INTERNATIONAL TELECOMMUNICATION UNION

ITU-T X.1051

(07/2004)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

Telecommunication security

Information security management system – Requirements for telecommunications (ISMS-T)

ITU-T Recommendation X.1051

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation X.1051

Information security management system – Requirements for telecommunications (ISMS-T)

Summary

For telecommunications organizations, information and the supporting processes, telecommunications facilities, networks and lines are important business assets. In order for telecommunications organizations to appropriately manage these business assets and to correctly and successfully continue their business activities, information security management is extremely necessary. This Recommendation provides the requirements on information security management for telecommunications organizations.

This Recommendation specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the telecommunication's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual telecommunications or parts thereof.

Source

ITU-T Recommendation X.1051 was approved on 29 July 2004 by ITU-T Study Group 17 (2001-2004) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation X.1051

Information security management system – Requirements for telecommunications (ISMS-T)

1 Scope

This Recommendation specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the telecommunication's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual telecommunications or parts thereof.

The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to the customers and business partners of telecommunications organizations as well as to other interested telecommunications parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a recommendation.

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

– ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

– ISO 9001:2000, *Quality management systems – Requirements*.

– ISO 14001:1996, *Environmental management systems – Specification with guidance for use*.

– ISO/IEC 17799:2000, *Information technology – Code of practice for information security management*.

– ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*.

– BS 7799-2:2002, *Information Security Management Systems – Specification with Guidance for use*.

3 Definitions

This Recommendation defines the following terms:

3.1 **availability**: Ensuring that authorized users have access to information and associated assets when required. [ISO/IEC 17799:2000]

3.2 **confidentiality**: Ensuring that information is accessible only to those authorized to have access. [ISO/IEC 17799:2000]

3.3 information security: Security preservation of confidentiality, integrity and availability of information.

3.4 Information Security Management System (ISMS): That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

3.5 integrity: Safeguarding the accuracy and completeness of information and processing methods. [ISO/IEC 17799:2000]

3.6 risk acceptance: Decision to accept a risk. [ISO/IEC Guide 73]

3.7 risk analysis: Systematic use of information to identify sources and to estimate the risk. [ISO/IEC Guide 73]

3.8 risk assessment: Overall process of risk analysis and risk evaluation. [ISO/IEC Guide 73]

3.9 risk evaluation: Process of comparing the estimated risk against given risk criteria to determine the significance of risk. [ISO/IEC Guide 73]

3.10 risk management: Coordinated activities to direct and control an organization with regard to risk. [ISO/IEC Guide 73]

3.11 risk treatment: Treatment process of selection and implementation of measures to modify risk. [ISO/IEC Guide 73]

3.12 statement of applicability: Document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes.

4 Abbreviations

This Recommendation uses the following abbreviation:

ISMS Information Security Management System

5 Overview

5.1 General

For telecommunications organizations, information and the supporting processes, telecommunications facilities, networks and lines are important business assets. In order for telecommunications organizations to appropriately manage these business assets and to correctly and successfully continue their business activities, information security management is extremely necessary. This Recommendation provides the requirements of information security management for the telecommunications organizations.

This Recommendation has been prepared for telecommunication managers and their staff to provide a model for setting up and managing an effective Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for a telecommunications organization. The design and implementation of an organization's ISMS is influenced by business needs and objectives, resulting security requirements, the processes employed and the size and structure of the telecommunications organization. These and their supporting systems are expected to change over time. It is expected that simple situations require simple ISMS solutions.

This Recommendation can be used by internal and external parties including certification bodies, to assess a telecommunication's ability to meet its own requirements, as well as any customer or regulatory demands.

5.2 Process approach

This Recommendation promotes the adoption of a process approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of an organization's ISMS.

A telecommunications organization must identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the following process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

A process approach encourages its users to emphasize the importance of:

a) understanding business information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls in the context of managing an organization's overall business risk;

c) monitoring and reviewing the performance and effectiveness of the ISMS;

d) continual improvement based on objective measurement.

The model, known as the "Plan-Do-Check-Act" (PDCA) model, can be applied to all ISMS processes, as adopted in this Recommendation. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the telecommunications organizations and interested parties associated with the telecommunication sector and through the necessary actions and processes produces information security outcomes (i.e., managed information security) that meet those requirements and expectations.

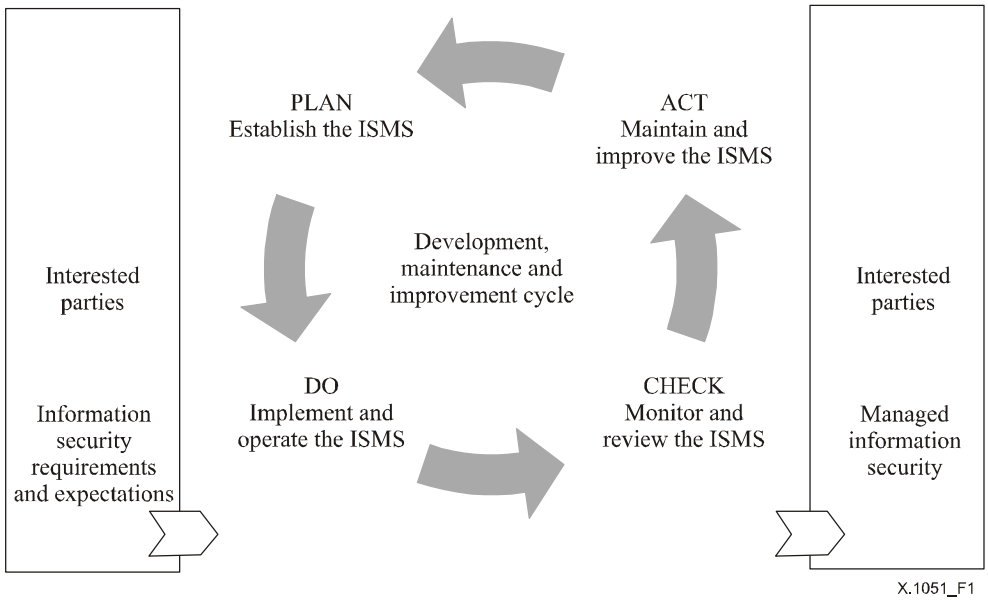

Figure 1/X.1051 – PDCA model applied to ISMS processes

5.2.1 Plan (establish the ISMS)

Establish security policy, objectives, targets, processes and procedures relevant to managing risks and improving information security to deliver results in accordance with an organization's overall policies and objectives.

