentication Code
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
POTS	Plain Old Telephone System
RF	Radio Frequency
SMTP	Simple Mail Transport Protocol

SSH	Secure Shell
SSL	Secure Socket Layer
USB	Universal Serial Bus
VPN	Virtual Private Network
VTAM	Virtual Terminal Access Method
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WS	Web Services
XML	Extensible Markup Language

5 Corporate information security policy

5.1 Purpose

All financial services institutions today rely heavily on the use of Information Technology (IT) and Information and Communication Technology (ICT), and therefore, need to protect information and to manage the security of their information assets. In order for management to fulfil their responsibilities, information security must be provided, and the management of information security must become an important component of the organization's management plan.

Development of an information security programme is a prudent business practice that will help a financial services organization to identify and manage risk. This Technical Report recommends a general, policy-based approach to information security management, and provides guidance that can be tailored to meet the business objectives of the organization. Business objectives must be supported by policies and procedures for protecting IT assets. A policy-based approach is applicable to different size institutions, different management styles, and organizational environments.

This Technical Report is intended to provide guidance, not specific solutions, on the management aspects of information security, and to assist financial services management in developing and maintaining an information security programme. Other references, especially ISO/IEC 17799, provide important general purpose detailed information that will be invaluable for implementation and maintenance. However, this Technical Report addresses the specific legal and regulatory requirements that must be considered by financial institutions when establishing a policy-based information management programme.

5.2 Legal and regulatory compliance

5.2.1 General

Regulatory authorities concern themselves principally with issues of safety, soundness and compliance with laws and regulations. One element of safety and soundness is the organization's system of safeguards that protects information from unavailability, and unauthorized modification, disclosure and destruction. Recent national and international legislation, such as Basel II, the Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley (GLB)[22] and European Directive 95/46/EC, has created an environment of legal and regulatory risk for global providers of financial services. The organization's security policy must address this risk.

Compliance officers should work with the CISO, CFO, business managers, risk managers and auditors to ensure that information security requirements derived from national and international laws and regulations are understood and addressed. Compliance officers should also remain current on new technologies or methodologies that may become subject of regulation; e.g. compliance with predefined functionality classes for Information Technology products.

5.2.2 Requirements for financial institutions

5.2.2.1 Overview

For Institutions in the financial sector there are some legal and regulatory requirements, which have an impact on IT security and have to be followed. The inherent problem is that these requirements differ from country to country. Although the European Union has led the way towards a legal alignment, there are still national regulations which demand specific attention.

In the following, each subclause will describe the most important laws from a perspective of a financial services provider operating in a global environment. A description of the legislative environment will be divided into three sectors: corporate governance, data protection (privacy) and financial sector legislation specific to financial services providers (e.g., money laundering legislation). The description of the regulatory environment will concentrate on financial reporting requirements and the Basel II recommendations, which are freely available from the Bank for International Settlement[19] in Basle, Switzerland at: http://www.bis.org/bcbs/publ.htm.

5.2.2.2 Legal requirements

5.2.2.2.1 Corporate governance

In recent years, many national and regional legislative bodies have brought forth laws that address corporate governance. Notable among these are the Sarbanes-Oxley (SOX) Act in the United States (U.S.), the Kontrolle- und Transparenz Gesetz (KonTraG) in Germany, and the European Union Draft Directive on Corporate Governance. All three have altered the landscape of legal risks faced by providers of financial services.

The Sarbanes-Oxley Act requires all companies publicly traded on U.S. stock exchanges to provide evidence that they have adequate controls in place for financial reporting. In detail, SOX obliges the CEO and CFO of any such company to assess the effectiveness of their internal control framework and explicitly sign and accept responsibility for the annual financial reports of the organization. With regards to IT, this requires that the operation of critical business applications and their associated risks must be assessed and controlled. In summary, the entire life cycle of these applications must be assessed and controlled, ranging from initial development to business continuity to ensure that adequate measures are in place. Though national in origin, this legislation is applicable to any company whose stocks are publicly traded within the U.S.

The German Kontrolle- und Transparenz Gesetz (KonTraG) legislation requires corporations to implement an internal monitoring process identifying internal developments and decisions that may pose a high risk to this corporation. Implicitly, this means that management has to implement a corporate-wide internal risk management system. It also obliges management to report any identified major risk in their reporting system (bi-annual and annual). With regards to IT, this covers a similar aspect as the Sarbanes-Oxley Act. However, since German publicly traded companies have a two-tier management board, this enforces stronger reporting from the management board to the supervisory board. Non-compliance act may lead to a reduction in the banking rating of the corporation and may therefore influence interest rates for credits.

The European Union (EU) is drafting a directive which will influence EU national legislation: all publicly listed companies are required to publish a corporate governance report. This report will provide details on the Board of Directors, its decisions, its financial situation and its compliance with national law. This report will also include the results of independent audits. This directive has similar implications to the Sarbanes-Oxley Act and Kontrolle- und Transparenz Gesetz (KonTraG) legislation for IT. There are other national laws in place covering this topic but none is so stringent that it would have the influence of an EU Directive.

5.2.2.2.2 Data protection (privacy)

Data protection is gaining more and more attention caused by various laws on the regional, national and state level. This legislation is triggered by the fact that the Internet and its use pose additional risks on misuse in that area and those individuals using this medium need appropriate protection.

The Gramm-Leach-Bliley (GLB) Act is intended to protect consumer information held by financial institutions. It requires these institutions to provide their customers with privacy notices explaining the institutions' information sharing practice. In turn, consumers have the right to limit some – but not all – sharing of their information. The law requires also that financial institutions protect information collected about individuals; it does not apply to information collected in business or commercial activities. The Federal Trade Commission (FTC) has published a set of standards which should be applied to achieve compliance with GLB.

The European Directive 95/46/EC is a joint effort to achieve privacy for all member states at a high level. It protects information of individuals during the whole processing life cycle. Simply spoken, it requires an institution to ask for permission if information is used other than for the officially intended (and stated) use. It also limits the transfer of personal data to those countries where adequate data protection is provided. In general, individuals have to grant permission explicitly (opt-in) to allow further processing. This is contrary to the procedure in the U.S. where individuals are asked to opt out, to prohibit further processing. This directive is implemented into national law within all member states.

The Swiss data protection law is similar to the laws existent in other European countries. It is mentioned here for two reasons: Switzerland is not part of the European Union and therefore it should be mentioned. On the other hand, the Swiss law prohibits the transfer of personal data into other states, if there is no adequate protection and requires the transmitting entity to inform the legal authority on the transfer. Another important law relating to financial institutions is the Swiss Bank Customer Secret (Schweizer Bankkundengeheimnis), which explicitly protects the customer information maintained by banks.

5.2.2.2.3 Money laundering

Almost all countries have some kind of money laundering legislation which usually means that money transfers exceeding a certain amount have to be examined to verify its sources and destination. As recently as the 1990s such legislation would have had no explicit security relevance for it could be implemented independently of any security issues.

The terrorist attacks of September 11th, 2001 in the United States vividly illuminated the importance of anti-money laundering laws and controls. The attacks fostered an even greater recognition of the importance of anti-money laundering cooperation around the world. This recognition galvanized international cooperation and led to significant modifications to anti-money laundering laws that have paid dividends in the world community's ability to trace the funds of those who finance international terrorism.

Since 2001, the United States has continued its vigorous inter-agency international anti-money laundering training programme to improve worldwide efforts to combat money laundering and financial crime. Other governments and international organizations have also strengthened anti-money laundering programmes. The European Union broadened its anti-money laundering directive and imposed anti-money laundering obligations on “gatekeepers", professionals such as lawyers and accountants who help place dirty money in the financial system. Regional anti-money laundering bodies in Europe, Asia and the Caribbean continued working effectively, and nascent anti-money laundering regional organizations in South America and Africa became operational.

A major money laundering focus of the year was the work of the Financial Action Task Force (FATF), the world's pre-eminent multilateral anti-money laundering body, which continued its non-cooperative countries and territories exercise. FATF moved quickly after 11/9/01 to convene an extraordinary plenary on the financing of terrorism, which decided to expand its mission beyond money laundering, and to focus its energy and expertise on the worldwide effort to combat terrorist financing. The FATF has since adopted eight special recommendations regarding terrorist financing.

The terrorist attacks gave strong impetus to many countries to amend and strengthen their money laundering laws. In the United States, the Uniting and Strengthening America by Providing Appropriate Tools Required to

Intercept and Obstruct Terrorism (“USA PATRIOT") Act of 2001 made major changes to the U.S. anti-money laundering regime. The broad new authorities provided in the USA PATRIOT Act will have significant influence on the relationships between U.S. financial institutions and their individual and institutional customers

An information security management programme can help financial institutions to thwart money laundering schemes. More importantly, these programmes can be used to demonstrate to law enforcement organizations that the institution is compliant with relevant legislation and provide documentation that it is systematically and actively taking measures to comply.

5.2.2.2.4 Financial market legislation

Most of the laws regulating the financial sector primarily define the responsibilities of a financial institution. This includes the obligation to provide qualified services. Some national authorities interpret this in such a way that it covers integrity of IT services used. The following national laws will point out specific IT security issues.

Under the Argentina central banking legislation, a financial institution has to incorporate an Information Security Officer (ISO) who provides an annual report to the Central Bank of Argentina. This report must reflect how the internal controls of the institution are established and maintained to ensure proper services.

European Union Directive 82/121/EEC regulates the reporting of financial institutions. It was recently updated to achieve more regular reporting throughout the European Union. European Union Directive 2000/31/EC (Electronic Commerce) requests a legal framework for electronic commerce, which must include customer privacy issues, spam handling, taxation, electronic contracts and their treatment, confidentiality of communications among others. It also defines a Code of Conduct as a medium to communicate the rights of involved entities.

The German Kreditwesengesetz (KWG) law regulates almost everything specific to financial institutions in Germany. It defines the way banks have to operate, who is allowed to lead a financial institution, what is to be reported, etc. Of special interest are three paragraphs. The first one deals with automated access to customer data by the financial authorities (§ 24c) which requires additional security measures in place. The second one (§ 25a) defines the specific obligations a financial institution has to fulfil which covers issues like internal risk management, security measures and internal audit and its cooperation with the overseeing authorities. Finally, there are regulations for if a financial institution or its management do not fulfil their obligations possibly leading to that management loosing its right to conduct business in the financial sector.

5.2.2.3 Regulatory requirements

There are two financial institution regulatory requirement topics of high relevance. The first concerns the obligations of the institution for financial reporting (usually overseen by national financial authorities). The second is the financial soundness obligation which is described in the Bank for International Settlement (BIS - see http://www.bis.org/bcbs/index.htm) Basel II accords. These requirements include the need for the institution to consider operational risks.

The Basel Committee on Banking Supervision formulates broad supervisory standards, guidelines and best practice recommendations. The committee expects individual national financial authorities to take steps to implement these recommendations through detailed arrangements – statutory or otherwise – in a manner that best suits their own national systems. Regulatory requirements lead to the need to audit institutions. In order to limit the disruptions that audits cause to normal business operations, institutions should put systems in place (internal audit, information security management, etc.) that can easily provide regulators with what they need to examine to be assured that the institution is compliant.

Each financial institution must interpret “operational risk" in terms of its own business activities and identify the risks that it is exposed to. An analysis of operational risks should include fraud and criminal activities, systems failures, human errors, natural disasters and acts of terrorism. The tsunami that caused widespread death and destruction throughout Asia in December 2004 and the September eleventh terrorist attacks in 2001 that targeted the financial services industry in New York City are both examples of extremely low probability events. But such events do happen and must be planned for.

Basel II enforces the need for an institution to perform a systematic risk analysis. Both qualitative and quantitative techniques for managing contingencies should be utilized, and the selection of controls for an individual business unit should be based on a cost benefit analysis that considers the likelihood of a contingency, its probable frequency, and the projected loss and impact on business operations should an event occur.

Note that there is a distinction between banking supervision to ensure a bank's financial health and bank oversight, which considers the institutions systems in terms of operational risk. This oversight is based not on Basel II but on the BIS Core Principles (see http://www.bis.org/publ/bcbs49b.pdf), which are aimed at systemically important payment systems. Those payment systems which are classified as having “systemic importance" to the health and normal operations of financial markets must meet all ten of the Core Principles. “Prominent systems" have only to meet at least seven. For other payment systems, requirements to meet the core principles vary, but institutions may use their compliance as a selling point, as compliance is viewed as a measure of quality.

5.3 Development

After establishing the information security objectives of the organization, and assessing the impact of regulations and legislation, a plan of action should be developed that is consistent with the established business objectives. This plan should be used as the roadmap for the development of a corporate information security policy (Policy)[1].

It is essential that a corporation develop a Policy and that it take into account the corporate objectives and particular aspects of the organization. The security policy must be consistent with the corporate business, culture, and the regulatory and legislative environment in which the business operates. The development of a Policy is essential to ensure that the results of the risk management process of the security programme are appropriate and effective. Management support across the organization is required for the development and effective implementation of the Policy. With the alignment of security policy to corporate business objectives, the Policy will help to achieve the most effective use of resources, and will ensure a consistent approach to security across a range of different information system environments.

5.4 Documentation hierarchy

5.4.1 Overview

5.4.1.1 General

Three levels of information security programme documentation are described in this guideline. These are the corporate information security policy (Policy) document, the security practice documents and the operational security procedures documents[2]. The documentation hierarchy and the meaning of each level are illustrated in Figure 1.

[1] Throughout this document, “Policy" is synonymous with “corporate information security policy".

[2] This nomenclature and hierarchy are not definitive. Organizations may use more levels of hierarchy and different nomenclature.

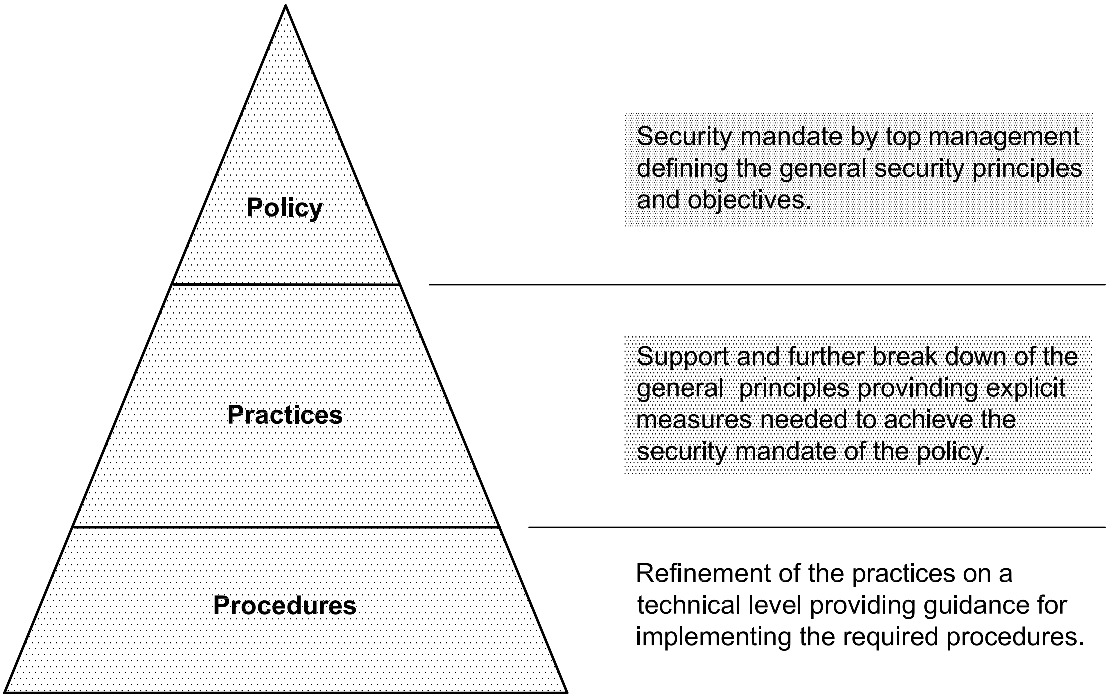
Policy
Security mandate by top management defining the general security principles and objectives.
Practices
Support and further break down of the general principles provinding explicit measures needed to achieve the security mandate of the policy.
Procedures
Refinement of the practices on a technical level providing guidance for implementing the required procedures.

Figure 1 — Programme documentation

The information security documents should range from the high level organizational goals down to the specific security settings of devices that implement the security policy. This range of general and specific information is best covered in multiple layers of documentation. The number of levels should be kept to a minimum, and this guideline recommends three: a Policy document, security practice documents, and operational security procedures documents.

Additional documents will be required as new and emerging technology is introduced into the organization. While the Policy document will often be a single page, the procedures documentation may consist of many multi-page documents representing separate, specific environments, business units, and policy issues within the organization. In some cases, a single, well-bounded system may also have its own practices document. All practices and procedures should flow from the higher level to the detailed level, maintaining a consistency with corporate risk assessments and the overall Policy.

5.4.1.2 Corporate information security policy

The Policy document is the smallest of all of the documents in the information security programme document hierarchy. Typically, the Policy is documented in a few paragraphs explaining that management regards information in any form as a valuable corporate resource that must be protected. The Policy should be broad in scope and stated as simply and concisely as possible, but should provide specific information of the assets to be protected, e.g., customer data, employee records, partner agreements and processes. For example, a very simple Policy document might contain the single assertion, "*The confidentiality, availability, and integrity of all corporate information assets must be protected by appropriate security controls*".