5.2.2 Do (implement and operate the ISMS)

Implement and operate the security policy, controls, processes and procedures.

5.2.3 Check (monitor and review the ISMS)

Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.

5.2.4 Act (maintain and improve the ISMS)

Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS.

5.3 Compatibility with other management system standards

This Recommendation is based on the standard BS 7799-2:2002. The Annex of BS 7799-2:2002 contains a set of ISMS control objectives and control compliance statements. These are based on ISO/IEC 17799:2000.

This Recommendation is also aligned with ISO 9001:2000 and ISO 14001:1996 in order to support consistent and integrated implementation and operation with related management Recommendations. It is also aligned with ITU-T Recs X.800 and X.805.

6 Information security management system specification

6.1 General

The organization shall develop, implement, maintain and continually improve a documented ISMS within the context of the organization's overall business activities and risk.

The process approach described in 5.2 is further detailed below. This Recommendation provides details of all the processes that need to be considered in each of the Plan, Do, Check and Act phases.

NOTE – The ISMS processes defined in clauses 6 to 9 below are directly derived and aligned with the processes given in BS 7799-2:2002. A more detailed description of these processes is provided in BS 7799-2:2002 clauses 4 to 7.

6.2 Information security management system processes

6.2.1 Establish the ISMS

The organization shall:

a) define the scope of the ISMS;

b) define an ISMS policy;

c) define a systematic approach to risk assessment;

d) identify the risks;

e) assess the risks;

f) identify and evaluate options for the treatment of risks;

g) select control objectives and controls for the treatment of risks (from Annex A);

h) prepare a Statement of Applicability;

i) obtain management approval of the proposed residual risks and authorization to implement and operate the ISMS.

6.2.2 Implement and operate the ISMS

The organization shall:

a) produce and implement a risk treatment plan;

b) implement controls;

c) implement training and awareness;

d) manage operations;

e) manage resources;

f) implement procedures.

6.2.3 Monitor and review the ISMS

The organization shall:

a) execute monitoring procedures;

b) undertake regular reviews;

c) review the level of residual risk;

d) conduct internal ISMS audits;

e) undertake a management review;

f) record actions and events that could impact the ISMS performance and effectiveness.

6.2.4 Maintain and improve the ISMS

The organization shall:

a) implement any identified ISMS improvements;

b) undertake any identified corrective and preventive actions;

c) communicate the results to all interested parties;

d) check that the improvements satisfy the intended objectives and purpose.

6.3 Documentation system

The organization shall have a documentation system in place for the ISMS. Documents in this system shall be appropriately protected and controlled. This system shall also include any records that are produced or maintained to provide evidence of effective operation of the ISMS. These documentation requirements are further specified in BS 7799-2:2002 and ISO 9001:2000.

7 Management responsibility

7.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of its ISMS.

7.2 Resource management

7.2.1 Provision of resources

The organization shall determine and provide the resources needed to:

a) establish, implement, operate and maintain an ISMS;

b) ensure that information security policy procedures support the business requirements;

c) identify and address legal and regulatory requirements and contractual obligations;

d) maintain adequate security by correct application of all implemented controls;

e) carry out reviews when necessary and to react appropriately to the results of these reviews;

f) where required, improve the effectiveness of the ISMS.

7.2.2 Training, awareness and competency

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks. The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

8 Management reviews

8.1 General

Management shall review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. These requirements are further detailed in BS 7799-2:2002.

8.2 Review input

The input to a management review shall include information on:

a) results of ISMS audits and reviews;

b) feedback from interested parties;

c) techniques, products or procedures to improve the ISMS performance and effectiveness;

d) status of preventive and corrective actions;

e) vulnerabilities or threats not adequately addressed in the previous risk assessment;

f) follow-up actions from previous reviews;

g) any changes that could affect the ISMS;

h) recommendations for improvement.

8.3 Review output

The output to a management review shall include any decisions and actions related to the following:

a) improvement of the effectiveness of the ISMS;

b) modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS;

c) resources needs.

8.4 Internal ISMS audits

The organization shall conduct internal ISMS audits at planned intervals to determine the control objectives, controls, processes and procedures of its ISMS.

9 ISMS improvement

9.1 Continual improvement

The organization shall continually improve the effectiveness of the ISMS.

9.2 Corrective action

The organization shall take action to eliminate the cause of non-conformities with the implementation and operation of the ISMS in order to prevent recurrence.

9.3 Preventive action

The organization shall determine action to guard against future non-conformities in order to prevent their occurrence.

Annex A

A set of controls customized to telecommunication requirements

A.1 Introduction

The control objectives and controls listed in this annex are directly derived from those listed in ISO/IEC 17799 and BS 7799-2:2002 (Annex A). They have been customized to telecommunication requirements. The list of controls in this annex (given below) is not exhaustive and an organization should also consider the other controls listed in ISO/IEC 17799 and BS 7799-2:2002 (Annex A). The control objectives and controls are selected as part of the ISMS processes specified in clauses 6 to 9 above.

A.2 Organizational security

A.2.1 Information security infrastructure

Objective: To manage information security within the telecommunications organization.