The Policy document is an abstract document, comprehensive in scope, and the most influential of the information security programme documents in its effects on the organization. Only a single instance of the Policy document should exist at any given time, and it should be promulgated throughout the organization. It should be signed by the board members involved in Information security, e.g. the Chief Executive Officer (CEO) and the Chief Information Officer (CIO).

The Policy document should be public in nature, widely distributed and made available to all of the organization's stakeholders. It should stress that protecting and providing information assets is the responsibility of management and all employees, and that management at the highest level is committed to security education and awareness.

It should be clear to all stakeholders that the Policy document derives its authority directly from the corporate officers and board-level personnel. The document should state the intention of the organization to operate in accordance with relevant local and international legal and regulatory strictures, and to base their information security programme on sound principals and practices recognized in national and international security standards.

The Policy document should be almost immutable. It should change only as required by shifts in strategic goals, changes in perceived business risk, or events affecting the regulatory and legal environment in which the organization operates. Corporate officers and board-level personnel should dictate the change control parameters and procedures.

5.4.1.3 Representation

When developing the Policy, representatives from a variety of functions should participate. The development group should include members of the board of directors, executive officers, legal representation, risk management committee and audit committee members. In formulation of the policy, the development group will obtain input from experts throughout the enterprise, e.g. information technology, physical security and finance functions.

5.4.1.4 Information classification

One aspect of implementing the Policy is the classification of information. Much like the military systems of "Top Secret", "Secret" and "Unclassified", financial organizations have information with differing values. The results of information asset classification will indicate when a good, better or best control should be implemented. There are many types of classification system. For the financial organization, the important point is to define classification levels and leverage the classification of the information in making risk acceptance decisions. For example, a risk that is acceptable for public information would likely be unacceptable for highly classified information. One benefit of classifying information is to communicate management's expectation of how employees should handle the information. If a document, file or database contains information at various classification levels, it must be treated according to the procedures established for the highest classification level of information it contains.

It is important to note that the classification level of information may change during its useful life. These changes should be controlled under the Policy of the organization.

5.4.2 Security practice documents

Security practice documents are derived from the content of the Policy document. These documents specify the general security standards that should be followed by the organization. They mirror the intentions and goals established by the highest levels of management in creating the information security programme, and document the intention to implement the Policy in a technology-independent way. Each security practice document is narrower in scope than the Policy document. Each practice document is a technology-neutral and content statement of the organization's security requirements. The size of a given practice document is variable and topic-dependant.

The number of practice documents should be kept to a minimum. The number of documents needed varies with the size of an organization and its business needs, and with the scope and complexity of the organization's activities. The legal and regulatory environment that affects the organization can also influence the number of practice documents needed.

A practice document is not public[3]. It is general purpose in nature, and technology-neutral. It is less abstract than a Policy document, and may have less influence on the overall organization, since it may be applied only to some aspects of the organization. For example, a very simple practice document might contain the simple assertion:

[3] There may be occasion to furnish a practice document to regulators.

> “Access to Corporate information assets must be authenticated in a manner commensurate with the sensitivity of the asset. Two-factor authentication is the minimum acceptable level of authentication; assets classified ‘Confidential’ by the asset owner should be accessible only with three-factor[4)] authentication. Two-factor (biometric and password-based) access control systems must enforce the following regulations…”

Though practice documents derive their authority from, and must strictly comply with, the Policy, they are more mutable than policy documents. This is because they are subject to changes that are more frequent, arising as new risks and controls are identified. Each practice document has a restricted audience, as it usually affects a specific part of an organization or business unit, does not affect the overall security management programme of the organization.

It is helpful to include a document scope section that indicates the audience and owner of each practice document. The owner of a practice might be a business manager, an IT manager or an operations manager. It is also helpful to include how information related to a given practice is classified, as the category of classification indicates the level of protection the information requires.

5.4.3 Operational security procedures documents

Operational security procedures documents are derived from one or more security practice documents. Their lengths vary with the topic and complexity of the procedures. These documents are the narrowest in scope of all of the documents in the document hierarchy. They are technology-specific expressions of how the Policy is implemented. These are applied to actual business systems, and vendor-specific product details are covered in platform-dependent documentation.

There should be as many procedures documents as necessary, but care should be taken when developing the documents that they are complete, accurate and appropriate and that none of them contradicts any other practice or Policy. An example of the type of guidance to be found in a very simple procedures document might be one that contains the instructions:

> “Use the ‘*pwadmin*’ command to ensure that user passwords meet the criteria established in the Corporate Access Control and Authentication Practice document. Issue the following commands ...”

Procedures documents must comply with the overall Policy of the organization and the practices that the procedures are based on. No procedure document should contradict any policy-based practice. Regulatory restrictions, externally produced standards, and other procedural documents must be taken into account.

The procedures documents should include results of previous security risk analysis and management reviews including identification of any residual risks, results of follow-up actions such as security compliance checking of implemented controls, a list of actions to be taken to monitor and review information security in day to day use, and reports of security relevant incidents.

6 Management of information security — Security programme

6.1 General

Implementing the Policy requires an information security programme. At the highest level, the ethical values and control imperatives of corporate management must be communicated and periodically reinforced with management and staff. Information security is a team-based process as well as an individual responsibility. Developing, maintaining, improving and monitoring an information security programme requires participation by multiple disciplines in the organization. Close coordination is required between the business managers and

[4)] The term “three-factor" is often expressed by the phrase “what you have, what you know and what you are". What you have may be a card or token. What you know may be a PIN or pass phrase. And a biometric is used to represent what you are.

the information security staff. Disciplines such as audit, insurance, regulatory compliance, physical security, training, personnel, legal, and others should be used to support the information security programme.

6.2 Programme establishment

The most important recommendation of this Technical Report is that organizations establish an information security programme. This programme should follow from the Policy established for the organization at the highest level of corporate management. The information security programme should provide for establishing and maintaining detailed security processes throughout the organization, compatible with the Policy.

The development of detailed information security processes and procedures may require coordination of different business functions in the organization, including audit, risk, compliance, and insurance, officers responsible for regulatory or legal compliance, as well as partners and customers.

6.3 Awareness

The security awareness programme should include a security education and awareness function that ensures that all employees remain knowledgeable and alert to the security implications of their actions and the actions of those around them. The programme should be structured to keep employees aware of their security responsibilities, and provide resources and encouragement to those with an interest in security to extend their knowledge.

6.4 Review

One or more officers of the organization should be assigned ongoing responsibility for the information security programme. Established practices should cause the programme to be reviewed and updated, and as new threats and technologies emerge, ensure that necessary safeguard investments are provided. The programme should include detailed processes and procedures that establish responsibility and accountability for measuring and reporting on the soundness of and compliance to the information security programme.

All monitoring and review reports should be made available to multiple levels of management, including executives. Procedures for addressing any policy exceptions or deviations should be identified and documented. There should also be procedures for the production of necessary audit and compliance records and the monitoring of the security of audit journal information. Special attention must be paid to identifying risks to audit journal information and requirements established to mitigate these risks and to provide assurance that these information assets are adequately protected.

6.5 Incident management

All information security events should be reported promptly, documented, and resolved according to the organization's practices. When unwanted or unexpected information security events have a significant probability of compromising business operations and threatening information security, they become information security incidents that must be addressed. Both incidents and events should be used by security professionals in their re-assessment of risk and their selection and implementation of security controls. Events and incidents should be used in the ongoing improvement of the information security programme.

6.6 Monitoring

Formal mechanisms should be established for reporting intrusions, system malfunctions and other security incidents, the results of forensics following security incidents, and incident management documentation results should be employed in the review process in order to influence investment in safeguards, and to cause the controls used to protect assets to be re-evaluated and changed over time.

6.7 Compliance

An independent review should ensure that the practices adhere to the established Policy, and that controls are adequate and effective. Any waivers granted should be documented and limited in time so that they are subject to periodic re-evaluation.

6.8 Maintenance

Established controls, such as firewalls and virus scanning software should be updated regularly so that they remain effective against new and emerging threats.

6.9 Disaster recovery

The information security programme should identify information assets that are critical to an organization continuing to conduct business activities in the event of a disruption. The programme should establish detailed written plans for the resumption of business following disasters. The skilled personnel, legal agreements, information back-up systems, processing resources and locations available to replace those that support critical business activities should be planned for, and these plans for resuming business following a disruption should be tested and evaluated regularly.

7 Organization for information security

7.1 Commitment

An organization-wide commitment to the goals of the information security programme must be based on an understanding of both the global and internal information security needs of the organization. The organization must demonstrate a commitment to the programme by its willingness to allocate resources for information security activities and to address its information security needs. There must be awareness, at the highest level of the organization, of what information security means to the organization, and its scope and extent.

The goals of information security should be promulgated throughout the organization. Each employee or contractor should know their role and responsibility and their contribution to information security and be empowered to achieve such goals.

7.2 Organization structure

7.2.1 Roles and responsibilities

The purpose of the information security programme is to ensure the confidentiality, integrity and availability of information assets. Achieving these goals is an interdisciplinary task. Appropriate assignment and demarcation of responsibilities should be associated with specific roles. Procedures should ensure that all important tasks are accomplished and that they are performed in an efficient way.

7.2.2 Directors

Directors of financial institutions have a duty to the organization and its shareholders to oversee the business management practices of the organization. Effective information security practices constitute prudent business practice, and demonstrate a concern for establishing the public trust. Directors should communicate the idea that information security is an important objective and support an information security programme.

7.2.3 Audit committee

The audit committee in a financial organization assists the board of directors in its overseeing and serves as an independent arm for objective checks and balance on internal controls and financial reporting. Monitoring and testing internal controls that are part of the information security programme are part of the audit committee's responsibilities, normally conducted through the organization's internal audit function and external auditors.

7.2.4 Risk management committee

The risk management committee under the board of directors should review the security programme, and support funding for information security projects whenever these projects reduce the operational risk (and therefore financial risk) of the organization. The risk management committee demonstrates the organizational commitment to security by funding and supporting projects that fulfil the information security policies of the organization. The committee must determine how regulations and legislation impact the information security programme as discussed in greater detail in 5.2.

7.2.5 Legal function

Organizations may rely on the specialized expertise of their legal department (or function) for some aspects of security information management. The legal department may be assigned responsibility to monitor changes in the law through legislation, regulation and court cases that could affect the organization's information security programme.

The legal department may be required to review contracts concerning employees, customers, service providers, contractors and vendors to ensure that legal issues relating to information security are addressed adequately. Such reviews may include privacy or workplace safety issues, as well as employee termination and grievance procedures.

The legal aspects of security incidents and how they affect the organization may require the advice of the legal department. Organizations may wish to rely on expert advice in assessing the implications of security incident handling procedures, and ensuring that they comply with the legal requirements of the operating environment, as they vary according to local jurisdictions. The legal department should be involved in developing, maintaining and improving procedures for handling follow-up to security incidents, such as preservation of evidence.

7.2.6 Executive officers

The Chief Executive Officer (CEO), or managing director, as the most senior officer of the organization, has ultimate responsibility for its operation. The CEO should authorize the establishment of, and provide support for, an information security programme consistent with recognized standards, oversee major risk assessment decisions and participate in communicating the importance of information security.

While many organizations are familiar with the role of the Chief Executive Officer, Chief Financial Officer (CFO), Chief Technical Officer (CTO) and Chief Operating Officer (COO), many organizations have begun introducing additional roles such as the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) near the top of the organizational chart. While there are many permutations on the roles of CTO, CIO, and CISO, every financial organization should have a senior or Chief Information Security Officer that ultimately reports to the CTO or CIO.

7.2.7 Business managers

Business managers specifically, and managers throughout the organization generally, serve as supervisory and monitoring agents for the organization and its employees. This makes them key players in information security programmes. Each manager should understand, support and abide by the organization's Policy, practices and procedures, and ensure that employees, vendors and contractors do so as well. Business managers should create a positive atmosphere that encourages employees, vendors and contractors to report information security concerns.

7.2.8 Employees

Security programme requirements should be incorporated into employee employment contracts. All personnel should be aware of the security implications of their actions, and the actions of those around them. They should promptly report any suspicious information security events.

7.2.9 External

Security programme requirements should be incorporated into vendor service agreements and contractor agreements. Vendors and contractors should understand, support, and abide by organizational and business unit information security practices and procedures. They must adhere to the corporate information security policy. While organizations may choose for economic or other business reasons to out-source banking functions the management of risk cannot be out-sourced and remains the responsibility of the organization.

7.2.10 Security roles

7.2.10.1 Introduction

Three security roles for personnel within an information security programme are identified here. These roles are invested with different levels of responsibility and functions necessary to carry out the information security programme. The roles are functionally defined and how the organization provides for administrative and managerial control of the personnel may vary.

In some organizations, the information security personnel may exist in a separate administrative unit. In other organizations, personnel in a business unit may be assigned information security responsibilities in addition to their business duties. There could also be a mixture of these two approaches.

Whatever structure the information security programme takes, the executive officers and managers must support it to make it effective. In large organizations, it may be helpful to develop other roles to efficiently perform specialized functions, e.g. a security architect. In smaller organizations, personnel may need to assume multiple roles.

7.2.10.2 Chief Information Security Officer (CISO)

The Chief Information Security Officer is responsible for the design, implementation and management of the information security programme. Under the direction of the CISO, personnel at the other levels perform duties that carry out the policy and practices of the information security programme. The CISO may have a dedicated staff and exercise administrative control of the information security personnel. In another scenario, the CISO may have limited operational control of personnel who perform information security duties in addition to their business duties. Regardless of the size or management style of the organization, the CISO is the person who is ultimately responsible to the directors and executive officers for the execution of the information security programme.

The CISO manages the information security programme in response to the conditions that have been identified by the organization as relevant to business success. The CISO is responsible for:

- preparing the budget and justifying the information security programme to the executive officers;
- developing a security architecture that is in concert with the business strategy;
- managing other levels of personnel who implement the security architecture and perform information security duties;
- performing risk assessments that will validate the security architecture and undercover flaws that need attention;
- publishing the security policy, practices, procedures and managing a security awareness programme;

- remaining aware of current threats and vulnerabilities and new information security techniques to counter them;

- ensuring appropriate organizational involvement in the critical infrastructure protection efforts for the countries where the organization does business.

7.2.10.3 Information Security Officer (ISO)

An Information Security Officer is any person in the organization who is responsible for developing, implementing and maintaining the information security programme under the direction of the CISO. ISOs may be on the staff of the CISO or may be under the administrative control of a business unit of the organization. An ISO may have a special designation such as Security Architect because of extensive knowledge and experience. Some ISOs may possess specialized expertise in information security techniques such as risk assessment, threat awareness, etc. and act as a resource for the entire organization. Other ISOs will provide guidance and advice to a particular business unit on information security concerns. The ISOs will be most effective if they understand the business objectives as well as the internal processes of the organization.

The ISOs should:

- understand the security architecture, practices, and procedures;

- develop local practices, publish them and update as appropriate;

- conduct risk assessments;

- monitor and audit security practices;

- assist in recovery from attacks on the IT system;

- make recommendations for improved practices and procedures;

- keep up-to-date on information security threats, technologies and techniques;

- promote information security awareness.

7.2.10.4 Security operators

Security operators perform the most detailed day-to-day actions in order to accomplish the objectives of the information security programme. Security operators may be on the staff of the CISO or may reside in other units of the organization. They must be knowledgeable of the hardware, software and security procedures necessary for their business units.

Because of the variety of technology that might be utilized in security architecture, security operators will need to perform a myriad of procedures. Some representative duties that might be required are: install and maintain security settings on network equipment; install security updates on operating systems; maintain and update accurate access control files; collect information security, audit information and monitor system and network activity to discover security problems. The wide variety of tasks shows the importance of security operators in the successful operation of the information security programme.

The security operator is responsible for:

- understanding how the security operator role supports the security architecture and programme;

- implementing and maintaining security practices and procedures;

- monitoring security procedures and reporting their status as appropriate;

- acting to correct security failures and to counter attacks;

- re-establishing appropriate security procedures in concert with business recovery after a failure or attack;
- making recommendations for improved practices and procedures.

8 Risk analysis and assessment

8.1 Processes

Organizations that wish to access their security posture should implement one or more risk analysis processes as part of their information security programme. These processes should be used to evaluate the entire organization's security posture, as well as the security of specific projects, systems, and products. Because management styles and organizational sizes and structure will differ, more than one strategy may be needed to tailor the risk analysis to the environment in which it is used[5].

A risk assessment process should result in recommendations for reducing the security risks of an organization to an acceptable level. These recommendations should guide in the selection of appropriate controls. These controls are the result of assessing and giving a value to the possible loss that could occur should identifiable system vulnerabilities be exploited by one or more threats. Organizational assets that are usually subjected to a risk assessment include: facilities and equipment, software applications, corporate databases, communications and computer operating systems.

Annex D provides an example of a method for performing risk assessments and an example of a typical risk assessment process. Additional risk assessment models can be found in other sources, such as ISO/IEC 13335 (all parts). The examples in Annex D are provided for illustrative purposes, and should not be used directly as implementation checklists by an organization.

8.2 Risk assessment process

Financial institutions and all other enterprises are impacted by risks to their business. Risks to the information assets of the enterprise come in many forms, and should to be methodically analysed. Risk assessments need to consider the vulnerabilities, threats and risks to information. Each banking application provides the context and understanding of the work processes and the potential threats and areas of vulnerability. This understanding is important when performing the risk assessment. The risk assessment is a three-step process:

1) assessing the risks of the potential threats for each area of vulnerability by completing the risk assessment matrix form (see Clause D.1);

2) assigning a combined risk level to each area of vulnerability by completing the risk assessment table (see Clause D.3);

3) determining the applicable security policies and safeguards by using the results of step 2 and the controls available.

A more detailed list of risk categories and how they apply to the risk assessment process is presented in Annex C.

8.3 Security recommendations and risk acceptance

A risk assessment may be performed to evaluate risk at the organization level, within a related set of systems, across a single system or applications, or on specific critical functions within a system. It is unrealistic to expect that the organizational level risk assessment is simply the combination of all the critical functions within the organization.

[5] See ISO/IEC 13335 (all parts) for additional information.

The vulnerabilities and threats change constantly as new technologies emerge, new vulnerabilities are discovered in systems, new or upgraded products are introduced and the organization continues to grow and evolve. Therefore the level of detail and the conclusions of a risk assessment may be widely different for different systems within an organization, and for similar systems within different organizations.

Nevertheless, any risk assessment should conclude with some set of security recommendations for the system that has been assessed. These recommendations will address the risks associated with the system as implemented. It is the responsibility of appropriate business managers to accept the risks. In many cases, additional controls may be applied (or may have been applied during the design or development phase) to reduce the risks to a more acceptable level. The risk acceptance should be guided by the organization's security practices. In considering exceptions to policy, the business manager should work with the information security team to ensure that compliance with policy will be met in the future, or that a longer-term exception to policy is accepted as residual risk.

9 Security controls implementation and selection

9.1 Risk mitigation

Any system will have vulnerabilities through which attackers may threaten to cause financial loss, productivity loss or loss of reputation to the organization. Minimizing and mitigating these risks is the joint responsibility of the business managers and information security team working with other groups within the financial organization. There are many facets to managing the risk, and many of the most important have already been discussed: commitment to information security from the highest management, a CISO responsible for implementing and managing a security programme, and the security programme itself.

In 9.2 to 9.7 are discussed important processes and technologies commonly used or considered for providing risk mitigation. These may be used during the development process, after a too high-risk assessment or after a new vulnerability has been identified. Business managers should keep in mind the well-documented advantages of designing security into a system rather than trying to patch a broken existing system.

The use of these technologies can provide direct control over the risks an organization assumes. An organization needs to assess how planned and existing controls reduce the risk identified in the risk analysis, identify additional controls available or able to be developed, develop information security architecture and determine constraints of various types. Appropriate and justified controls should then be selected to reduce the assessed risks to an acceptable level of residual risk. Additional details on the selection of controls can be found in ISO/IEC 13335[4] (all parts).

9.2 Constraint identification and review

Many constraints can affect the selection of controls. These constraints must be taken into account when making recommendations and during the implementation. Typical constraints and considerations include:

Constraint	Consideration
Time	Controls should be implemented within a period acceptable for management, implemented within the lifetime of the system and remain effective for as long as management deems necessary.
Financial	Controls should not be more expensive to implement than the value of assets they are designed to protect.
Technical	Controls should be technically feasible and compatible with the system.
Sociological	Controls may be specific to a country, a sector, an organization, or even a department within an organization to ensure acceptability to staff.
Environmental	Controls selected need to accommodate: space availability, climate conditions, surrounding natural and urban geography, etc.
Legal	Controls need to respect legal factors like personal data protection or criminal code non-IT specific laws and regulations like fire department regulations, labour relations laws etc.

9.3 Logical access control

9.3.1 General

Logical access control refers to the group of technical control techniques employed within systems and applications to limit access to information according to the practices of the organization. In general, users should be given the minimum access needed to perform their job functions, but often system limitations, design or other constraints may result in people having some additional access. Nonetheless, it is critical to have accountability for system access: i.e. to know who is being granted access, to know to what individuals have access, and to know when that access has occurred. Most important of all it is critical to enforce access limitations once defined. The following controls should be put into place to achieve effective access control.

9.3.2 Identification of user

Many different types of users may have reason to have access to the information and information systems of a financial organization. Examples of types of users include employees, customers, system administrators and managers. In most instances, it is necessary to know with some certainty, which class of user is attempting to gain access to a particular application. It is very often necessary to know not only the class, but also the exact identity of who is attempting to gain access.

Traditionally, each information system had its own identification process. With the rapid expansion of systems, there is a continuing need for an identification process that will satisfy multiple systems. It may prove feasible to have these identification services out-sourced. The following guidelines should apply no matter who is providing identification services.

To provide higher levels of confidence in the identity of users, the organization should establish and enforce policies requiring verification of user identity before a user ID can be issued. Prudent business practice demands that “know your customer” and “know your employees” requirements are integrated into user ID issuance activities. Moreover, the organization should establish and enforce procedures to ensure that, prior to its issuance, each new user ID is indeed unique and can be traced to both the individual identified and the issuer.

9.3.3 Authorization

Authorization is the act of providing a user with the ability to perform specific actions on a system based on the authenticated identity of the user. The organization should determine the access rights of each user. No user should be allowed to access any information or application unless specifically authorized.

Several paradigms exist for maintaining records of such role based access controls (RBAC). One traditional paradigm is the maintenance of a central listing of the privileges for each user. Information System Security Administrators, usually working under dual control, track and maintain such records. Security software matches a user ID against the records and allows users access to information or applications according to the records.

Another paradigm is for distributed maintenance of records with an access control listing on each system, or separate access for different types of application (e.g. thin client, fat client, web, multi-tier, web services, etc.).

9.3.4 Authentication of users

9.3.4.1 Mechanisms

User authentication refers to the process (e.g., procedural, physical or via hardware/software) by which a user’s identity is verified to the system. Users may be internal or external to the organization and failure to authenticate a user’s identity reduces the ability of an organization to prove accountability for the actions of an individual and may allow unauthorized access to data and computer resources.

There are several types of authentication mechanism. They are based on one or more of the following characteristics: something the user knows (e.g. passwords); something the user possesses (e.g. a smart card); some physical characteristic of the user's (e.g. fingerprint or other biometric measurement). Combining multiple authentication mechanisms can ensure higher levels of authentication.

9.3.4.2 Digital certificates

Digital certificates can be used for signing or encrypting information, and providing user, program code and device authentication. Digital signatures based on certificates can be used to provide authentication of origin of information, data integrity and non-repudiation services. Certificate-based data privacy services can be provided using encryption. ISO 15782 specifies controls and syntax needed for certificate management of X.509 certificates in the financial services. ISO 21188 provides detailed information on how to manage certificate security policy information in the organization, and the necessary elements of certification practice statements.

9.3.4.3 Passwords

The most common authentication method used today is the password. A password is a character string composed of any combination of letters, numbers and special keyboard characters. Knowledge of the password that is associated with a user is considered proof of authorization to use the capabilities associated with that user (e.g. access to specific programmes, capabilities and files on the system).

Passwords can be either dynamic (e.g. generated and changed automatically and usually frequently by the software) or static (e.g. changed infrequently at the discretion of the user). Guidelines for forming and controlling the use of passwords can be found in many publications and on the web. “US Dept. of Defense Password Management Guideline” dated 12 April 1985 (CSC-STD-002-85) provides technical treatment on the generation, control and use of passwords within an organization. The discussion at http://computing.fnal.gov/security/UserGuide/password.htm provides a more general treatment of the topic and includes discussion on password sharing, composition and length, changing, and storage.

9.3.4.4 Biometrics

Biometrics is the science of identifying persons by some physical characteristic that can be measured and has a high probability of being unique to an individual. Fingerprints are perhaps the best known biometric. Electronic devices exist that are capable of reading a fingerprint and comparing the print with a print already stored in the system. Other physical features that may be used in a biometric identification system include retinal patterns in the eye, hand geometry, facial features and the voice.

ISO 19092[11] describes how biometric information can be managed in the financial services as part of the organization's information security management programme. This Technical Report specifies control objectives, controls and a detailed event journal for managing biometric information, and achieving these objectives.

9.4 Audit journals

Audit journals are system-generated records of activity used by organizations to provide a means of reconstructing events and establishing accountability. The audit journal information is essential to problem or dispute resolution and provides evidence for regulatory compliance. Audit journals help to deter unauthorized activity and provide an early detection of such activity. All systems should provide some level of audit journal based on the organizational policies. Likewise, the level of detail should be as detailed as possible, consistent with the operational needs and policies of the organization. Where practicable, audits can provide real time alarms of significant security events.

The audit system should support prompt investigation and reporting of suspicious activity, to aid in deterring and detecting unauthorized activity. Management reviews of audit journal information should be performed on a timely basis, usually daily, and all security exceptions and unusual occurrences should be investigated and reported.

Audit journal information should be retained for an appropriate period relative to business requirements. This information must be protected from accidental or malicious deletion, modification or fabrication.

9.5 Change control

To protect the integrity of an organization's information-processing facilities, change control procedures should be implemented. Without change control, monetary and productivity losses may occur due to improper processing or loss of services. Change control procedures should exist for hardware changes, software changes for both applications and operating systems patch management, and manual procedure changes. These change control procedures must also address management of emergency changes.

Business managers must ensure proper change control processes for the systems under their control. The information security team should be prepared to help manage security-related changes and to manage changes on security systems that the information security team is directly responsible for managing.

9.6 Information security awareness

Part of the information security programme should be a security awareness campaign to educate employees to protect the organization’s valuable information. The programme is meant to influence, in a positive way, employees' attitudes towards information security. Security awareness should be addressed on an on-going basis.

A security awareness programme should provide an induction class for new employees and employees of a new company. The programme should educate users whenever new applications are introduced, or existing applications are extensively modified. It should constantly address security concerns that appear in the press.

Different levels of management and staff have different concerns. Specific concerns of each group should be emphasized when addressing each group. Presentations must be made in such a way that people of all levels and skills will be able to understand. Managers should be made aware of the exposure, risks and loss potential, as well as regulatory and audit requirements. This should be presented both in business terms and with examples pertinent to the manager's area of responsibility, with positive messages being the most effective.

9.7 Human factors

The work force is one of the most important assets of a financial organization. The interest and cooperation of employees are essential in any successful information security programme. Through heightened security awareness, the employees will be alert to noticing abnormalities in the organization’s technology or operational procedures which may indicate a possible security problem.

On the other hand, human beings also make mistakes. They can misuse the technology. They may also commit crimes. These human failures make it imperative for the CISO to dialogue with all departments of the organization in the development of the information security programme and security awareness. Other departments can contribute their insights about the organization's employees to minimize opportunities for mistakes and criminal activity.

Certain positions in any organization may be designated “trusted” because the position grants or requires access to sensitive personnel or financial information. Another trust position is an employee who has extensive privileges or powerful capabilities on the organization’s computers or IT assets. Personnel selected for “trust” positions should have high integrity and undergo a thorough background investigation. Employees in trust positions should be counselled on the need to limit their discussions with family and acquaintances about the sensitive business procedures. Business competitors may attempt “social engineering”, the seduction of a person to disclose information to unauthorized people. The seducer uses false interest in the person’s work, technical discussions and flattery to have the employee unwittingly reveal sensitive information.

10 IT systems controls

10.1 Protecting IT systems

There are many ways to protect IT systems. These controls may include policies within the organization. However, for the purposes of Clause 10, controls will represent system settings and external countermeasures (like encryption), which can be used to provide authentication, authorization, confidentiality, integrity, availability and other security services. Countermeasures and controls currently in use as well as those expected to be available in the future will be discussed.

In addition to the initial placement of controls and countermeasures, the organization must take steps to ensure their long-term operation and maintenance. Otherwise, over time, as new vulnerabilities become known and issued patches are ignored, the system security will erode. A well-run security programme includes maintenance processes and procedures that ensure required controls remain in place, and are kept up to date.

10.2 Hardware systems controls

The protection of the hardware systems in the IT environment is critical to the integrity of information assets. Some of the most important controls for protecting critical resources are discussed in Annex D. This Technical Report does not attempt to include a comprehensive list of all the IT resources an organization might use, rather, a short discussion for each of the several major types of resources, and some of the appropriate controls that may be used to reduce the threats to these resources is provided in Clause D.1. Each discussion follows a similar pattern. Key concerns are addressed in each discussion. These include why a particular system is important, what security areas may be most important, and what controls need to be considered.

One issue not addressed, and that organizations sometimes fail to consider, is the providers of their hardware systems. It is common to take as a matter of trust that equipment providers and manufacturers are working on the behalf of the financial organization, or with an awareness of their security objectives and policies. However, it is possible that machines can come from the manufacturer or reseller configured to provide unauthorized access to information or network connections. Random purchasing and sporadic distribution of machines around the network can help safeguard against this kind of malicious or unintended security threat. For high security applications, controls that build trust between the organization and the vendor may need to be considered.

For cryptographic devices in particular, hardware evaluations such as FIPS 140-2[6)][17] should be considered critical. For other devices, common criteria evaluations against appropriate or industry standard protection profiles should be relied on in choosing and using a device.

[6)] FIPS 140-2 is being progressed as international standard ISO/IEC 19790.

10.3 Software systems security

Because modern financial institutions rely on automation to process almost all of their transactions, at the heart of the information security programme is software security. Providing security for software systems is difficult because of the complexity, the myriad interactions and the multiple ways to access the software. In addition, many systems like firewalls, web servers and application servers are designed to operate on many hardware platforms. The material in Clause A.2 discusses software systems security at a high level as abundant literature exists that focuses in detail on the security of each type of software system.

10.4 Network and network systems controls

Although an organization's computing complex, including end systems and various types of servers, is often thought of as most important, the great majority of traffic between systems runs across a network that is neither encrypted, nor particularly well managed. Much of the Internet and many companies' dedicated "leased lines" use the same open protocols, routing systems, and in some cases share the same network devices and switches with the traffic of other companies.

Network traffic is vulnerable to rerouting, copying, and packet sniffing[7)] attacks that can easily occur completely undetected by the network and systems using the network. While encryption is often treated as a magic bullet for communication security, network layer encryption can be too expensive and costly in performance, throughput and latency for many enterprises. While SSL, IPSEC and other communication security protocols may be used, they are not necessarily the first line of defence for network security. For managing network security, consideration should be given to the guidance available in the "ISO/IEC 18028.

Instead, the first line of defence is often the contractual arrangement between the organization and the telecom provider, and the trust in the telecommunications provider. Therefore, the use of reputable telecommunications providers, with well defined service level agreements and thorough contract language is often the first and most important control. The next most important network control would be the system of border controls (as described in 10.5) used to secure, monitor and manage the organization's connections between internal and external networks.

10.5 Border and connectivity controls

10.5.1 General

Much has been written in the literature about the increasing openness of corporate networks. What was once a hardened, tightly controlled perimeter has been opened for web services, business partnerships, outsourced support, customer interaction with systems of record, temporary and contract labour, as well as employee access – both remote accesses from home and external connections to other businesses. The increasing permeability of the border means that border and connectivity systems continue to be a critical element of corporate information security. The permeability also means that more and more devices are possible entry points for malicious activity. These devices need to have consideration for firewalls, intrusion detection and potentially for other controls, as noted in the discussion of end systems in Clause D.1.

All of these border connections between the enterprise and the larger networked environment are critical; any border represents an opportunity for threats to attack vulnerabilities in the enterprise. Enterprises need to determine their own policies for how border controls are applied. For instance, an organization could require isolation to achieve a highly secure environment, e.g. all users and end systems to be physically connected inside the organization's building. On the other hand, an organization could protect all of its assets within a secured database behind a secure web application server, behind multiple layers of firewalls and intrusion

[7)] A "packet sniffer" is a programme that analyses information "packets" as they travel along a network looking for information that can be used to launch an attack, such as the contents of e-mail messages, user names and passwords, or network addresses.

detection software, or with strong user authentication checks. What's appropriate depends on the assets of the organization, their risk assessment, and their policies.

10.5.2 Firewalls

Firewalls represent a mature technology for providing border controls at the network layer. While there are variations in actual capability and function, all firewalls sit between a border router and switch connecting the enterprise to other entities or the Internet, and the enterprise's internal network routers. A well-designed firewall is an essential element in protecting the organization's network.

The firewall monitors the network traffic based on addressing, ports, protocols and in some cases the packet contents. For many organizations, the firewall will only be open to a very small set of all available addresses, ports and protocols. As an example, a firewall protecting a web server complex might only allow the HTTP protocol on port 80, or HTTPS protocol on port 443 (also known as SSL). Other common ports for FTP services, SMTP (e-mail) may also be opened or closed in accordance with organizational needs and policies.

Many organizations apply two layers of firewalls to create a so-called DMZ or De-Militarized Zone. Web servers, and other outward facing servers and services would sit between the firewall layers, and reformat and redirect traffic requests for services or data inside the larger enterprise. The external firewall might only support http traffic, while the inner firewall might allow SSH (secure shell) or other services to support access for managing the web servers, or to allow the web servers access to internal databases. A common practice is to use firewalls of two different types (manufacturers) for the internal and external positions.

Historically, firewalls have been special purpose software or dedicated appliances that sit in the network path and protect large parts of the enterprise; they were a major part of the strength of hardened perimeters. Over the past 2-3 years, firewalls have been incorporated into end systems, often as so-called personal firewalls. Both trends, that of dedicated appliance type firewalls for major network connections, and personal firewalls on PCs and other end systems are continuing.