A.2.2 Allocation of information security responsibilities

Control

Responsibilities for the protection of individual telecommunication assets and for carrying out specific security processes shall be clearly defined.

Implementation requirement for telecommunications

Network maintenance line managers are responsible for ensuring the security of each telecommunication switch as defined by specific security policy. The network maintenance manager is responsible for:

a) ensuring that network maintenance user terminals are located in a restricted area as described in the physical security policies and procedures;

b) ensuring that dial access user logs and user ID logs are appropriately established and maintained;

c) ensuring that central office exchange service authorization codes are appropriately administered;

d) maintaining security measures to ensure that access to telecommunication switches is controlled.

A.3 Asset management

A.3.1 Accountability for assets

Objective: To achieve and maintain appropriate protection of telecommunications assets.

A.3.1.1 Inventory of assets

Control

Each asset shall be clearly identified, and an inventory of all important assets shall be drawn up and maintained.

Implementation requirement for telecommunications

A telecommunications organization shall identify all assets and document the importance of these assets.

An inventory of assets shall be drawn up and maintained of the important assets associated with each telecommunications organization. There are many types of assets associated with telecommunications organization including:

a) Switching assets: Switches for telephone, Internet communications, mobile communications which manage routing information, subscriber information and blacklist information, registered service information, etc.

b) Transmission assets: Transmission relay systems, network cables.

c) Operation assets: Telecommunication management systems to operate switching and transmission assets which contain operational information, trouble information, configuration information, customer information, billing information and traffic statistical information, etc.

d) Telecommunication services assets: Portal information services, credit/prepaid call services, operator-assisted services, ADSL service, mail service, web-building service, mobile service, roaming service, mobile mail service, dialling/directory services, etc.

e) People and their qualifications and skills.

f) Intangibles, such as reputation and image of the organization.

A.3.1.2 Ownership of assets

Control

For reasons of accountability, each asset shall have a designated owner.

Implementation requirement for telecommunications

The term 'owner' identifies an individual or entity that has approved management responsibility for controlling telecommunication services, maintenance, use of, and access to telecommunications assets. The term owner does not mean that the person actually has any property rights to the asset. Ownership may be allocated along:

a) a business process;

b) a defined set of activities;

c) an application/service; or

d) a defined set of data.

A.3.2 Information classification

Objective: To ensure that information assets receive an appropriate level of protection.

A.3.2.1 Classification guidelines

Control

Information and outputs from systems handling classified data shall be classified in terms of its value, sensitivity and criticality to the telecommunications organization.

Implementation requirement for telecommunications

Classifications and associated protective controls for information shall take account of business needs for sharing or restricting information, and the business impacts associated with such needs.

Classification guidelines shall include conventions for initial classification and reclassification over time, in accordance with some predetermined policy.

Classification of information assets can be made in terms of confidentiality, integrity and availability, or any other criterion suitable to express the protection needs.

Information associated with subscribers and customers shall be handled in a sensitive manner. Information related to switching and transmission assets shall also be managed in a critical manner.

A.3.2.2 Information labelling and handling

Control

An appropriate set of procedures for information labelling and handling shall be developed in accordance with the classification scheme adopted by the telecommunications organization.

Implementation requirement for telecommunications

Procedures for information labelling need to cover information assets in physical and electronic formats.

Output from systems containing information that is classified as being sensitive or critical shall carry an appropriate classification label (in the output).

For each classification level, handling procedures including the secure processing, storage, transmission, declassification and destruction shall be defined. This shall also include the procedures for logging of any security relevant event.

Agreements with other telecommunication bodies that include information sharing shall include procedures to identify the classification of that information and to interpret the classification labels from other telecommunication bodies.

A.4 Personnel security

A.4.1 Responding to security incidents and malfunctions

Objective: To minimize damage from security incidents and malfunctions, and to monitor and learn from such incidents.

A.4.1.1 Reporting security incidents

Control

Security incidents shall be reported through appropriate telecommunication management channels as quickly as possible.

Implementation requirement for telecommunications

Security incidents caused by various types of threads such as viruses, Trojan horse, worms, malicious mobile code shall be immediately reported to the related employees and contractors based on a formal reporting procedure. As the action to be taken on the receipt of an incident report, an incident response procedure shall be established properly. Feedback processes to recover from the

incidents shall be implemented to minimize the damages of telecommunication facilities and services. If necessary, it is also required to promptly report the incidents to the related customers through direct e-mails and/or home-page provided by the telecommunications organization.

A.4.1.2 Reporting security weaknesses

Control

Users of information services shall be required to note and report any observed suspected security weaknesses in, or threats to, systems or services.

Implementation requirement for telecommunications

Telecommunication body shall be well aware of the system configurations and specifications in view of security, and shall be taken care of security weaknesses and/or vulnerabilities there. If the weaknesses are found, they should be reported to the related management in order to maintain the system in a secure manner.

A.4.1.3 Reporting software malfunctions

Control

Procedures shall be established for reporting software malfunctions.

Implementation requirement for telecommunications

Procedures shall be established for reporting software malfunctions existed in telecommunication system. The following actions should be considered:

a) The signs of the problem and any messages appearing on the telecommunication management system should be noted.

b) The telecommunication system should be isolated, if possible, and use of it should be stopped. The appropriate contact should be alerted immediately. If the system is to be examined, it should be disconnected from any telecommunication operating networks before being re-powered.

c) The matter should be reported immediately to the information security manager. Appropriately trained and experienced staff should carry out to recover it.

A.4.1.4 Learning from incidents

Control

Mechanisms shall be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.

Implementation requirement for telecommunications

This information should be used to identify recurring or high impact incidents or malfunctions.

A.5 Physical and environmental security

A.5.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to business premises and information.

A.5.1.1 Physical security perimeter

Control

Telecommunications body shall use security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) to protect areas, which contain switching, transmission, operation and information processing facilities.