The most recent trend is the combination of firewall functionality with intrusion detection capability.

10.5.3 Intrusion detection system (IDS)

Firewalls frequently accept or deny connections based on the address, port and protocol. Within these parameters, there may be many possible data streams that are actually attacks or malicious software – as well as the majority, which are of legitimate data streams intended to support legitimate business activities. Intrusion detection systems look at the data within the packets and compare that to characteristics of known attacks. The detection systems then send alerts through e-mail, 'phone calls or pagers to appropriate personnel within the organization. There are two major kinds of IDS: network detectors are attached to network routers, switches and servers and look at traffic on the network; host based detectors are software loaded on to servers and end systems that look at traffic connecting to a specific device. Both types of detectors are being deployed in growing numbers across enterprises[8)].

One major limitation of IDS systems is the reliance on known attack characteristics, whilst valid, new attacks, with unknown characteristics, may slip through undetected. IDS systems have begun to look for anomalies in the behaviour of systems such as, ftp traffic where there is normally only http traffic or traffic at odd times or abnormal volumes. These anomaly detection capabilities are becoming more sophisticated and complex, but their value is still largely unproven. Nonetheless, many organizations, and most IDS vendors have begun adding IDS analysis capabilities or analysis that looks for anomalies not only at the borders, but also within the enterprise network itself.

Some analysis tools are pure tools, relying on other devices to capture the data used to look for anomalies. Firewall and IDS systems are beginning to converge; often a vendor will sell combined products that do both firewall and IDS functions. These combined products are also being used – especially when the IDS includes anomaly detection features – to perform intrusion prevention. In these emerging intrusion prevention systems,

[8)] Note that work has begun in the JTC 1/SC 27 IT Security Techniques group to define an IDS standard, ISO/IEC 18043.

the network connection used for a detected attack is closed to stop or prevent the attack before it can be completed. While this is a perfectly acceptable practice, there is a trade-off since other legitimate traffic may be coming through the same connection. Organizations must determine for themselves when the value of allowing legitimate traffic outweighs the possible damage of an attack.

This value judgment of allowing possible attacks versus the possible damage from an attack, highlights one of the limitations of IDS systems. In virtually any IDS system there will be some number of false positive results. That is in some cases the IDS will create an alert on traffic that looks like an attack but is actually valid. Likewise, there is the (very slim) possibility that an attack will go through undetected. IDS systems allow the organization a great deal of flexibility in tuning the system to minimize both false positives and false negative responses.

10.5.4 Other protective countermeasures

There are many other protective countermeasures for network borders and connectivity. Various use cases demand different considerations. For example, a close business partner might have a direct connection to the internal network, or they might be routed through a single firewall, rather than through two firewalls. The routers and switches that make up the organization’s internal networks need to be secured and well managed. Many firewall functions act as a layer of security behind the routing functions already performed by the network infrastructure. Beyond network, firewalls and IDS, there are two other major countermeasures: encryption and authentication. Encryption obviously can be used to protect private information. This can be done at many layers and in many places, but at some cost. These tradeoffs need to be evaluated against organizational policy and the value of corporate information.

Authentication can be used for both authenticating the devices, as well as the users of the devices (including software ”users“). Devices can be authenticated using IPSEC or to some degree through SSL. The end user may be authenticated through SSL, although SSL may not really authenticate the actual user (some browsers for example, remember user names and passwords, so anyone using that computer and browser would appear to be John Smith from a web server perspective. Using multiple factors, not just a user ID and password, can strengthen authentication but so can possession of a token or smart card, possession of the private key associated with a digital certificate, or fingerprints (or other biometric).

11 Implementation of specific controls

11.1 Financial transaction cards

11.1.1 General

Financial transaction cards may be magnetic stripe cards, which may store information on magnetic media or ”smart cards"[9] which may process information, perform cryptographic functions, and store much more information than possible on magnetic media. Since smart cards have more flexibility than magnetic-stripe cards, other uses for these cards may be developed in the future. Please refer to ISO 10202 for security concerns for smart cards.

Financial card associations maintain their own minimum-security standards for financial institutions and contractors providing services to financial institutions. In addition to those security programmes, organizations using financial transaction cards should employ the controls listed below.

[9] The term “smart card" describes a class of payment card-sized devices that have different functionalities and varying capabilities. These devices have an almost identical appearance to the familiar magnetic-stripe cards used for standard credit, debit, ATM and POS transactions, and include integrated circuit cards (ICC), stored-value cards and contactless cards.

11.1.2 Physical security

To protect against the destruction, disclosure, or modification of transaction card information while in the processing stages, the card personalization facility should be located in an area regularly patrolled by public law enforcement services and served by fire protection services. The facility should be protected by an intrusion alarm system with auxiliary power.

11.1.3 Insider abuse

To prevent fraudulent transactions being made through access to card information, all media containing valid account information, account numbers, PIN numbers, credit limits, and account balances should be stored in an area limited to selected personnel. Production and issuing function for cards should be kept physically separate from the production and issuing function for PINs.

11.1.4 Transportation of PINs

To prevent losses from PINs being intercepted by unauthorized persons, PINs should be handled in accordance with ISO 9564-1 to -4 or ISO 10202-1 to -8. ISO 9564 specifies the basic principles and techniques for providing the minimum-security measures required for effective international PIN management. It also specifies PIN protection techniques applicable to financial transaction card originated transactions in an online environment, and a standard means of interchanging PIN data. ISO 9564 also covers PIN management and security in the offline PIN environment and the electronic commerce environment. These techniques should be used by organizations responsible for implementing techniques for the management and protection of PIN information at Automated Teller Machines (ATMs) and acquirer sponsored Point-of-Sale (POS) terminals.

NOTE ISO 13491-1[5] specifies the key management controls needed for financial services devices (POS, ATM).

This Technical Report does not cover the privacy of non-PIN transaction data, protection of the PIN against loss or intentional misuse by the customer or authorized employees of the issuer, protection of transaction messages against alteration or substitution, e.g. an authorization response to a PIN verification, protection against replay of the PIN or transaction, or specific key management techniques. These techniques should be used by organizations responsible for implementing techniques for the management and protection of PIN information at Automated Teller Machines (ATMs) and acquirer sponsored Point-of-Sale (POS) terminals. ISO 10202 specifies the principles for the protection of integrated circuits throughout their life cycle, from manufacture and issue, through use by customers and employees, to termination. The minimum level of security required for interchange is also specified in ISO 10202, along with security options that allow the financial transaction card issuer or supplier to select a level of security appropriate with application policy. Cryptographic key relationships, proper use of cryptographic algorithms and the key management techniques needed for the security for the processing of financial transactions are also specified in ISO 10202. Security requirements for application modules that can be added to card accepting devices are also described.

11.1.5 Personnel

To prevent the assignment of unsuitable personnel to credit card processing duty, credit and criminal record checks should be conducted for all employees handling embossed or unendorsed cards, including part-time and temporary employees, where permissible by law.

11.1.6 Audit

To ensure the integrity of control and audit information requires that controls and audit logs be maintained for printed plastic sheets, plates, embossing and encoding equipment, signature panel foil, holograms, magnetic tape, semi finished, and finished cards, sample cards, cardholder account numbers information and waste disposal equipment.

11.1.7 Counterfeit card prevention

To prevent information disclosed on sales drafts from being used to produce counterfeit magnetic stripe cards, cryptographic check digits should be encoded on the magnetic stripe, and these digits should be validated on as many transactions as possible.

To prevent intercepted information from being use to produce counterfeit cards, physical Card Authentication Method (CAM) should be used to validate the authenticity of cards.

11.1.8 Automated teller machines

Automated Teller Machines (ATM) are those devices that allow a customer to check account balances, make cash withdrawals and deposits, pay bills, or perform other functions that are generally associated with tellers. These devices may be inside an organization's buildings, attached to the outside of such a building, or remote from any organization office.

Additional precautions to reduce robbery of customers and vandalism to the machines are recommended, but beyond the scope of this Technical Report. Manufacturers of these devices and ATM network providers generally publish security guidelines for the use of ATMs. These documents should be consulted. ATM transactions should adhere to the security requirements as specified by the card payment schemes.

11.1.9 Cardholder identification and authentication

The most common means of cardholder authentication is the Personal Identification Number (PIN). They are used to control access to ATM and POS devices. Users should be educated to understand that PIN secrecy is their responsibility. In addition to PINs, biometric and other technologies are beginning to be used for cardholder identification.

To prevent unauthorized transactions caused by guessing the PIN of a card being used by a non-authorized person, the number of PIN entry attempts should be limited to three. After three unsuccessful attempts, it is recommended that the card be captured and its owner contacted.

11.1.10 Authenticity of information

To prevent the unauthorized modification of information transmitted to and from ATMs, the use of a Message Authentication Code (MAC) generated under the requirements of ISO 16609 and distributed under the requirements of ISO 11568 should be required for each transmission. To prevent unauthorized modification, destruction or disclosure of information residing in an ATM, physical access control to the interior of ATMs should be consistent with physical protection controls on containers of currency.

11.1.11 Disclosure of information

To prevent the unauthorized use of ATM and Point of Sale (POS) terminals through the unauthorized disclosure of PIN information entered by the user, only devices with encrypting keypads that conform to ISO 9564 should be used. Consider encrypting all information transmitted from the ATM. PINs should be managed in accordance with relevant ISO standards.

11.1.12 Fraud prevention

To detect and prevent fraudulent use of ATMs, such as kiting schemes, empty envelope deposits and disavowed transactions, a number of practices is recommended. These include limiting the number of transactions and amount of funds withdrawn per day per account, balancing the ATM under dual control daily, installing video cameras if fraud experience or potential warrant it, and maintaining operation of ATMs on line whenever possible, i.e., requiring that the ATM have the ability to check account balances prior to completing transactions. If online operation is not possible, establish more stringent card issuance requirements than would be used if operation were on line.

11.1.13 Maintenance and service

To prevent unauthorized access to information during maintenance and servicing of ATMs, ensure that ATMs are placed ”out-of-service" to customers prior to any maintenance being performed. Dual control procedures should be established for the servicing of ATMs that involve opening the vault.

11.2 Electronic fund transfer

11.2.1 Unauthorised source

The threats and controls associated with Electronic Fund Transfer (EFT) applications can be evaluated in a manner that is independent of the technology that they use. To prevent loss through the acceptance of a payment request from an unauthorized source, the source of messages requesting fund transfer should be authenticated. Source authentication should be based on a security procedure specified in a customer or correspondent agreement. Cryptographic authentication is recommended whenever cost and performance make application of this control feasible.

A MAC generated under the requirements of ISO 16609 with a cryptographic key distributed under ISO 11568 provides cryptographic authentication. Alternatively, successful decryption of a message encrypted under ISO/IEC ISO 18033 (coupled with ISO/TR 19038[10] or ANSI X9.52[14]) or FIPS 197[18] with a key distributed under ISO 11568 may be used to establish authenticity of the source of the message. Digital signature may also be used.

11.2.2 Unauthorized changes

To prevent an improper payment due to changed message contents, whether intentional or accidental, authenticate the payment date, value date, amount, currency, beneficiary name and possibly beneficiary account number or IBAN components of a message, using a security procedure specified in a customer or correspondent agreement. Full text authentication should be used whenever practical. Cryptographic authentication is recommended.

11.2.3 Replay of messages

To prevent an unauthorized repeated payment caused by a replayed message, require the use and verification of unique message identification. Include this identification in any authentication performed.

11.2.4 Record retention

To preserve evidence that may be needed to prove authorization in making a payment, record the messages requesting transfer of funds, regardless of media used to transmit the messages. Material necessary to prove authentication, including supporting cryptographic material, should be preserved.

11.2.5 Legal basis for payments

To ensure that payments are being made in compliance with a signed agreement, establish a system that will ensure that agreements underlying EFT requests are in place and current.

11.3 Cheques

11.3.1 General

Cheques, also known as negotiable orders of withdrawal, or share drafts, are written orders directing a financial organization to pay money. Several new approaches to processing cheques should raise security concerns to financial institutions. The image of a cheque and other truncation schemes are examples of techniques that generate security concerns. Many national bodies have published standards on various aspects of cheque processing operations[10].

11.3.2 New customers

The requirement to “know your customer” poses special challenges when services are delivered through open networks. While it may be desirable to advertise services using a homepage or other electronic medium, a personal visit to a financial organization’s place of business should be a prerequisite to opening a new account (except when operating under a legally established method) until a universally recognized and enforceable electronic method of positive personal identification is available. Normal customer qualification procedures should be observed.

11.3.3 Integrity issues

Each transaction should be protected to ensure identification of user, authenticity of user, authenticity of message, confidentiality of sensitive information, and non-repudiation of instructions.

Transaction requests should be digitally signed using a key authenticated by the organization’s certification authority. Properly implemented, this should provide assurance that the user is identified, the message contents unchanged, and the user is legally bound to his or her actions.

Account numbers, PINs, or other information, which, if revealed, would allow unauthorized use of an account, should be protected with encryption.

12 Miscellaneous

12.1 Insurance

In planning the information security programme, the Information Security Officer and business manager should consult with the insurance department and, if possible, the insurance carrier. Doing so can result in a more effective information security programme and better use of insurance premia.

Insurance carriers may require that certain controls, called Conditions Prior to Liability or Conditions Precedent, be met before a claim is honoured. Conditions Prior to Liability often deal with information security controls. Since these controls must be in place for insurance purposes, they should be incorporated into the organization's information security programme. Some controls may also be required to be warranted, i.e. shown to have been in place continuously since inception of the policy.

Business interruption coverage, errors and omissions coverage in particular, should be integrated with information security planning.

12.2 Audit

The following quotation from the Institute of Internal Auditors defines the auditor's role as follows:

> “Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control,

[10] Subcommittee B of X9 (USA) has published standards on cheque processing operations such as ANSI X9 TG-2 *Understanding and Designing Checks* and ANSI X9 TG-8 *Check Security Guideline*. To achieve consistency among financial organizations and improved processing performance, financial organizations are strongly urged to follow the recommendations of X9 Technical Guideline 2 (TG-2) and X9 Technical Guideline 8 (TG-8).

> and governance processes. Internal auditing reviews the reliability and integrity of information, compliance with policies and regulations, the safeguarding of assets, the economical and efficient use of resources, and established operational goals and objectives."

More specifically, in the area of information security, auditors should evaluate and test safeguards over the information assets of a financial organization, and engage in an ongoing dialogue with Information Security Officers and others to bring appropriate perspectives to the identification of threats, risks, and the adequacy of safeguards for both existing and new products.

Auditors should provide management with objective reports on the condition of the control environment and recommend improvements that can be justified by need and cost benefit, and specify retention and review of audit journal information. Where the audit review function is combined with other functions, management attention is required to minimize conflict of interest potential.

12.3 Disaster recovery planning

An important part of an information security programme is a plan to continue critical business activities in the event of a disruption. Disaster recovery is that part of business resumption planning that ensures information and information-processing facilities are restored as soon as possible. A disaster recovery plan identifies the range of disasters that must be protected against, and outlines the roles and responsibilities of personnel under those conditions.

The disaster recovery plan should include an accurate listing of those business activities that are considered critical, preferably with priority rankings, and should include time frames for resumption adequate to meet the business commitments of the organization. The plan should identify the processing resources and locations available to replace those that support critical business activities.

In the event that personnel are unable to report to the organization to assist in disaster recovery, replacement personnel capable of restoring and operating information processing resources should be identified. When possible, the organization should seek to obtain agreements with service providers for the priority resumption of services. The disaster recovery plan should ensure the availability of adequate information back-up systems capable of locating and retrieving critical information in a timely fashion.

It is important that the disaster recovery plan identify the information to be backed up, and ensure that this information is saved securely and on a stated schedule. The location for information storage should also be identified, with consideration given to on site and off site requirements.

The disaster recovery plan should be tested as frequently as necessary to find problems and to keep personnel trained in its operation. A periodic re-evaluation of the recovery plan should be undertaken periodically to ascertain that it is still appropriate for its purposes. The organization should specify a minimal frequency for both tests and re-evaluations.

12.4 External service providers

Financial institutions require that externally provided critical services, such as data processing, transaction handling, network service and software generation, receive the same levels of safeguard and information protection as those activities conducted within the organization itself. External service provider contracts should include the elements necessary to satisfy the financial organization that:

— providers abide by the security policy and practices of the organization;

— reports prepared by the providers own public accounting firm are made available to the organization;

— internal auditors from the organization have the right to conduct audits of providers relating to the organizations procedures and safeguards;

— providers are subject to escrow agreements of delivered systems, products or services.

In addition to the above, an independent financial review of the provider should be conducted by specialists within the financial organization before engaging in a contract with a service provider.

No business should be transacted with a service provider unless a letter of assurance has been obtained stating information security safeguards are in place. The CISO should examine the service provider's security programme to determine if it is in concert with the organization's. Any shortfall should be resolved either by negotiations with the provider or by the risk acceptance process within the organization.

In addition to information security requirements, contracts with service providers should include a non-disclosure requirement and clear assignment of liability for losses resulting from information security lapses.

12.5 Penetration test teams

The use of a penetration tester, usually a contractor, to access the effectiveness of system security by attempting system penetration, with the full knowledge and consent of an appropriate official of the organization, is one method of deriving assurance for the security programme.

As computer systems become increasingly complex, security will become increasingly harder to maintain. Use of penetration test teams can help in finding specific points of weakness in an organization's system. However, some issues must be considered. The contractor should be adequately bonded or of sufficient strength to meet any liabilities arising from their efforts.

The organization should not rely solely on penetration test reports to monitor its security programme.

Non-disclosure of results should be addressed in the contract with the penetration testers. Any disclosure of security problem should be at the discretion of the organization.

12.6 Cryptographic operations

The growth in IT has made the traditional methods of controlling information much more challenging. The popularization of cryptographic devices has provided the opportunity for financial institutions to recapture the level of security previously associated with banking, while also reaping the benefits of increased information processing technology.

As with any emerging technology, there is a danger of misapplying cryptographic solutions. It is important for organizations to make appropriate decisions on the selection, use and continuing evaluation of their cryptography based safeguards.

It is assumed that the need for a cryptographic safeguard has been identified. The safeguards suggested in Clauses 9 to 15 employ encryption, message authentication codes and digital signature. Each of these services also requires key management or certification services.

Appropriate cryptographic safeguards can counter threats against confidentiality and integrity of information. Cryptographic safeguards such as encryption and authentication require that certain material, e.g. cryptographic keys, remain secret.

One or more facilities that generate, distribute and account for cryptographic material may be required to support cryptographic safeguards. ISO standards on banking key management should be used wherever possible.

The facilities providing cryptographic material management should be subject to the highest level of physical protection and access control. Key management must be performed under split knowledge to preserve the security of the system.

Sound cryptographic practices and effective disaster recovery planning foster conflicting objectives. Close consultation between those responsible for disaster recovery and cryptographic support is imperative to ensure that neither function compromises the other.

Supply of cryptographic materials to customers should be done in a manner that minimizes the possibility of compromise. The customer should be made aware of the importance of security measures for cryptographic material. Interoperation with a customer's, correspondent's or service provider's cryptographic system should only be allowed under a fully documented letter of assurance.

The quality of security delivered by cryptographic products depends on the continued integrity of those products. Both hardware and software cryptographic products require integrity protection consistent with the level of security they are intended to provide. Use of appropriately certified integrated circuits, anti-tamper enclosures and key zeroizing, make hardware systems somewhat easier to protect than software. When circumstances allow, software cryptographic products may be used. Features that enhance system integrity, such as self-testing, should be employed to the maximum degree feasible.

Cryptographic products are subject to varying governmental regulations as to use, import and export. Local regulations on the use, manufacture, sale, export and import of cryptographic devices vary widely. Consultation with local counsel or authorities is advised.

12.7 Key management

As with any technology, there are elements that are relatively easy to implement and maintain and others that pose major efforts to accomplish. One such area that requires careful planning, education and precise implementation is cryptographic key management. Standards that address key management include ISO 11568.

Key management is that part of cryptography that provides the methods for the secure generation, exchange, use, storage and discontinuation of the cryptographic keys used by the cryptographic mechanism. The incorporation of cryptographic techniques like encryption and authentication into computer systems and networks can achieve many security objectives. However, these techniques are of no value without the secure management of the cryptographic keys.

The major functions of key management are to provide the cryptographic keys required by the cryptographic techniques and to protect these keys from any form of compromise. The specific procedures and security requirements for key management depend on the type of cryptosystem upon which the cryptographic techniques are based, the nature of the cryptographic techniques themselves and the characteristics and security requirements of the computer system or network being protected.

The most important element to consider is that key management must be flexible enough for efficient use within the computer system or network, but maintain the security requirements of the system. Key management services must be available when and where they are needed, including at back-up sites. Key management must be part of an organization disaster recovery plan.

12.8 Privacy

Financial institutions possess some of the most sensitive information about individuals and organizations. Laws and regulations require that this information be processed and retained under certain security and privacy rules. Certain technical and business developments, such as networks, document imaging, target marketing, and cross-departmental information sharing, have led to concerns about the adequacy of banks' privacy protection.

Financial institutions should review all privacy laws and regulations, such as those involving credit information. Consideration should also be given to keeping current on emerging national privacy legislation, through bank law offices, bank industry sources, or other independent information sources. In addition, banks that have international operations need to be aware of regional and international and other privacy laws and regulations that apply.

Financial institutions should review their operations to determine whether information on their customers and employees is adequately protected. Specific policies and procedures should be developed concerning how information is gathered, used and protected. These policies and procedures should be made known to relevant employees. Privacy policies and procedures should address:

- collection of information to ensure that only information that is relevant to an identified business need, and is accurate be collected;
- processing of information to provide appropriate restrictions over access, including determination of who should have access to information, quality control to avoid errors in data entry or processing, and protection against inadvertent unauthorized access;
- sharing of information, so that it occurs only through pre-determined procedures, that information is used for purposes relevant to the reasons for its original collection, and that such sharing does not lead to new opportunities for unauthorized privacy invasion by other parties;
- storage of information to ensure that it occurs in protected fashion to disallow unauthorized access;
- notification of information use and the availability of procedures that allow the person whose information is being held, to correct errors and to raise objections over the use of this information;
- secure destruction of information when no longer needed.

In addition, electronic and other forms of employee monitoring must meet legal requirements that vary by jurisdiction. Employee privacy protection and due process rights need to be considered in addition to employer rights.

Financial institutions might consider developing a privacy audit. This audit evaluates how well the organization is achieving privacy protection and considers ways by which IT can address privacy problems.

13 Follow-up safeguards

13.1 Maintenance

The maintenance of safeguards, which includes administration of these safeguards, is an essential part of a financial organization’s security programme. It is the responsibility of all levels of management to ensure that:

- responsibility for the maintenance of safeguards is clearly established;
- organizational resources are allocated to the maintenance of safeguards;
- safeguards are periodically reviewed and re-validated to ensure that they continue to perform as intended;
- hardware/software modifications and upgrades to an IT system do not change or negate the intended performance of the existing safeguards;
- advances in technology do not introduce new threats nor vulnerabilities;
- safeguards are upgraded and/or new safeguards added when new requirements are discovered;
- security policies are reviewed and amended, or new policies added, based any changes to the safeguards.

When the maintenance activities described above are accomplished, adverse or costly impacts will be avoided.

13.2 Security compliance

Security compliance checking, also known as security audit or security review, is a very important activity. Compliance checking is used to ensure conformance and compliance with the IT information system security plan, and to ensure an appropriate level of information security remains effective throughout the operational lifetime of an IT project or system. This includes the design, development and implementation phases, as well as the application of updates, enhancements or revisions. Care must also be taken when replacing or disposing of system components.

Security compliance checks may be conducted using external or internal personnel (e.g., auditors) and are often based on the use of checklists relating to the IT project or system security policy. Security compliance checking should be planned and integrated within the IT project or system plan.

An additional technique that is particularly helpful in determining whether operational support staff and users are conforming to specific safeguards and procedures is spot checks. Checks should be made to ensure that the correct security safeguards are implemented, used correctly and, where appropriate, verified through testing. Where safeguards are found to not conform to the system security plan, area management should be advised, a corrective action plan should be produced, implemented, tested and the results reviewed.

13.3 Monitoring

Monitoring is an important component of the information security plan. Monitoring can give management an indication of the safeguards that have been implemented, whether these safeguards are satisfactory, and whether a safeguard maintenance programme has been implemented. An initial security plan can be compared with the results of monitoring to determine which safeguards did and did not work.

Many safeguards produce output logs of security relevant events. These logs should be periodically reviewed, and, if possible, analysed using statistical techniques to permit the early detection of trend changes, and the detection of recurring adverse events. All changes to assets, threats, vulnerabilities and safeguards potentially could have a significant effect on the risks, and early detection of change permits preventive action to be taken. The use of logs only for post event analysis is to ignore an important safeguard mechanism.

Monitoring should also include procedures for reporting to the relevant information security officer and to management on a regular basis.

14 Incident handling

14.1 Managing events

A security event is an identified occurrence of a state in an information or communications system that indicates a possible breach of security Policy or the failure of a safeguard to adequately protect an asset. Any previously unknown or unexpected situation may have security relevance and should be treated as a security event. A security incident is a series of one or more unwanted or unexpected security events that have a significant potential of threatening information security and harming business operations. It is inevitable that security events will occur. Each event should be investigated to determine whether it is a security incident. This investigation should be, to a depth, commensurate with the damage caused by the event, or the potential damage the event could have caused.

Incident handling provides an ability to react to accidental or deliberate disruption of normal IT system operation. An incident reporting and investigation scheme suitable for the whole of the organization's IT systems and services should be developed. This scheme should include reports to IT and business line groups, to gain a wider view of the occurrence of information security incidents and related threats, and their associated effects on IT assets and business operations. Additional information on incident handling and managing events can be found in ISO/IEC TR18044[9].

The fundamental objectives during an information security incident investigation are to react to an incident in a sensible and effective manner, and to learn from the incident so that future similar adverse events may be avoided. In some situations it may be necessary, particularly to safeguard the organization's reputation, from ill informed adverse public criticism, to protect the confidentiality of the information relating to the security incident.

A prepared plan of actions with predefined decisions will allow an organization to react in reasonable time to limit further damage and, where relevant, to continue business via auxiliary means. A plan for incident handling must include the requirement for the chronological documentation of all events and actions. This should lead to the identification of the source of the incident. This is a precondition to reaching the second aim, namely to reduce future risk by improving the safeguards.

It is important that an incident analysis be also executed and documented, addressing the following questions.

- Was the chronology of events and actions documented correctly?
- Was the plan followed?
- Was the required information available to the relevant staff?
- Was the required information available on time?
- What would the staff propose to do differently the next time?
- Was the incident analysis process (detection/response/reporting) functioning efficiently or can it be improved?
- Are there any controls to prevent the security event from happening again?

Answering these questions and resolving the findings will reduce the impact of future incidents.

14.2 Investigations and forensics

Some incidents will require additional investigation. Fraud perpetuated over time, dissatisfied employees and some legal matters will demand an ability to investigate activities on the IT systems. System logs, IDS logs, and sometime whole disk drives may need to be gathered and analysed to support an investigation. Forensic analysis of the data on a drive, including looking for deleted files, and other types of detailed analysis may be needed. Most organizations will have only a limited in-house capability to perform these investigations and analyses. However, all security programmes should include some minimal training in evidence handling, and a plan for who will carry out the investigations, how they will be engaged, and what kinds of forensic analysis they can and will perform. Actual needs will vary widely from organization to organization, and incident to incident.

14.3 Incident handling

The incident-handling plan should be well known to all who will participate in handling the incident. It should consider many potential issues: out of normal stated hour incidents, communication needs (both for those within the organization and communication with media and customers), back-up and contingency plans, communication with vendors and suppliers – including business partners.

14.4 Emergency problems

To maintain integrity during emergencies, security processes should not be bypassed. Specific processes to permit emergency fixes only to resolve production problems should be in place, and a return-to-normal change procedure should be made as soon as possible. In any change, those making the change, including emergency support personnel, must document changes. Finally, review all emergency changes.

Annex A
(informative)

Sample documents

A.1 Board of directors resolution on information security

Resolved:

Information is an asset of the corporation.

As an asset, information and information processing resources of the corporation shall be protected from unauthorized or improper use.

The Chief Executive Officer is directed to establish an information security programme, consistent with prudent business practice with the goal of properly securing the information assets of the corporation.

A.2 Information security policy

INFORMATION SECURITY POLICY

for

THE ABC FINANCIAL ORGANIZATION

ABC Financial Organization considers information, in any form, to be an asset of the corporation and requires appropriate safeguards to be in place to protect these assets from unauthorized or improper use. Information is vital to the efficient and effective day-to-day operation of the corporation. This information must only be used for its intended purpose – the conduct of ABC Financial Organization's business operations. It is our corporate policy to provide access to information only on a proven “business need to know” basis and deny access to all others.

Each ABC Financial Organization's business unit senior managers has the responsibility to maintain the confidentiality, integrity and availability of their information assets and must comply with all policies, standards and procedures published by the Information Security Department concerning the protection of corporate information assets.

All employees have a continuing responsibility to understand, support, and abide by all corporate policies, standards and procedures governing the protection of information assets.

A.3 Employee awareness form

The Corporation considers information to be an asset that should be protected.

It is my duty to understand, support and abide by corporate policies, standards and procedures governing the protection of information assets.

I have been given a copy of the Corporate Information Security Handbook, and agree to follow the rules in it.

I agree to use corporate information and information processing equipment to which I have access, only for the purpose of discharging the duties of my job.

I understand that the organization may review any information or messages I may generate using information processing resources of the organization. This includes, but is not limited to, word processors, e-mail systems, and personal computers.

I agree to report any suspicious behaviour or situation that may endanger corporate information assets, to my supervisor immediately.

I understand that misuse of corporate information assets may result in disciplinary proceedings being taken against me.

Date ________________________

________________________________ ____________________________________

Printed Name of Employee Signature

____

Witness (or supervisor)

A.4 Sign-on warning screens

This is a private computer system with access restricted to those with proper authorization. Authorized parties are restricted to those functions that have been assigned to perform related duties. Any unauthorized access will be investigated and prosecuted to the full extent of the law. If you are not an authorized user, disconnect now.

Alternatively:

This computer system is restricted to authorize users. Unauthorized access/attempts will be prosecuted. If unauthorized, disconnect now.

A.5 Facsimile warnings

Payment Warning

WARNING

Do not rely on this transmission for paying money or initiating other transactions without independent verification of its authority

Proprietary Statement

The documents included with this facsimile transmittal sheet contain information from the ABC Corporation that is confidential and/or privileged. This information is for the use of the addressee named on this transmittal sheet. If you are not the addressee, please note that any disclosure, photocopying, distribution or use of the contents of this faxed information is prohibited. If you have received this facsimile in error, please notify the sender by telephone immediately so that we can arrange for the retrieval of these documents at no cost to you.

A.6 Information security bulletin

COMPUTER VIRUS ALERT

According to national reports, a computer virus known as “The Michelangelo Virus” has been spreading rapidly throughout the world and could be the most damaging virus in years. It is known to infest DOS based systems running version 2.xx or higher.

IMPACT

This virus sits passively on infected computers until the trigger date of March 6th (Michelangelo's birthday). On that date, it overwrites critical system data, rendering the disk unusable. Data infected includes the boot record and the file allocation table (FAT) on the boot disk (whether floppy or hard disk).

Recovering user data from a damaged disk will be very difficult.

SYMPTOMS

Reported symptoms include:

- a reduction in the free/total memory by 2048 bytes and
- floppy disks which become unusable or display odd characters during DIR (directory) commands.

It is important to note that the Michelangelo virus does **not** display any messages on the PC screen at any time.

INFECTION RISK

The virus is spread by:

- booting from an infected diskette (even if the boot is unsuccessful) or
- by booting from a hard disk while there is an infected diskette in the “A” drive and the drive door is closed.

Data storage media, which are used on both business and home computers, may present a higher than normal risk.

A.7 Risk acceptance form

INFORMATION SECURITY RISK ACCEPTANCE

This form should be completed only where a business process or system does not comply with the Information Security Policies and Standards, and there is no plan to comply with the policy in question in the near future.

Division ____________________ Requesting Unit Number ______________________

Unit Manager ________________ Requesting Unit Name ________________________

Page and Item Number in Policy/Standards _______ Date ________

Risk Acceptance Requested for (describe) ____

____

____

____

Description of Business Process (attach additional documentation as appropriate)

____

____

____

Total number of transactions by period ____

Total monetary volume of transactions by period ____

Is transactions time dependent? (describe) ____

Are general ledger accounts affected? ____________________

Level of management receiving output ____________________

Significance of decisions based on output ____________________

Regulatory/legal considerations ____________________

Is output distributed to customers? (describe) ____________________

Highest classification of information processed ____________________

Description of System Used to Support the Business Process (attach additional documentation as appropriate) ____________________

____

____

Describe type of equipment (number of computers, models, etc.) ____________________

____

Describe type of network connectivity (LAN, VTAM, dial-up, etc.) ____________________

____

Processing locations ____________________

Number of users ____________________

Geographic distribution of users ____________________

Describe interfaces to other systems ____________________

____

Availability requirements ____________________

Are other applications run on this equipment? (describe) ____________________

____

Are systems supported by Central Systems Group? If not, describe support arrangements.

____

____

Describe business/system requirements for policy compliance ____

____

____

Estimated cost of compliance ____

Describe current or proposed safeguards to mitigate risk ____

____

____

Estimated cost of current or proposed safeguards ____

Other factors to consider in this decision (other alternatives considered, additional business factors, what other companies do, etc.) ____

____

____

Recommended by ______________________________ Date __________________________

Unit Manager

Reviewed by : _________________________________ Date: _________________________

Information Security Officer

Comments: ____

____

____

Approved by: __________________________________ Date _________________________

Senior Officer with Delegated Authority

Risk Acceptance Number (assigned by Security Officer) ______________________________________

Date of next review ____

Information Security Classification:

A.8 Telecommuter agreement and work assignment

EMPLOYER - EMPLOYEE TELECOMMUTING AGREEMENT

This agreement, effective is between ________________________ , (hereinafter referred to as “Employee”), and _________________ (hereinafter referred to as “Company”). The parties, intending to be legally bound, agree as follows:

SCOPE OF AGREEMENT

Employee agrees to perform services for Company as a “Telecommuter.” Employee agrees that telecommuting is voluntary and may be terminated at any time, by Company with or without cause.