Implementation requirement for telecommunications

The following guidelines shall be considered and implemented where appropriate for physical security perimeters:

a) Security perimeters shall be clearly defined, and the siting and strength of each of the perimeters shall depend on the security requirements of the assets within the perimeter and the results of a risk assessment.

b) Physical security is crucial in telecommunication facilities, and shall be effectively installed, with all local security policies rigorously enforced to ensure the protection of corporate assets at all times. If a system is malfunctioning or a policy is not followed, it is imperative that the issue be resolved immediately.

c) Perimeters of a building or site containing information processing facilities shall be physically sound (i.e., there shall be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site shall be of solid construction and all external doors shall be suitably protected against unauthorized access with control mechanisms, e.g., bars, alarms, locks, etc. Doors and windows shall be locked when unattended and external protection shall be considered for windows, particularly at ground level. Especially, perimeters of base stations for mobile communications, which are located in isolated areas, shall be strongly protected by such control mechanisms.

d) A manned reception area or other means to control physical access to the site or building shall be in place. Access to sites and buildings shall be restricted to authorized personnel only.

e) Physical barriers shall, where applicable, be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination.

f) All fire doors on a security perimeter shall be alarmed and monitored and shall slam shut.

g) Suitable intruder detection systems shall be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows. For telecommunications operations centres, strong physical intruder detection systems shall be equipped. Unoccupied areas shall be alarmed at all times. Cover shall also be provided for other areas, e.g., computer room or communications rooms.

h) Information processing facilities managed by the telecommunications bodies shall be physically separated from those managed by third parties.

i) Facilities for telecommunications organizations, e.g., transmission facilities, switching facilities and telecommunications infrastructure, shall be physically separated to install from other facilities, e.g., customer facilities in managed data centre.

A.5.1.2 Physical entry controls

Control

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Implementation requirement for telecommunications

The following guidelines shall be considered:

a) Visitors to secure areas shall be supervised or cleared and their date and time of entry and departure recorded. They shall only be granted access for specific, authorized purposes and shall be issued with instructions on the security requirements of the area and on emergency procedures.

b) At front desk, other visitor's information shall be protected. e.g., their date and time of entry and departure record should not be kept in easily viewable place. The receptionist shall also check visitor's belongings if he keeps dangerous objects with him.

c) Access to areas where sensitive information is processed and that contain information processing facilities shall be controlled and restricted to authorized persons only. Authentication controls, e.g., access control card plus PIN, shall be used to authorize and validate all access. Especially, operation rooms to operate facilities shall be adequately protected by mechanism of strong entry controls.

d) An audit trail of all access shall be securely maintained.

e) All personnel shall be required to wear some form of visible identification and shall be encouraged to challenge unescorted strangers and anyone not wearing visible identification.

f) Third-party support services personnel shall be granted restricted access to secure areas or sensitive information processing facilities only when required. This access shall be authorized and monitored.

g) Access rights to secure areas shall be regularly reviewed and updated.

h) Telecommunications operator shall contract with an appropriate security company to physically protect the sensitive telecommunications facilities. If an unauthorized physical access is detected, the operator shall immediately contact with the security company against the incident.

A.5.1.3 Securing offices, rooms and facilities

Control

A telecommunications organization shall design and apply additional physical security for offices, rooms and facilities against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.

Implementation requirement for telecommunications

Consideration shall be given to any security threats presented by neighbouring premises, e.g., a fire in neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street shall be considered.

The following general guidelines shall be considered to secure offices, rooms and facilities:

a) Key facilities shall be sited to avoid access by the public.

b) Where applicable, buildings shall be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities.

c) Directories and internal telephone books identifying locations of sensitive information processing facilities should not be readily accessible by the public.

d) Hazardous or combustible materials shall be stored securely at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area until required.

e) Fallback equipment and back-up media shall be sited at a safe distance to avoid damage from a disaster at the main site.

The following specific guidelines shall be considered for telecommunication facilities:

a) *Securing communication centres*

To protect communication facilities such as switching facilities for providing telecommunications business (hereafter referred to as communication centres), the following shall take place:

i) A site on rigid ground shall be selected for communication centres. If necessary, less than rigid ground may be selected provided adequate measures are taken to prevent uneven settlement.

ii) A site whose environment is least susceptible to damage from wind and water, etc. shall be selected for communication centres. If necessary, less than satisfactory site may be selected provided appropriate measures are taken against wind and water hazards, etc.

iii) A site whose environment is least susceptible to damage from strong electromagnetic field shall be selected for communication centres. If necessary, less than satisfactory site may be selected provided appropriate measures are taken to protect telecommunications equipment rooms with electromagnetic shields, etc.

iv) Sites adjacent to facilities storing dangerous articles that pose the danger of explosion or combustion shall be avoided for communication centres.

v) The building for communication centres shall be of earthquake-proof construction.

vi) The building for communication centres shall be of fire-proof construction or of fire-resistant construction.

vii) The building for communication centres shall have the required structural durability against floor load.

viii) Automatic fire alarms shall be installed in communication centres wherever necessary.

ix) Fire extinguishers shall be installed in communication centres wherever necessary.

b) *Securing telecommunications equipment room*

To protect a room in which communication facilities are set for providing telecommunications business (hereafter referred to as telecommunications equipment room), the following controls shall be considered:

i) The telecommunications equipment room shall be located where it is least susceptible to external effects such as natural disasters.

ii) The telecommunications equipment room shall be located where it is least susceptible to intrusion by unauthorized personnel. This may not be necessary, however, if adequate measures are taken to prevent such intrusions.

iii) The telecommunications equipment room shall be located where it is least susceptible to flooding. If the room must be located where it is susceptible to flooding, one shall take necessary measures such as raising the floor level, installing a water blockade, or installing special water drainage facilities.