Other than those duties and obligations expressly imposed on Employee under this agreement, the duties, obligations, responsibilities and conditions of Employee's employment with Company remain unchanged.

The terms “remote work location” or “remote workplace” shall mean Employee's residence or any remote office location approved by Employee's management.

TERMS OF AGREEMENT

This agreement shall become effective as of the date first written above, and shall remain in force and effect as long as Employee telecommutes, unless sooner terminated.

TERMINATION OF AGREEMENT

Employee's participation as a telecommuter is entirely voluntary and is available only to employees deemed eligible at Company's sole discretion. There exists no right to telecommute. However, when you volunteer and are selected to telecommute, Employee will make a commitment to telecommute for a period of no less than “x” months. Company will not be held responsible for costs, damages or losses resulting from cessation of participation as a telecommuter. This writing is not a contract of employment and may not be construed as such.

COMPENSATION

Work Hours, Overtime, Shift Differentials, Vacations: Employee agrees that work hours, overtime compensation, shift differentials and vacation schedule will conform to the terms agreed upon by Employee and Company.

TELECOMMUTING AND INCIDENTAL EQUIPMENT

Employee agrees that use of equipment, software, data supplies, and furniture, provided by Company for use at the remote work location, is limited to authorized persons for purposes relating to the business, including self development, training and tasks. Employee will use telecommunications equipment strictly for business use. Company will in no way be responsible for telecommunications charges incurred by employee while conducting personal business.

The Company, at its sole discretion, may choose to purchase equipment and related supplies for use by Employee while telecommuting or permit the use of Employee-owned equipment. The decision as to the type, nature, function and/or quality of electronic hardware (including, but not limited to, computers, faxes, video display terminals, printers, modems, data processors and other terminal equipment), computer software, data and telecommunications equipment (i.e.: phone lines) shall rest entirely with the Company.

The decision to remove or discontinue use of such equipment, data and/or software shall rest entirely with the Company. Equipment purchased for use by Employee shall remain the property of the Company. The Company does not assume liability for loss, damage or wear of Employee-owned equipment.

Employee agrees to designate a workspace within Employee's remote work location for placement and installation of equipment to be used while working. Employee shall maintain this workspace in a safe condition, free from hazards and other dangers to Employee and equipment. The Company must approve the site chosen as the Employee's remote workplace. If any changes to the initial installation and set-up location of telecommunications equipment by the Company, Employee is responsible for expenses.

Employee agrees that Company may make on-site visits to the remote work location for the purpose of determining that the site is safe and free from hazards, and to maintain, repair, inspect or retrieve Company-owned equipment, software, data and/or supplies. In the event legal action is necessary to regain possession of Company-owned equipment, software, data and/or supplies. Employee agrees to pay all cost of suit incurred by Company, including attorney’s fees, should Company prevail.

In the event of equipment failure or malfunction, Employee agrees to immediately notify Company in order to effect immediate repair or replacement of such equipment. In the event of delay in repair or replacement, or any other circumstance under which it would be impossible for Employee to telecommute, Employee understands that Employee may be assigned to do other work and/or assigned to another location, at Company's sole discretion.

Furniture, lighting, environmental protection and household safety equipment incidental to use of Company-owned equipment, software and supplies shall be appropriate for their intended use and shall be used and maintained in a safe condition, free from defects and hazards.

Employee agrees that all Company-owned data, software, equipment, facilities and supplies must be properly protected and secured. Company-owned data, software, equipment and supplies must not be used to create Employee-owned software or personal data. Employee will comply with all Company policies and instructions regarding conflicts of interest and confidentiality. Any software, products or data created as a result of work-related activities are owned by Company and must be produced in the approved format and medium. Employee agrees that upon termination of employment, Employee will return to Company all things belonging to Company.

LIABILITY FOR INJURIES

Employee understands that Employee remains liable for injuries to third persons and/or members of Employee's family on Employee's premises. Employee agrees to defend, indemnify and hold harmless Company, its affiliates, employees, contractors and agents from and against any and all claims, demands or liability (including any related losses, costs, expenses and attorneys fees) resulting from or arising in connection with any injury to persons (including death) or damage to property, caused directly or indirectly, by the services provided hereunder by Employee or by Employee's wilful misconduct or negligent acts or omissions in the performance of Employee's duties and obligations under this Agreement, except where such claims, demands or liability arise solely from the gross negligence or wilful misconduct of the Company.

MISCELLANEOUS CONDITIONS

Employee agrees to participate in all studies, inquiries, reports or analyses relating to telecommuting for Company, including inquiries that Employee might consider personal or privileged. Company agrees that Employee's individual responses shall remain anonymous on request by Employee, but that such data may be compiled and made available to the general public without identification of Employee.

Employee remains obligated to comply with all Company rules, policies, practices, instructions, and this Agreement and understands that violation of such may result in preclusion from telecommuting and/or disciplinary action, up to and including termination of employment.

I affirm by my signature below that I have read this agreement and understand its subject matter. I affirm that I was given the opportunity to have this agreement reviewed by my own counsel prior to entering into it.

Employee’s Signature: ______________________________

Date: ____

Telecommuting, or working from another location such as home, is an assignment that may be chosen to be made available to some employees when a mutually beneficial situation exists.

Telecommuting is not an employee benefit, but rather is an alternate method of meeting the needs of this Company. Employees do not have a “right” to telecommute; the Company can terminate the arrangement at any time.

These are the conditions for telecommuting agreed upon by the telecommuter and his or her supervisor.

1) The employee agrees to work at the following location:

2) The employee will telecommute _________days per week.

3) The employee's work hours will be as follows:

4) The following are the assignments to be worked on by the employees at the remote location with the expected delivery dates:

5) The following equipment will be used by the employee in the remote work location:

6) The following is the arrangement agreed upon for handling telephone calls made by the telecommuter from the remote work location for Company business:

7) The employee agrees to obtain from ___________ all supplies needed for work at the alternate location; out-of-pocket expenses for supplies regularly available at the Company office will not normally be reimbursed.

8) Employee will be required to make regular visits to the ___________________________ Centre to attend training and team/supervisor meetings.

I have reviewed the above material with ________________________ prior to his or her participation in the Company's telecommuting programme.

Date __________ Supervisor's Signature _____________________________________

The above material has been discussed with me.

Date __________ Employee's Signature ______________________________________

Annex B
(informative)

Web services security analysis example

B.1 High level security analysis

B.1.1 Overview

Like policies, which can be very high level, or extremely detailed, a risk analysis can be completed at varying levels of detail. This subclause provides a high level discussion of web services, an emerging technology important to many financial services companies and others using the Internet for business. This example analysis is for illustrative purposes only, and should not be considered as a specific security recommendation. As noted throughout this document, each organization must make its own security and risk determinations based on their specific policies and business needs.

Web Services (WS) is the general industry term for the emerging set of Extensible Markup Language (XML)-based standards that allow computers to exchange data and enact business functions and transactions over the Internet. The core WS functions allow the creation of information services that can be accessed by other computers rather than human eyes through browsers. Web Services are powerful in their ability to interoperate across systems, across business units and across companies.

The main components of a Web Service are:

- an application server that houses the service (i.e. where the service software code runs);
- an interface for the service (often described in Web Services Description Language, WSDL);
- a data store or directory with the WSDL interface description so WS clients can find (and use) the interface;
- a WS client that wants to use the Web Service;
- a communications protocol (Simple Object Access Protocol or SOAP) allowing the WS client to talk to the service.

There are a large number of "definitions" of what constitutes a Web Service, but the generally agreed-upon definition is an information service that exposes information via the W3C[20] standard Simple Object Access Protocol (SOAP). A client of a SOAP interface must know how to access those information services. That access can be described in the format of another W3C standard, Web Services Description Language (WSDL). The creators of the SOAP-based services publish WSDL files.

B.1.2 Web services security

Web services security should address the application server that maintains the service, the service description, the service repository, the client consuming the service, and the communication protocol. WS-Security Framework and a handful of specifications have been developed by various vendors and consortia. In addition, the ubiquitous web security solution, SSL can be used to provide some security for web services. Additional Web Services security details will be discussed throughout this clause.

B.1.3 Security standards

SOAP and WSDL are messaging and service definitions, respectively, that must be secured for each of the business services in which they are used. However, they do not currently specify the complete means for web services applications to provide data integrity, authentication of origin or confidentiality services. New requirements are anticipated and SOAP has an extension framework that allows for security elements and protocols to be added in a standardized fashion. This subclause gives an overview of some security standards related to web services.

The Security Assertion Markup Language (SAML) specifies an XML-based framework for the exchange of security information, expressed as assertions about an entity, which has an identity in some security domain. These assertions are conveyed in SAML request and response messages. The security information exchanged is in the form of SAML assertions that can convey details about prior authentication events, attributes of human or computer subjects, and authorization decisions that allowed or disallowed a subject access to resources. The evolution of SAML is being monitored closely by the industry, which hopes that it will become the standard means for conveying login information for SOAP based web services. SAML currently has a binding description for SOAP.

Web Services-Security (WS-Security) is a proposed set of SOAP extensions that allow web service transactions to have integrity and confidentiality. WS-Security intends to provide integrity and confidentiality through security token propagation, message integrity, and message confidentiality. Microsoft- and IBM-proposed WS-Security and responsibility has since transitioned to OASIS.

XML Encryption is a W3C specification for how to communicate XML information in a standard encrypted manner. XML Encryption allows the encryption and decryption of digital content including the XML document itself at the element but not attribute level. The specification also allows the secure transmission about key information for decryption of content by the XML document receiver.

XML Signature is a draft recommendation by a joint team from the IETF and W3C for how to represent digital signature information in XML documents. “XML Signatures provide integrity, message authentication and/or signer authentication services for data of any type, whether located within the XML which includes the signature or elsewhere.” XML Signature is a foundation standard that is referenced in other security standards including XML Encryption, SAML and WS-Security.

The Liberty Alliance Project is an industry consortium, lead by major businesses, intended to allow the interoperable open use of federated identity technologies. A federated identity allows a consumer to use a single recognized identity at multiple organizations. That consumer can use that same trusted identity information within the group of organizations and that customer does not have to present new identity, proprietary identity credentials.

XML Key Management (XKMS) is a W3C specification for a protocol to describe and register public keys that can be used in conjunction with the XML Signature and XML Encryption specifications. XKMS is on version 2 of the specification. Toolkits for key management are available from a variety of vendors.

B.2 Web Services standards

B.2.1 Overview

Standards for web services are rapidly evolving. There are three key areas of work to complement the basic SOAP transaction standards: Service Discovery, Security and Business Process. The key service discovery standard is UDDI that describes how a central repository for WSDL files, in a public or private setting, can allow users to find and invoke services. There are a large number of security standards being used to provide authenticity, encryption, signature and assertion services on a user and message-level. The Business Process standards efforts are linked to answering the question: “How do I tie services together to create a whole useful process rather than atomic functions?”.

B.2.2 Implementation

Implementing Web Services at least from a generic standpoint requires some consideration for the risk or threats the web service faces, and the security mitigation that can be applied against those threats. For this analysis, consider Figure B.1, and a relatively simple web service (WS1), which deals with clients in other positions throughout the organization's network. In this figure, four clients may request services from WS1. Note that these clients may also be web services in their own right, thus a web service providing functionality to a client, may itself act like a client to request services from another service in order to complete its own functionality. For example, a mortgage calculator web service might depend on a rate determination web service in order to provide a monthly payment calculation service.

The client S2 is collocated on a nearby network rail, perhaps within the same data centre as WS1. Client S3 is also on the companies' internal network, but may be much farther away, perhaps in a campus in another state, or another country. Client S4 is in an Internet-connected De-Militarized Zone (DMZ) and has some level of connections to both the Internet, and the company's internal network. Finally, it is possible that an internal service like WS1 could be available to clients on the Internet like S5.

B.2.3 Security

Security requirements for WS1 can generally be summarized into a few categories against generic threats. First, there is the confidentiality of the input data in the request for service, and the confidentiality of the output data going back to the client. Integrity of the confidential data is an implied, or assumed requirement as well. Second, there is the authentication and authorization of the client request, ensuring the client identity and preventing unauthorized clients from using the service. Finally, there are often some logging requirements to allow the reconstruction of transactions and trace activity. For some web services there may be data integrity requirements without confidentiality requirements.

While the security requirements for WS1 are straightforward, the considerations for building a solution can be complex. For example, secure authentication between a WS client and a WS server can be done with passwords, certificates or possibly other methods. While certificates offer a great deal of security, other functional considerations: performance, load balancing, fail-over, may make implementing them problematic. Passwords, while less secure in some circumstances, may be sufficient in other scenarios. For example, for a WS client talking to a WS running on the same hardware, passwords passing through machine memory may provide sufficient security. If the WS clients are located farther from the service, encrypted passwords may be required. Passwords could be encrypted at the application level using the WS-Security standards, or at the transport layer using SSL, or at the network layer using IPSEC (IP Security Protocol). The input and output data confidentiality requirements could likewise be met at the application layer, the transport layer or the network layer.

Note that the authentication requirements specifically address the client (which is also software) and not the end user. A web service may assume that the client authenticates the end user, **OR** a web service may authenticate the end user through the information in the web service request.

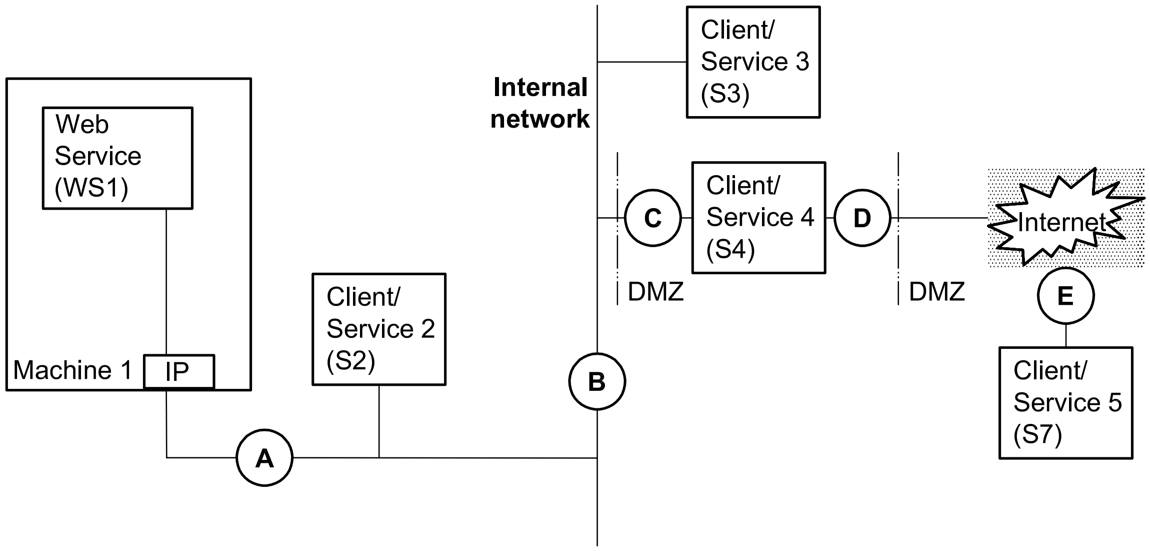

Figure B.1 — Web services general model

B.2.4 Threat analysis

Threats to WS1 include misusing the service, denial of service and unauthorized use of the service. In most cases misusing the service should be prevented by the service itself; WS1 should check the validity of all input and output, and create an error message when I/O falls outside expected bounds. Denial of service can be handled by creating multiple instantiations of the service on different machines, load balancing requests across instantiations, and other methods well known for ensuring the availability of IT services. Unauthorized use is prevented by securely authenticating the client requesting service. A specific web service may not need to authenticate client requests, or it may require very strong authentication of client requests, depending on the nature of the WS. A WS that moves money between accounts specified in the request should be very secure; otherwise, it invites someone creating rogue clients to request the money transfer service. A WS that calculates loan payments based on input loan values and mortgage rates needs no security since it is just a calculator.

B.2.5 Solutions

Solutions for WS1 security requirements may vary with the client requesting service. Consider if WS1 is only supporting clients like S2 that are located physically close to WS1. In these cases, at S2, the client and service are closely located, and the opportunity for unauthorized service requests could be minimized by routing tables, virtual LANs, internal firewalls between network segments or other techniques. Assuming WS1 and S2 are reasonably secured from outside communications, it may be reasonable to presume the confidentiality of data and password authentication simply based on their isolation from the rest of the world.

The complexity increases as we move farther away from WS1. Between client S3 and WS1, the service requests pass along a larger network opening the service requests to more opportunities for sniffing, and more points where an unauthorized request could be generated and injected. Thus, additional security is needed between WS1 and S3. As described previously, this might be certificate-based authentication, it might be IPSEC between the S3 hardware and the WS1 hardware.

For a client S4, the location in the organization’s DMZ means additional security concerns. De-Militarized Zones are used to provide breaks that separate the Internet connections from internal networks. By necessity, the systems in the DMZ are at greater risk, and therefore additional security may be needed. For S4, a combination of application layer and transport or network layer security may be the appropriate way to meet an organization’s security policies.

Finally, for web service requests from outside the organization at S5, incoming requests will likely require a complex solution. The authentication information might be secured at the application layer, and passed securely across the Internet, through the DMZ, and into WS1, so that WS1 can determine whether S5 is authorized to request services. Likewise, the input data for the request could be encrypted at the application layer, but the application layer data encryption might be terminated (or decrypted) in the DMZ, checked to ensure that the data falls within appropriate parameters, then re-encrypted for transport to WS1 where the information would again be decrypted. Similarly, the whole WS request might be additionally encrypted at the transport or network layer to an intermediate service (S4 perhaps) in the DMZ which would re-create the request to WS1, perhaps in a slightly different format, so that the WS1 interface is never exposed outside the organization.

A summary of WS Security concludes that there are many possible combinations of authentication mechanism, password encryption and data encryption that would meet various needs for authentication and confidentiality. There are also numerous locations throughout a typical organizational network where web services might be used. The threat and required countermeasures depend on the location of the WS client, and the WS server, as well as the network path between the two systems.

There are many other considerations as well. Performance between client and server is often critical. Fail over, backup, recovery, and similar contingency concerns may make some countermeasures more attractive. The WS development tools available from different companies provide different kinds of support for SSL and WS-Security standards; your tool may not support certificate-based SSL session re-use. Since the application server may have different capabilities with respect to the standard tools, results may vary.

Annex C
(informative)

Risk assessment illustrated

C.1 Risk assessment matrix form

VULNERABILITY: Personnel Identify the level of risk resulting from the threat of the following:	Risk of monetary loss			Risk of productivity loss			Reputation risk		
Unauthorized disclosure, modification or destruction of information	H	M	L	H	M	L	H	M	L
Inadvertent modification or destruction of information	H	M	L	H	M	L	H	M	L
No delivery or misdirected delivery of information	H	M	L	H	M	L	H	M	L
Denial or degradation of service	H	M	L	H	M	L	H	M	L

VULNERABILITY: Facilities and equipment Identify the level of risk resulting from the threat of the following:	Risk of monetary loss			Risk of productivity loss			Reputation risk		
Unauthorized disclosure, modification or destruction of information	H	M	L	H	M	L	H	M	L
Inadvertent modification or destruction of information	H	M	L	H	M	L	H	M	L
No delivery or misdirected delivery of information	H	M	L	H	M	L	H	M	L
Denial or degradation of service	H	M	L	H	M	L	H	M	L

VULNERABILITY: Applications Identify the level of risk resulting from the threat of the following:	Risk of monetary loss			Risk of productivity loss			Reputation risk		
Unauthorized disclosure, modification or destruction of information	H	M	L	H	M	L	H	M	L
Inadvertent modification or destruction of information	H	M	L	H	M	L	H	M	L
No delivery or misdirected delivery of information	H	M	L	H	M	L	H	M	L
Denial or degradation of service	H	M	L	H	M	L	H	M	L

VULNERABILITY: Communications Identify the level of risk resulting from the threat of the following:	Risk of monetary loss			Risk of productivity loss			Reputation risk		
Unauthorized disclosure, modification or destruction of information	H	M	L	H	M	L	H	M	L
Inadvertent modification or destruction of information	H	M	L	H	M	L	H	M	L
No delivery or misdirected delivery of information	H	M	L	H	M	L	H	M	L
Denial or degradation of service	H	M	L	H	M	L	H	M	L

VULNERABILITY: Environmental software and operating systems Identify the level of risk resulting from the threat of the following:	Risk of monetary Loss			Risk of productivity loss			Reputation risk		
Unauthorized disclosure, modification or destruction of information	H	M	L	H	M	L	H	M	L
Inadvertent modification or destruction of information	H	M	L	H	M	L	H	M	L
No delivery or misdirected delivery of information	H	M	L	H	M	L	H	M	L
Denial or degradation of service	H	M	L	H	M	L	H	M	L

C.2 Risk assessment matrix description

C.2.1 Areas of vulnerability

The risk assessment matrix is a one-page form designed to help assess a business function's risks. It is divided into five areas of vulnerability:

1) personnel;

2) facilities and equipment;

3) applications;

4) communications;

5) environmental software and operating systems.

C.2.2 Potential threats

Under each area of vulnerability on the risk matrix form, four potential threats to be evaluated are listed:

1) unauthorized disclosure, modification or destruction of information;

2) inadvertent modification or destruction of information;

3) no delivery or misdirected delivery of information;

4) denial or degradation of service.

C.2.3 Risk levels and categories

To the right of each threat are the risk levels within the three risk categories, monetary loss, loss of productivity and damage to reputation. The information security policy, programme and procedures are risk management tools that are used by the organization to assess and mitigate business risk. The risk of monetary loss in earnings or capital can arise from problems with services, information systems or product delivery. The level of this risk is a function of internal controls, information systems, employee integrity and operating processes.

The risk to earnings, capital and business reputation arising from negative public opinion can affect the financial institutions ability to establish new or maintain existing relationships or services. The risk can expose the organization to litigation, financial loss or further damage to its reputation. Further risk to earnings or capital from violations of, or non-conformance with, laws, rules, regulations, prescribed practices or ethical standards can expose the financial organization to fines, civil money penalties, payment of damages and the voiding of contracts.

The risk levels used in this guideline are

- high (H) - significant monetary loss, productivity loss or damage to reputation resulting from a threat occurring through the respective vulnerability;

- moderate (M) - nominal monetary loss, productivity loss or damage to reputation occurring;

- low (L) - a minimal chance of either monetary loss, productivity loss or damage to reputation or none at all.

C.2.4 Risk assessment instructions

The matrix is completed by assigning a risk level of high (H), moderate (M) or low (L) for the impact of each threat category on each of the five vulnerability categories as they pertain to the business function. To assess the risks to the enterprise:

- analyse what each of the potential threats on the matrix means to the business function being assessed;
- ask how and who would be at risk and what level of risk would result from each potential threat occurring through each vulnerability.

There are no absolutes in determining the level of risk. Establishing monetary ranges, staff hour ranges and worst-case events may be beneficial in making a determination. When in doubt in analysing potential threats, assume that the worst-case event will occur and choose the higher risk level.

When completing the risk assessment matrix, the key assumption must be that no safeguards exist.

As an example, the first threat on the matrix under facilities and equipment could be analysed as follows.

1) If an individual with normal access disclosed information about your facilities and equipment (i.e. a department employee discloses the combination of a department safe containing valuables or confidential information), could there be monetary loss, productivity loss, or damage to the reputation of the institution?

2) Would the level of loss and/or damage to reputation be high, moderate or low?

Threats that have been identified (i.e. a department employee discloses the combination of a department safe containing valuables or classified information) should be documented along with the rationale used. A “not applicable” (N/A) response for a given threat through a vulnerability or an entire category of vulnerability may be appropriate for some business functions. When this occurs, the rationale underlying the decision should be documented and all documentation should be retained in a file with the completed matrix.

Once threats have been identified, the choice is to either accept the risks, provided there is authority to do so, or to mitigate the risks. Risks can be mitigated by risk assignment (insurance), addressing the risks (reduction) by the application of security controls, or risk avoidance by removing the source of threats by changing a business aim.

C.3 Risk assessment table

For each risk category, enter the risk level, high (H), moderate (M), or low (L), related to each vulnerability. After rating each risk category, assign an overall risk to each vulnerability. Once this table is completed, select appropriate controls.

	Risk category			
Vulnerabilities	**Monetary loss**	**Productivity loss**	**Damage to reputation**	**OVERALL RISK**
Personnel				
Facilities and equipment				
Applications				
Communications				
Environmental software and operating systems				

C.4 Risk assessment table description

C.4.1 Overview

The risk assessment table is used to show the combined risk level for each vulnerability. The three risk categories are listed across the top and the five areas of vulnerability in the left hand column.

The risk assessment table is completed by assigning a combined risk level to each of the five areas of vulnerability. The combined risk level should be obtained from the four threats previously identified from the risk assessment matrix in D.2.2.

C.4.2 Risk table instructions

To combine the risk for each category, examine the risk levels circled for each vulnerability on the risk assessment matrix (see D.1). Take each risk category separately and determine what the combined risk level would be for the four threats (see D.2.2). Write the risk level on the risk assessment table.

To assign an overall risk, after rating each risk category, analyse the rationale behind the level of risk assigned to each vulnerability, and assign an overall risk of high (H), moderate (M), or low (L) to each vulnerability.

Consider that there are no absolute rules for determining the combined risk levels for each vulnerability. However, the following should be considered.

- The possibility or likelihood of the threat occurring. Threats with greater likelihood of occurring should have a more significant bearing on the level of risk assigned. Those threats with the least likelihood of occurring should have a less significant bearing.
- Threats that have the greatest relevance to the business function being assessed should be weighed more heavily when assigning the level of risk.
- Be conservative in assessing the levels of risk, and when in doubt, choose the higher risk.

As an example for the overall risk rating, the threat of no delivery or misdirected delivery of information may be given greater weight in the selection of an overall risk level because no delivery may be judged to be more significant to the business function being analysed than the unauthorized disclosure of that information.

C.4.3 Selection of controls

The selection of security safeguards provides an institution direct control over the risk it accepts. An institution needs to assess how planned and existing safeguards reduce the risk identified in the risk analysis, identify additional safeguards available or able to be developed, develop an IT security architecture and determine constraints of various types (see 8.3 to 8.7). Appropriate and justified safeguards should then be selected to reduce the assessed risks to an acceptable level). Additional details on the selection of safeguards can be found in ISO/IEC TR 13335.

C.4.4 Ranking impact and likelihood

A scale of 1-9 is used for both likelihood and impact. This subclause defines what these mean in practice, by assigning a common assessment to the likelihood scale and defining impact under each of the six main categories of the Enterprise Risk Framework. Although this does give a “quantified” feel, the values should be treated as guidance on order of magnitude and not as absolutes.

The following scoring range for likelihood is adopted:

1) **negligible** - once every 1 000 years or less

2) **extremely unlikely** - once every 200 years

3) **very unlikely** - once every 50 years

4) **unlikely** - once every 20 years

5) **feasible** - once every 5 years

6) **probable** - annually

7) **very probable** - quarterly

8) **expected** - monthly

9) **confidently expected** - weekly

Very approximately each one is four times more likely than the previous one.

The following is the scale of impact against each of the six major headings in the framework. Not every box is filled in, but it does give a range. Some risk assessments may need different words but the levels used should be broadly similar.

Table D.1 — Risk assessment

Rating		Description	Reputation	Operational	Security	Legal/ regulatory	Financial	Strategic
LOW	1	**negligible**			Local password to non-sensitive data revealed but not used		< $100	
	2	**very minor**	Attacks on banking system on local radio or in local press	Low-grade operational problems with no customer impact.	Local password to sensitive data revealed but not used	Regulatory responses from clearer not met within timescale set by law.	~ $1 000	
	3	**minor**	“Routine” sniping in the national press or posted on Internet about banking system, e.g. reader’s letter	Temporary loss of service (~ 1 h) to one system member; problems with limited customer impact.	Attempted access to operational systems; minor operational information leaked or compromised	Rectifiable potential non-compliance identified	~ $5 000	Policies or standards not maintained
MEDIUM	4	**noticeable**	National press or radio attention e.g. bad review of DD scheme	Operational problems with clearing-wide impact	Abuse of legitimate access privilege	Inability to provide data demanded by law, e.g. by Sarbanes-Oxley Act	~ $20k	
	5	**significant**	Serious and critical article in press or item on radio or television documentary liable to viewed as being from a credible source	Temporary loss of service to multiple members or prolonged loss of service (up to whole day) to 1 system member; significant customer impact	Logical or physical penetration into one or more system members’ operational systems; e.g. malicious virus with some damage done.	Regulatory intervention, complaint not upheld.	~ $100k	Policies or standards do not exist
	6	**very significant**	Public criticism from regulator or industry body.	System member unable to operate clearing	Successful low- to medium- value fraud	Police or regulatory investigation launched; regulatory intervention, complaint upheld	~ $1m	

Table 1 (*continued*)

Rating		Description	Reputation	Operational	Security	Legal/ regulatory	Financial	Strategic
HIGH	7	**major**	Lead story in multiple broadsheets and/or television main news	Loss of service to multiple system members at a critical period of the day (3 pm, Friday afternoon)	Successful high-value fraud; operational data or control systems compromised	Prosecution brought against clearing house (unsuccessful)	~ $10m	Management control compromised
	8	**very major**	Government intervention or comparable political repercussions	Loss of complete clearing for a whole working day	Clearing system hacked and seriously compromised	Prosecution brought against a clearing house (successful)	~ $100m	
	9	**catastrophic**	Major press and television coverage, complete loss of confidence by public and system members	Total loss of service for several days /weeks	Clearing house or its cryptographic systems totally compromised; high-value fraud with no known fix.	Systematic and deliberate flouting of the law at senior management level	~ $1 bn	Future existence of a clearing house in doubt; payments industry compromised

Note that the assessment is on **net** and not **gross** risk. In other words, consideration should be given to their effect **in the presence of current controls**. Normally the presence of preventive controls will reduce the likelihood of an event occurring but not affect its impact; controls addressed specifically at mitigation of impact will not usually affect likelihood.

Exposure or "importance"

Once "scored" for impact and likelihood the following model is used as a means of defining the exposure. Five levels are included; in practice, anything scoring level 1 is not worth further analysis, and anything scoring level 5 should be dealt with immediately instead of continuing with the risk assessment! So in effect we end up with a three-point scale.

Key to shading:

Exposure/Importance

Critical - 5	*5*
Major - 4	*4*
Significant - 3	*3*
Minor - 2	*2*
Negligible - 1	*1*

Impact	9	3	3	4	4	4	5	5	5	5
	8	3	3	3	4	4	4	5	5	5
	7	2	3	3	3	4	4	4	5	5
	6	2	2	3	3	3	4	4	4	5
	5	2	2	2	3	3	3	4	4	4
	4	1	2	2	2	3	3	3	4	4
	3	1	1	2	2	2	3	3	3	4
	2	1	1	1	2	2	2	3	3	3
	1	1	1	1	1	2	2	2	3	3
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
		Likelihood								

Clearly the greater the importance the more effort should be put into both analysing and controlling the risk. It doesn't pay at this stage to follow the "scoring" system slavishly, what should have been achieved is identifying key risk issues for management to deal with – in whatever order they see fit, based on all the available information, including but by no means limited to the risk exposure. Factors to take into account at this stage will be all the usual factors governing the management of a business: resource availability, budget, company strategy and goals at the time, political influences and so on.

Follow-up actions

In order to deal with risks that have been identified, there are typically four courses of action from which to choose. They are:

— **Avoid** – As the name suggests, this simply means removing the source of a threat or changing a business aim so a risk no longer applies. Although it sounds the ideal way to deal with a risk, it tends to be applicable only in a small number of instances. "No risk, no business"! For example you might avoid the risk of being knocked down by a car by never leaving your house, but you wouldn't have much of a life. As an example closer to business operations, we might avoid the effects of third party failure by not using third parties – in which case we probably wouldn't have much of a business left to operate! However, where a risk can genuinely be avoided it is often a cheap – and lasting solution.

— **Address** – Addressing risks is what we tend to do most often, and is in a sense implicit in the *modus operandi* we have accepted which says, "develop an action plan". It simply means performing actions which will reduce the likelihood of a risk materializing or which will contain the effects of an event and thereby reduce the impact. Examples are many and largely obvious – address the risk of data loss via the use of a backup regime, contain the effects of compromise of a cryptographic key by restricting its lifetime and so on.

— **Assign** – Assigning a risk means loading the majority of the impact on to a third party. The classic means of achieving this is via insurance. Clearly assignment is rarely achieved without some ongoing cost! For example we might assign our liability for giving poor advice via a professional indemnity policy – at a price. Risks can sometimes be assigned to third parties via contractual arrangement (as liability), though their ability to deal with the consequences may itself be a risk!

— **Accept** – The final option is simply to accept a risk; be aware that the risk may happen but, having evaluated the cost and desirability of the other three options, decide that the magnitude of the risk is outweighed by the potential benefits of running it. For example, we may decide to accept the risk of enforced physical access to our premises by criminals wielding firearms because the cost of physical security measures is very high and their implementation would adversely affect the welcome we give to members.

It is of course possible to use mixed approaches to particular risks – this is not an exact science – so to pursue the example of criminal armed access, while we may have accepted a level of risk we may have addressed lesser threats (such as people casually walking in off the street) by using unarmed security guards, chosen to contain its effects by adding PIN-pad access to key areas or by narrowing down the functions which can be performed (under threat) on key systems, and perhaps assigned part of the risk by taking out life insurance coverage on our employees.

Residual risks

Determine what actions and monitoring activities to take to manage residual risks and assign responsibility for all actions.

Annex D
(informative)

Technological controls

D.1 Hardware

D.1.1 End system controls

Most organizations today use some combination of desktop PCs and laptop PCs as the primary user-facing systems. These end systems use a variety of operating systems, although the vast majority are from a single vendor. Additionally, these machines are being augmented, or in some cases replaced, by the smaller Personal Digital Assistant (PDA). Cell phones too are becoming more capable, and may sometimes be used as end systems. Knowledge workers for documents, presentations, spreadsheets and similar information often use PC-based solutions. Other enterprise users are frequently using web-based technology for applications – thus granting access for use to PDAs and cell phones.