iv) The telecommunications equipment room shall be located where it is least susceptible to damage from strong electromagnetic field. If the room must be located where it is susceptible to electromagnetic field, it shall be protected by electromagnetic shields or something else.

v) Important facilities shall be placed in an exclusive telecommunications equipment room with doors of sufficient strength.

vi) Measures shall be taken to prevent the materials used for the floor, walls, ceiling, etc., from collapsing and falling, etc. due to earthquakes of normally predictable magnitude.

vii) Materials used for the floor, walls, ceiling, etc., shall be non-combustible or fire-resistant.

viii) Measures shall be taken to deal with static electricity.

ix) If power supply facilities are installed within the telecommunications equipment room, measures shall be taken, as necessary, to prevent interference from electromagnetic field.

x) Through-holes of the telecommunications equipment room shall be designed to check the spread of fires.

xi) If necessary, measures shall be taken to protect the data storage room and data safe from electromagnetic interference.

xii) Fire-proofing measures shall be taken for a data storage room and dedicated data warehouses as needed.

xiii) Automatic fire alarms shall be installed in the telecommunications equipment room and the air-conditioning facility room, etc., wherever necessary.

xiv) Fire extinguishers shall be installed in the telecommunications equipment room and the air-conditioning facility room, etc., wherever necessary.

xv) The telecommunications equipment room shall be air-conditioned as necessary.

xvi) Air-conditioning of telecommunications equipment room housing important facilities shall be performed by a system separate from that for offices and other rooms. This may not be necessary if adequate measures are taken to properly air-condition the telecommunications equipment room.

xvii) In managed data centre, customer information shall be properly protected when systems for several companies in same trade are installed. These systems shall be placed in different floor or place.

c) *Physically isolated operating area*

To protect physically isolated operating area (e.g., mobile base station) in which communication facilities are set for providing telecommunications business (hereafter referred to as isolated operating area), the following controls shall be considered:

i) Isolated operating area shall be earthquake proofing to meet on the mandated national or regional standards.

ii) Isolated operating area shall be equipped with self-fire control equipment.

iii) Isolated operating area shall be monitored by a remote office for the purpose of detecting facility failures, power failures, fire, humidity and temperature, etc.

iv) Security guard shall be physically provided in a proper manner such as provision of fence to cover the isolated operating area. Since it is normally operated in a self-service, it shall equip an automatic alert function to the maintenance centre in the event of incident.

A.5.1.4 Working in secure areas

Control

Additional controls shall be considered to prevent the compromise of sensitive information and other assets contained in a secure area.

Implementation requirement for telecommunications

The following guidelines for working in secure areas shall be considered:

a) Personnel shall only be aware of the existence of, or activities within, a secure area on a need-to-know basis.

b) Unsupervised working in secure areas shall be avoided both for safety reasons and to prevent opportunities for malicious activities.

c) Vacant secure areas shall be physically locked and periodically checked.

d) Photographic, video, audio or other recording equipment should not be allowed, unless authorized.

e) Third-party support services personnel shall be granted restricted work in secure areas only when required. These working activities shall be authorized and monitored.

A.5.1.5 Isolated delivery and loading areas

Control

Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Implementation requirement for telecommunications

The following guidelines shall be considered:

a) Access to a delivery and loading area from outside of the building shall be restricted to identified and authorized personnel.

b) The delivery and loading area shall be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building.

c) The external door(s) of a delivery and loading area shall be secured when the internal door is opened.

d) Incoming material shall be inspected for potential threats before it is moved from the delivery and loading area to the point of use.

e) Incoming material shall be registered, if appropriate, on entry to the site.

A.5.2 Equipment security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

A.5.2.1 Equipment siting and protection

Control

Equipment shall be sited or protected to reduce the risks from environmental threats, and opportunities for unauthorized access.

Implementation requirement for telecommunications

The following guidelines shall be considered to protect equipment:

a) Equipment shall be sited to minimize unnecessary access into work areas.

b) Telecommunications facilities handling sensitive data shall be positioned to reduce the risk of information being viewed by unauthorized people during their use.

c) Items requiring special protection shall be isolated to reduce the general level of protection required.

d) Controls shall be adopted to minimize the risk of potential physical threats, e.g., theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation,

vandalism. In particular, telecommunication equipments shall be implemented and stably placed against earthquake. Thunder-resistant transformer shall be equipped as a thunder measures.

e) An organization shall consider guidelines for eating, drinking and smoking in proximity to telecommunications facilities.

f) Environmental conditions shall be monitored for conditions, which could adversely affect the operation of telecommunications facilities.

g) Lightning protection shall be applied to all buildings and lightning protection filters shall be fitted to all incoming power and communications lines.

h) The impact of a disaster happening in nearby premises, e.g., a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street shall be considered.

A.5.2.2 Supporting utilities

Control

Equipment shall be protected from power failures and other disruptions caused by supporting utilities.

Implementation requirement for telecommunications

All supporting utilities, such as electricity, water supply, sewage, heating/ventilation and air conditioning, shall be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.

The following guidelines shall be considered for supporting utilities:

a) An uninterruptible power supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Power contingency plans shall cover the action to be taken on failure of the UPS. UPS equipment shall be regularly checked to ensure it has adequate capacity and tested in accordance with the telecommunications' requirements especially for operation centres.

b) A back-up generator shall be considered if processing is to continue in case of a prolonged power failure. If installed, generators shall be regularly tested in accordance with the telecommunications' instructions. An adequate supply of fuel shall be available to ensure that the generator can perform for a prolonged period.

c) Emergency power switches shall be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting shall be provided in case of main power failure.

d) In particular, electric facilities in the isolated area such as mobile base stations shall possibly provide a capacity for all loading. If that is impossible, monitoring mechanism for loading capacity on vulnerable part shall be installed. As measures for electric power failures, battery shall be equipped. Especially in isolated area, battery capacities shall be increased or private electric generator shall be adequately equipped.