With any end system, the first base to cover is the security settings within the operating system. Unused and unnecessary sub-systems, such as database and operating system functions, should be disabled and removed. Other functions should be limited to the minimum necessary for the user to operate properly. In addition, the enterprise must have some mechanism for patching systems and distributing updates, as they are available from vendors for both the operating system, and any applications running on the end systems. For example, there have been several issues identified with Microsoft’s macro capability found throughout the office suite.

Beyond the operating system, enterprises should consider the roles of these end systems, and whether additional features like anti-virus, intrusion detection, intrusion prevention, firewalls and Virtual Private Networks are necessary for the enterprise users. In many cases the organization’s perimeter systems (as specified in 11.5) will provide features like anti-virus, firewalls, and intrusion detection and prevention. However, with mobile systems, and the rise of business partnerships and outsourcing, duplicating these features on mobile systems, and potentially PDAs and desktops makes sense for a traditional layered defence. For example, a mobile user PC connected to a broadband connection at home and using a VPN into the enterprise becomes a conduit for attack, and a temporary perimeter device – requiring the same security as other perimeter devices.

D.1.2 Server systems controls

Like the end systems, server systems need to have both internal, operating system level controls, and external controls applied. Servers often require functionality and subsystems not required by end systems. Since the server may run a database, a web server, an FTP service, and/or many other functions, these servers have a larger potential window of vulnerability. These services require granting access to other devices, which may not always be trustworthy. In addition, like the end systems, provisions must be made for testing, updating, and managing the systems as new release and patches are released. An appropriate process would include testing the new patch in a non-production environment before patching production systems.

On the internal control’s side, the server must always take advantage of operating system controls that limit the functions and access to critical parts of the server. This means, for example, that a server used to support web pages doesn’t necessarily need to enable the FTP service, or open ports for generic database queries. Likewise and FTP server shouldn’t be open to HTTP ports and protocols.

Beyond the operating system, some consideration needs to be made for anti-virus, intrusion detection and firewalls in and around the server. This may take the shape of arranging the server within a secured zone behind a firewall and using a network device-based intrusion detection system, or it may use all three-security services on the server host itself. A variety of organization, network and security concerns drive the assessment and determination of what controls are appropriate for what server systems.

D.1.3 Mainframe system controls

Mainframe systems are built by only a handful of manufacturers for heavy load processing. As a result, mainframes have tended to be regarded as both more secure, and more powerful than other IT processing systems. Nonetheless, mainframe systems need to be managed using the same security principles as other systems. The core operating system needs to be secured or “hardened” and additional measures beyond the OS should be considered. Typically, a mainframe system will house an organization’s most valuable information and business rules, so they are placed at the core of layered network security architecture. Each user is assigned an appropriate ID with limited functionality; there are few personnel with administrative control of the mainframe. As with other systems, separation of duties should be carefully considered as one part of the mainframe security controls.

D.1.4 Other hardware system controls

Other hardware devices and systems will have similar concerns, and these should be evaluated before production deployment within an organization. These devices could be dedicated encryption systems, the new hardware types favoured by many firewall and intrusion detection system vendors, or network hardware such as routers and switches. In all cases, the product should be evaluated to understand the underlying operating system, and that operating system should be hardened to prevent easy attack. In addition, appropriate placement of these devices with respect to internal network connections, anti-virus scans, firewalls and intrusion detection is important.

D.2 Software

D.2.1 Web servers

Web Servers are a very common and frequently used software application intended primarily to dispense web pages to users. Applications can range from very simple – providing only canned pages of information, to the very complex – multi-paged form documents supporting scripts, active software computer instructions and more. Organizations have to determine what degree of complexity they can live with, and the appropriate connections between the Internet, the web server(s) and the internal data. Typically, financial institutions insist on a three-tier architecture with firewalls providing a boundary between the Internet and the web server, and between the web server and internal data. Multi-tier architectures, which separate additional layers of application or business logic, are frequently used to provide tighter control of data flows.

Many vendors distribute web server software, and each version has its own set of concerns, settings, and updates that must be managed. Often the vendor or a third party will have distributed suggested security settings on the Internet. These should be considered and evaluated against the specific policies, practices and needs of a specific organization.

D.2.2 Application servers and web services

Specialized web servers have evolved to act as application servers – servers that run functional pieces of an application as reusable components that can be called by many applications. For example, a function to move money between accounts might run as a component on an application server and be used both by applications that provide customers with an online banking experience, and by call centre operators acting on behalf of a customer who calls for banking services. These component application pieces have been given interfaces that allow the components to be called over the web as services. These web services act much like older remote procedure calls, but with a web flavour enhanced by the use of Extensible Markup Language (XML), which can be used on any device, even those that do not support traditional web browsers. Many vendors provide application servers that support web services. More information on web services and web services security can be found in Appendix B.

As with web servers, many vendors distribute application server and web services software, and each version has its own set of concerns, settings and updates that must be managed. Often the vendor or a third party will have distributed suggested security settings for use on the Internet. These should be considered and evaluated against the specific policies, practices and needs of a specific organization.

D.2.3 Software application development process

Many organizations customize software, or create specific applications using the development tools provided by large and small vendors. These software development tools rarely guide one to incorporate information security. Therefore, it is critical that organizations plan to incorporate information security into their software development process. Security practitioners maintain that the most effective information security results when security requirements are incorporated into the software during development rather than adding security software modules to a completed system.

Before software development begins, the developers must be informed of the Corporate Information Security Policy, how it relates to the development and understand the threats against the organization. They should be informed of the information security programme and where they can obtain guidance as the development continues. A strong foundation about the organization's Policy, its practices, and continuing dialog with the information security officials will ensure that the software provides efficient and effective information security.

Two aspects should be considered in a software application development that incorporates security requirements. The first is that the software development process itself follows well-structured and well-documented steps. The goal is to produce software that only meets its requirements and does not allow unwanted operations to be performed either accidentally or maliciously. To reach this goal, an organization should meet and follow the guidance provided by ISO/IEC 21827[13]. Additional information on the Capability Maturity Model may be obtained at http://www.sei.cmu.edu/cmmi/. Software applications with critical information security requirements should be developed using processes defined by Level 3 or higher in the maturity model, which requires that the software process for both management and engineering activities is documented, standardized and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.

The second aspect is to insure that the appropriate security requirements are incorporated into the software application. The Corporate Information Security Policy, the Security Architecture and the risk assessment will generate these requirements. All requirements will need to be documented, incorporated and tested during the development process. The security requirements should also specify what amount of evidence would be required to show that the requirements fully satisfy the security policy and any controlling legislation.

Because knowledge of how the security software operates may compromise the application, documentation such as test results and operator’s instructions should be controlled so that it is not inadvertently made available to unauthorized persons. A complete description of the major development issues can be found in the freely available publication, NIST SP800-64 “Security Considerations in the System Development Life Cycle” at http://csrc.nist.gov/publications/nistpubs/index.html.

D.2.4 Security software acquisition

An organization may contract with another to develop security software or applications with security considerations. The issues identified in E.2.3 are relevant to this acquisition but there are two differences in the development process. The first difference is that the development process is constrained by the written contract. Changes in the requirements will change the contract and probably result in cost and schedule growth. The second difference is that a contractor will not usually be aware of an organization's structure and culture. Assumptions and misunderstandings about an organization will likewise contribute to contract changes. Thus, it becomes incumbent on the purchasing organization to be very rigorous in specifying the requirements, in selecting the developer and in conducting acceptance testing.

Organizations may also purchase off-the-shelf security software to satisfy some requirements of the security architecture. There must be a clear understanding of the capabilities and limitations of the software. This knowledge is necessary so that the residual requirements can be identified that will be satisfied by other elements of the architecture.

New software needs to be compatible with existing software so that it does not invalidate or compromise existing security procedures. A commonly used benchmark for security software is the Common Criteria (CC) which is a set of security requirements and specifications defined in ISO/IEC 15408[7]. The CC describes both functional and assurance requirements; it is useful for vetting requirements and for comparing products from multiple sources.

The Common Criteria is freely available for unrestricted use at http://niap.nist.gov/cc-scheme/index.html.

D.3 Networks

D.3.1 Wide area networks

D.3.1.1 Overview

Wide area network (WAN) systems cover broad geographical areas; using telecommunications protocols intended to go well beyond a local campus of buildings or an area within a building. The Internet is composed of many somewhat smaller WANs, each with its own set of routers, switches and gateways to other WANs. The so-called Plain Old Telephone System (POTS) is another Wide Area Network. In all cases, these networks allow data to flow everywhere. In addition, they provide multiple access points where the information is vulnerable.

Within an organization, especially larger organizations with geographic separation, the organization’s network will include connections to a broad WAN like the Internet, several Local Area Networks on each campus, or within a building, and some dedicated WAN connections dedicated to the organization. Typically these dedicated WAN connections are treated as being internal to the organization, and lack the border controls used to connect to other businesses or external WANs like the Internet. Organizations must consider, as part of regular risk assessments, the possibility that dedicated WAN connections can be monitored, and that high-value information should be encrypted. In addition, access granted to users outside the organization network must be closely controlled.

D.3.1.2 Wired WAN systems

Most WAN systems are wired using fibre or copper connecting switch and router points. As noted above, encryption is rarely an option for wired WAN systems except on the most crucial network links. More frequently, WAN cables are protected physically, within walls, cupboards and crawl spaces where few people have access. These forms of physical protection, and perhaps a periodic audit of the connections, are all the security associated with most WANs. Where a company has purchased dedicated lines, some testing may be involved, but there are few alternatives to contractual-based trust in the telecommunications provider. Sometimes, even a supposedly wired WAN connection actually includes microwave, laser, or RF links (including satellite), which introduce additional opportunities for monitoring the information flowing on the WAN.

D.3.1.3 Wireless WAN systems

As cell phone networks continue to proliferate, new data transmission systems are coming along. While most are still fairly slow (around 20 kbs), there is the promise of future megabit transmission capabilities through cell phone based network protocols. Because these systems leverage the mobile nature of the cell network, but support high bandwidth activities, they are often referred to as Wireless WAN systems. These systems also have limited opportunities to provide encryption and similar security capabilities. However, the increasing sensitivity of many organizational customers to WAN security issues, particularly for cell phones, had resulted in more “designed-in” security including encrypted data at least as far as the telephone - see 9.3.2.2.

D.3.2 Local area network

D.3.2.1 General

Within a campus area, or a floor in a building, or even at a home office, Local Area Network (LAN) systems are proliferating as well. These networks often use the same protocols and routing systems as their larger cousins the Wide Area Network, but typically provide a security veneer by using some type of gateway between the LAN and the WAN. The gateway may be a simple aggregator of traffic bandwidth and routing, or it may include firewalls, anti-virus scanners, intrusion detection and other border security controls (as specified in 11.5). In all cases maintaining an understanding of the network connections and the control of the gateway devices is a critical aspect of securing a LAN. Other specifics are discussed below.

D.3.2.2 Wired LAN systems

Wired LANs typically are typically secured physically by managing the routers, switches and cable connections. In some cases the distribution of IP addresses and other management functions can limit the ability to plug new devices into the LAN, although managing the network this tightly can be very difficult and frustrating for the users within an enterprise.

D.3.2.3 Wireless LAN systems

D.3.2.3.1 General

Wireless LAN systems, particularly Wi-Fi or 802.11x systems typically provide a short range [< 300 ft (~100 m)] RF signal that can be used for network connections and data distribution. There are numerous security issues with wireless LAN systems, the most obvious being the intentional broadcast of potentially sensitive company information. More sophisticated attacks, taking over a connection, redirecting traffic and trust are also possible. After several years of partial secure solutions (Wired Equivalent Privacy) open, interoperable and secure standards for 802.11x systems are becoming available. Modelled on a Cisco proprietary security standard called Lightweight Extensible Agent Platform (LEAP), the open Protected Extensible Authentication Protocol or PEAP, is becoming available in various wireless systems. The use of PEAP or similar security mechanisms should be carefully considered in building out any wireless LAN system within an enterprise.

When building out a wireless environment, there are two major architectural alternatives. One alternative is to use PEAP and ensure that only authorized systems and users have wireless access to the network, and build the LAN inside the enterprise network, treating all wireless users as trusted members of the company. The other alternative is to connect the wireless LAN external to the company network, and leverage a Virtual Private Network, SSL Web sites or similar security overlays to protect access to company resources. These are explained in more detail in D.3.2.3.2 to D.3.2.3.4.

D.3.2.3.2 Wireless LAN inside the enterprise boundary

Leveraging PEAP companies can ensure that only authorized users can access the wireless LAN and use the company resources. This type of solution is still subject to denial-of-service attacks, but if the wireless service is managed and maintained largely inside a building or campus area controlled by the company, this type of solution is very reasonable. It allows for mobile users within the organization, a situation typified by those attending many meetings in different conference rooms, or executives who travel frequently between major company sites. Further, this type of solution limits access to network bandwidth, Internet connections, and other company resources only to those authorized users. There are too many details for securely implementing PEAP in this internal architecture model to discuss in depth here. Many resources from vendors and the Internet are available.

D.3.2.3.3 Wireless LAN outside the enterprise boundary

An alternative to locking down the wireless network to authorized users is providing a wireless connection with Internet connectivity, external to the enterprise networks. In this case, the wireless users might be anyone walking by, or anyone subscribing to a service. They would not have immediate access to the company resources. Instead, users needing access to company resources would use a VPN (see 11.2.1) to connect securely into the company network.

There are network management disadvantages to this solution; however there may be user advantages. While financial institutions generally would not want outside users to use the wireless LAN resources, a university might want to make a wireless LAN available to visitors at the university campus. Alternatively, a property management company might want to make a wireless LAN available to all the renters within a building complex.

D.3.2.3.4 Other wireless LAN considerations

Much as if a broadband connection at home makes an end system a boundary device between the Internet and the company network and resources, a wireless LAN also transforms end systems (like laptops) into boundary devices. Therefore end systems using wireless connections should be considered likely candidates for anti-virus, firewalls and intrusion detection software running locally on the end system.

Users of mobile laptops with wireless LAN connections will drive additional requirements. Whether the company wireless LAN is internal or external to the enterprise network, these mobile users will need access to the company resources through a VPN (either IPSEC or SSL) to access company resources because of the increasing popularity of wireless “hotspots.” These hotspots are locations at airports, parks, universities, coffee shops, restaurants, hotels and other locations frequented by business travellers. A mobile executive with wireless access will want Internet connectivity whenever, and wherever, they can find it. The VPN provides the mobile user with access to company resources while on the go.

A major issue in managing these mobile users at “hotspots” is the trust for common Internet IP addresses. Many companies use the 10. and 168. IP address ranges internally for file and print services shared across the company. These non-routable addresses are re-used frequently, so that a home network, coffee shop network, and the networks at multiple companies may all use the same address (for example 10.1.1.100) with each network having a different device and resource at that address. Because VPN profiles often make encryption and routing decisions based on address, these “10.” and “168.” addresses may be trusted inappropriately by the mobile laptop creating new potential risks. Like the VPN, firewalls and IDS systems also make connection and trust decisions based on addresses. Therefore, while it may be appropriate for a mobile laptop to trust the printer at work, and even the printer at home, trusting a file server in a coffee shop should be an entirely different consideration. Policies, software, and other countermeasures to these concerns should be evaluated and applied based on overall company policy.

D.3.3 Other telecommunications considerations

There are always other considerations with telecommunications. Although it is really just beginning to take off, the continuing convergence of voice and data on the same networks is opening a new range of telecommunications concerns and countermeasures. Recently, voice firewalls, trunked VPNs and multimedia intrusion detection systems (IDS) solutions that address the data/voice convergence issues have begun to show up as products and be discussed seriously by major vendors. These solutions are also being implemented by companies, often paid for with cost savings from better management of the voice telecommunications within the company.

Bibliography

[1] ITU-T Recommendation X.509 (2001) | ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

[2] ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[3] ISO/IEC 10181-1, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*

[4] ISO/IEC 13335 (All parts), *Information technology — Security techniques — Management of information and communications technology security*

[5] ISO 13491-1, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

[6] ISO/IEC 13888 (All parts), *Information Technology — Security Techniques — Non-Repudiation*

[7] ISO/IEC 15408 (All parts), *Information Technology — Security Techniques — Evaluation criteria for IT security*

[8] ISO/IEC 18043, *Information technology — Deployment and operation of Intrusion Detection Systems*

[9] ISO/IEC TR 18044, *Information Technology — Security techniques — Information security incident management*

[10] ISO TR 19038, *Banking and related financial services — Triple DEA — Modes of operation — Implementation guidelines*

[11] ISO 19092 (All parts), *Financial Services — Biometrics*

[12] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

[13] ISO/IEC 21827, *Information Technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)*

[14] ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation*

[15] ANSI X9.79-2001, *Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework*

[16] ANSI X9.84-2003, *Biometric Information Management and Security for the Financial Services Industry*

[17] FIPS 140-2, *Security Requirements for Cryptographic Modules*, National Institute for Standards and Technology (USA.). http://csrc.nist.gov/cryptval/140-2.htm

[18] FIPS 197, *Advanced Encryption Standard (AES)*, National Institute for Standards and Technology (USA.). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[19] *Security Of Electronic Money*, published by the Bank of International Settlement, Basle, August 1996

[20] W3C Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation, Copyright © [6 October 2000] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2000/REC-xml-20001006/

[21] *Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing*

[22] Gramm-Leach-Bliley (GLB) Act of 1999, http://www.senate.gov/~banking/conf/

ICS 03.060

Price based on 72 pages