A.5.2.3 Cabling security

Control

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

Implementation requirement for telecommunications

The following guidelines for cabling security shall be considered:

a) Power and telecommunications lines into information processing facilities shall be underground, where possible, or subject to adequate alternative protection.

b) Network cabling shall be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas.

c) Power cables shall be segregated from communications cables to prevent interference.

d) For sensitive or critical systems further controls to consider include:

   i) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

   ii) use of alternative routings or transmission media providing appropriate security;

   iii) use of fibre optic cabling;

   iv) use of electromagnetic shielding to protect the cables;

   v) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables.

A.5.2.4 Equipment maintenance

Control

Equipment shall be correctly maintained to ensure its continued availability and integrity.

Implementation requirement for telecommunications

The following guidelines for equipment maintenance shall be considered:

a) Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications.

b) Only authorized maintenance personnel shall carry out repairs and service equipment.

c) Records shall be kept of all suspected or actual faults and all preventive and corrective maintenance.

d) Appropriate controls shall be taken when sending equipment off premises for maintenance especially regarding deleted, erased and overwritten data. All requirements imposed by insurance policies shall be complied with.

A.5.2.5 Security of equipment off-premises

Control

The security provided to off-site equipment shall be equivalent to that for on-site equipment used for the same purpose, taking into account the risks of working outside the telecommunications' premises.

Implementation requirement for telecommunications

Regardless of ownership, management shall authorize the use of any equipment outside a telecommunications' premises for information processing.

The following guidelines shall be considered for the protection of off-site equipment:

a) Equipment and media taken off the premises should not be left unattended in public places. Portable computers shall be carried as hand luggage and disguised where possible when travelling.

b) Manufacturers' instructions for protecting equipment shall be observed at all times, e.g., protection against exposure to strong electromagnetic fields.

c) Home-working controls shall be determined by a risk assessment and suitable controls applied as appropriate, e.g., lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office.

d) Adequate insurance cover shall be in place to protect equipment off site.

e) Security risks, e.g., of damage, theft and eavesdropping, may vary considerably between locations and shall be taken into account in determining the most appropriate controls.

A.5.2.6 Secure disposal or re-use of equipment

Control

All items of equipment containing storage media, e.g., fixed hard disks, shall be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal.

Implementation requirement for telecommunications

Devices containing sensitive information shall be physically destroyed or the information shall be destroyed, deleted or overwritten using approved techniques rather than using the standard delete or format function.

A.5.3 General controls

Objective: To prevent compromise or theft of information and information processing facilities.

A.5.3.1 Clear desk and clear screen policy

Control

Telecommunications body shall consider adopting a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.

Implementation requirement for telecommunications

A clear desk/clear screen policy reduces the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. Information left out on desks is also likely to be damaged or destroyed in a disaster such as a fire, earthquake, flood or explosion.

The following guidelines shall be considered:

a) Paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.

b) Sensitive or critical business information shall be locked away (ideally in a safe or cabinet protecting from physical damage) when not required, especially when the office or facility room is vacated.

c) Personal computers and computer terminals and printers should not be left logged on when unattended and shall be protected by key locks, passwords or other controls when not in use.

d) Incoming and outgoing mail points and unattended fax machines shall be protected.

e) Unauthorized use of photocopiers shall be prevented.

f) Sensitive or classified information, when printed, shall be cleared from printers immediately.

A.5.3.2 Removal of property

Control

Equipment, information or software should not be taken off-site without authorization.

Implementation requirement for telecommunications

The following guidelines shall be considered:

a) assets should not be taken off-site without authorization;

b) individuals who have authority to permit off-site removal of assets shall be clearly identified;

c) where necessary and appropriate, equipment shall be logged out and logged back in when returned;

d) spot checks shall be undertaken to detect unauthorized removal of property;

e) individuals shall be made aware that spot checks will take place.

A.6 Communications and operations management

A.6.1 Operational procedures and responsibilities for information security infrastructure

Objective: To ensure the correct and secure operation of information processing facilities.

A.6.1.1 Incident management procedures

Control

Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents and to collect incident related data such as audit trails and logs.

Implementation requirement for telecommunications

The following guidelines shall be considered:

a) Procedures should be established to cover all potential types of security incident, including:
   i) telecommunication system failures and loss of service;
   ii) denial of service;
   iii) errors resulting from incomplete or inaccurate business data;
   iv) breaches of confidentiality.

b) In addition to normal contingency plans (designed to recover systems or services as quickly as possible), the procedures should also cover:
   i) analysis and identification of the cause of the incident;
   ii) planning and implementation of remedies to prevent recurrence, if necessary;
   iii) collection of audit trails and similar evidence;
   iv) communication with those affected by or involved with recovery from the incident;
   v) reporting the action to the appropriate authority.

c) Audit trails and similar evidence should be collected and secured, as appropriate, for:
   i) internal problem analysis;
   ii) use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings;
   iii) negotiating for compensation from software and service suppliers.

d) Customer-initiated issues regarding the operation of existing customer configurations such as hardware outages, network problems, etc. and the company configurations that affect both customer and employees shall be escalated. All customers shall be made full aware of customer escalation procedures and have pertinent documentation provided to them. For example, customer-initiated issues can be prioritized according to the criteria provided:

i) Priority 1 (P1) – Customer site is completely down or is failing to meet SLA requirements;

ii) Priority 2 (P2) – Customer site is being significantly impacted by the outage; one or more systems down or significant packet loss and/or latency;

iii) Priority 3 (P3) – Customer service degraded;

iv) Priority 4 (P4) – Customer requests;

v) Priority 5 (P5) – Pending closure.

e) Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures should ensure that:

i) only clearly identified and authorized staff are allowed access to live systems and data;

ii) all emergency actions taken are documented in detail;

iii) emergency action is reported to management and reviewed in an orderly manner;

iv) the integrity of telecommunication systems and controls is confirmed with minimal delay.

A.6.1.2 Separation of development and operational facilities

Control

Development and testing facilities shall be separated from operational facilities. Rules for the migration of software from development to operational status shall be defined and documented.

Implementation requirement for telecommunications

Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data. The following controls shall be considered:

a) Development and operational software shall, where possible, run on different computer processors, or in different domains or directories.

b) Development and testing activities shall be separated as far as possible.

c) Compilers, editors and other system utilities should not be accessible from operational systems when not required.

d) Different log-on procedures shall be used for operational and test systems, to reduce the risk of error.

e) Development staff shall only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls should ensure that such passwords are changed after use.

A.6.1.3 External facilities management

Control

Prior to using external facilities management services, the risks shall be identified and appropriate controls agreed with the contractor, and incorporated into the contract.

Implementation requirement for telecommunications

The use of an external contractor to manage telecommunication facilities may introduce potential security exposures, such as the possibility of compromise, damage, or loss of data at the contractor's site. These risks should be identified in advance, and appropriate controls agreed with the contractor and incorporated into the contract.

A.6.2 Protection against malicious software

Objective: To protect the integrity of software and information from damage by malicious software.

A.6.2.1 Controls against malicious software

Control

Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.

Implementation requirement for telecommunications

Protection against malicious software shall be based on security awareness, appropriate system access and change management controls. The following controls shall be considered:

a) When software is installed, the quality shall be validated.

b) When software or data is changed, measures in software shall be made to prevent errors.

c) Program faults shall be immediately detected and reported when they occur.

A.6.3 Housekeeping

Objective: To maintain the integrity and availability of telecommunication services.

A.6.3.1 Information back-up

Control

Back-up copies of essential telecommunications information and software shall be taken and tested regularly.

Implementation requirement for telecommunications

Adequate back-up facilities shall be provided to ensure that all essential telecommunication information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of business continuity. The following guidelines should be considered:

a) A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of back-up information shall be retained for important business applications and services.

b) Back-up information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site shall be extended to cover the back-up site.

c) Back-up media shall be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.

d) Restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

e) The retention period for essential telecommunication information, and also any requirement for archive copies to be permanently retained, shall be determined.

A.6.3.2 Operator logs

Control

Operational staff shall maintain a log of their activities. Operator logs shall be subject to regular, independent checks.

Implementation requirement for telecommunications

Logs shall include, as appropriate:

a) system starting and finishing times;

b) system errors in detail and corrective action taken against them;

c) confirmation of the correct handling of data files and system output;

d) the name of the person making the log entry.

A.6.3.3 Fault logging

Control

Faults shall be reported and corrective action taken.

Implementation requirement for telecommunications

Faults reported by users regarding problems with telecommunication systems should be logged. There should be clear rules for handling reported faults including:

a) review of fault logs to ensure that faults have been satisfactorily resolved;

b) review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

A.6.4 Network management

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

A.6.4.1 Network controls

Control

A range of controls shall be implemented to achieve and maintain security in networks.

Implementation requirement for telecommunications

To achieve security in telecommunication networks, the following recovery controls shall be applied:

a) Transmission facilities such as transmission cables shall be well maintained. In case of emergency situation, the facilities shall be repaired promptly as possible.

b) Switching facilities for telecommunication services shall be well maintained and their traffic load shall be monitored constantly. In case of emergency situation, the facilities shall be promptly switched to back-up facilities or other routes in order to avoid a serious traffic congestion.

c) In the case of DoS attacks, the switching facilities such as routers must process a larger amount of traffic compared with ordinary situation. One of the controls shall be to limit the traffic to an allowable level.

A.7 Access control

A.7.1 Telecommunication business requirement for access control

Objective: To control access to information.

A.7.1.1 Access control policy

Control

Telecommunication business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.

Implementation requirement for telecommunications

Access control rules and rights for each telecommunications user or group of users shall be clearly stated in an access control policy. Users and service providers should be given a clear statement of the telecommunication business requirements to be met by access controls.

The policy should take account of the following:

a) security requirements of individual telecommunication business applications;

b) identification of all information related to the business applications;

c) policies for information dissemination and authorization, e.g., the need to know principle and security levels and classification of information;

d) consistency between the access control and information classification policies of different systems and networks;

e) relevant legislation and any contractual obligations regarding protection of access to data or services.

A.7.2 Application access control

Objective: To prevent unauthorized access to information systems held in information systems.

A.7.2.1 Information access restriction

Control

Access to information and application system functions shall be restricted in accordance with the access control policy.

Implementation requirement for telecommunications

Restrictions to access shall be based on individual telecommunication business application requirements. The access control policy shall also be consistent with the access policy of telecommunications organization.

A.7.2.2 Sensitive system isolation

Control

Sensitive systems shall have a dedicated (isolated) computing environment.

Implementation requirement for telecommunications

The following points shall be considered for sensitive system isolation:

a) The sensitivity of an application system shall be explicitly identified and documented by the application owner.

b) Sensitive systems such as a customer database system shall run on a isolated computer and shall only share resources with trusted application systems under the agreement with the owner of the sensitive application.

A.8 System development and maintenance

A.8.1 Security requirements of telecommunication systems

Objective: To ensure that security is built into telecommunication systems.

A.8.1.1 Security requirements analysis and specification

Control

Telecommunication business requirements for new systems, or enhancement to existing systems shall specify the requirements for controls.

Implementation requirement for telecommunications

Security requirements and controls shall reflect the business value of the information assets involved, and the potential business damage, which might result from a failure or absence of security.

System requirements for information security and processes for implementing security shall be integrated in the early stages of information system projects.

The framework for analysing security requirements and identifying controls to fulfil them is based on risk assessment and risk management.

A.8.2 Security in applications

Objective: To prevent loss, unauthorized modification or misuse of data in application systems.

A.8.2.1 Input data validation

Control

Data input to applications should be validated to ensure that it is correct and appropriate.

Implementation requirement for telecommunications

Checks shall be applied to the input of business transactions, standing data (e.g., customer names and addresses, credit limits, customer reference numbers) and parameter tables (e.g., call charge rate, currency conversion rates, tax rates).

A.8.2.2 Output data validation

Control

Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Implementation requirement for telecommunications

Output validation shall include:

a) plausibility checks to test whether the output data is reasonable;

b) providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision and classification of the information;

c) procedures for responding to output validation tests.

A.8.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information.

A.8.3.1 Policy on the use of cryptographic controls

Control

A telecommunications organization shall develop a policy on its use of cryptographic controls for protection of its information.

Implementation requirement for telecommunications

When developing a policy the following shall be considered:

a) the management approach towards the use of cryptographic controls across the telecommunications organization;

b) the approach to key management including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

c) roles and responsibilities for the implementation of the cryptographic policy;

d) how the appropriate level of cryptographic protection is to be determined;

e) the impact of using encrypted information on controls that rely upon contents scanning techniques (e.g., virus detection in the middle of communication).

A.8.3.2 Encryption management

Control

Encryption shall be applied to protect the confidentiality of sensitive or critical information.

Implementation requirement for telecommunications

Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used. When implementing the cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information. In addition, consideration should be given to the controls that apply to the export and import of cryptographic technology.

A.8.3.3 Key management

Control

A key management shall be in place to support the telecommunication's use of cryptographic techniques.

Implementation requirement for telecommunications

All keys shall be protected against modification and destruction, and secret and private keys need protection against unauthorized disclosure. Physical protection shall be used to protect equipment used to generate, store and archive keys.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g., with a certification authority, shall cover issues of liability, reliability of services and response times for the provision of services.

A.8.4 Security of system files

Objective: To ensure the security of access to system files shall be controlled.

A.8.4.1 Control of operational software

Control

Procedures shall be in place to control the implementation of software on operational systems.

Implementation requirement for telecommunications

To minimize the risk of corruption of operational systems, the following guidelines shall be considered:

a) the updating of the operational software, applications and program libraries shall only be performed by trained administrators upon appropriate management authorization;

b) applications and operating system software shall only be implemented after extensive, sufficient and successful testing. If they are to be implemented to sensitive systems such as switching facility, the test shall be carried out with a full coverage of path;

c) an audit log shall be maintained of all updates to operational program libraries;

d) previous versions of application software shall be retained as a contingency measure. If it is a sensitive application software, then at least three generations of software shall be retained;

e) old versions of software shall be archived, together with all required information and parameters, procedures, configuration details and supporting software;

f) any decision to upgrade to a new release shall take into account the security of the release, i.e., the introduction of new security functionality or the number and severity of security problems affecting this version;

g) software patches shall be applied when they can help to remove or reduce security weaknesses.

A.8.4.2 Protection of system test data

Control

Test data shall be protected and controlled.

Implementation requirement for telecommunications

The use of operational data containing personal information or any other sensitive information shall be avoided for test data. If personal or sensitive information is used for the test, all sensitive details and content shall be removed or modified beyond recognition before the test.

The following guidelines shall be applied to protect operational data, when used for testing purposes:

a) the access control procedures, which apply to operational application systems, shall also apply to test application systems;

b) there shall be separate authorization each time operational information is copied to a test application system;

c) operational information shall be strictly erased from a test application system immediately after the testing is complete.

A.8.4.3 Access control to program source library

Control

Strict control shall be maintained over access to program source library.

Implementation requirement for telecommunications

The following requirements shall be considered to control access to program source libraries in order to reduce the potential for corruption of computer programs:

a) program source libraries shall not be held in operational systems;

b) IT support staff for telecommunication facilities shall not have unrestricted access to program source libraries;

c) programs under development or maintenance shall not be held in operational program source libraries. These programs shall be held in the development or maintenance facilities;

d) an audit log shall be maintained of all accesses to program source libraries;

e) maintenance and copying of program source libraries shall be subject to strict change control procedures.

A.8.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

A.8.5.1 Change control procedures

Control

The implementation of changes shall be strictly controlled by the user of formal change control procedure.

Implementation requirement for telecommunications

Formal change control procedures for telecommunication systems shall be strictly documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems shall follow a formal process of documentation, specification, testing, quality control, and managed implementation.

This process shall include a risk assessment, analysis of the impacts of changes, and specification of security controls needed.

This process shall include:

a) ensuring changes are submitted by authorized users;

b) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;

c) identifying all computer software, information, database entities and hardware that require amendment;

d) obtaining formal approval for detailed proposals before work commences;

e) ensuring that the authorized user accepts changes prior to any implementation;

f) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

g) maintaining a version control for all software updates;

h) maintaining an audit trail of all change requests;

i) ensuring that the implementation of changes takes place at the right time and is not disturbing the telecommunication business processes involved.

A.8.5.2 Technical review of applications after operating system changes

Control

Application systems shall be reviewed and tested when changes occur.

Implementation requirement for telecommunications

This process shall cover:

a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;

b) ensuring that notification of operating system changes is provided in time to allow appropriate tests and reviews to take place before implementation.

A.8.5.3 Outsourced software development

Control

Controls shall be applied to secure outsourced software development.

Implementation requirement for telecommunications

Where software development is outsourced, the following points shall be considered:

a) licensing arrangements, code ownership and intellectual property rights;
b) certification of the quality and accuracy of the work carried out;
c) escrow arrangements in the event of failure of the third party;
d) rights of access for audit of the quality and accuracy of work done;
e) contractual requirements for quality of code;
f) testing before installation to detect malicious code.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communications**
Series Y	Global information infrastructure, Internet protocol aspects and Next Generation Networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2004