International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 34

(01/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1051 – Supplement on code of practice for information security controls for telecommunication organizations

ITU-T X-series Recommendations – Supplement 34

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Supplement 34 to ITU-T X-series Recommendations

ITU-T X.1051 – Supplement on code of practice for information security controls for telecommunication organizations

Summary

This Supplement highlights and shares the implementation of a code of practice for information and network security management by the Malaysian information and communication industry, based on Recommendation ITU-T X.1051. The sets of requirements have been identified and documented in the "Requirements for Information and Network Security (INS)" developed by MTSFB (Malaysian Technical Standards Forum Bhd) and approved by MCMC (Malaysian Communications and Multimedia Commission) on 5 October 2016. The requirements are based on Recommendation ITU-T X.1051 for establishing, implementing, maintaining and continually improving information and network security management within the context of an organization. The code of practice for information security controls based on Recommendation ITU-T X.1051 for Malaysian telecommunication organizations provides four (4) families of control focusing on organization, infrastructure, people and environment.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 34	2019-01-30	17	11.1002/1000/13869

Keywords

Information security, network security, risk management, security requirements.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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 publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

			Page
1	Scope		1
2	References		1
3	Definitions		1
	3.1	Terms defined elsewhere	1
	3.2	Terms defined in this Supplement	1
4	Abbreviations and acronyms		1
5	Conventions		1
6	Methodology		1
	6.1	Organization context	2
	6.2	Risk management	2
	6.3	Information and network security objectives and planning to achieve them	4
7	Roles and responsibilities		4
	7.1	Leadership and commitment	4
	7.2	Policy	5
8	Support		6
	8.1	Resources	6
	8.2	Competence	6
	8.3	Awareness	6
	8.4	Communication	6
	8.5	Documented information	6
9	Operation		7
	9.1	Operational planning and control	7
10	Performance evaluation		8
	10.1	Monitoring, measurement, analysis and evaluation	8
	10.2	Internal audit	8
	10.3	Management review	8
11	Improvement		9
	11.1	Nonconformity and corrective action	9
	11.2	Continual improvement	9
Appendix I – Reference to applicable controls and how they can be applied			10
	I.1	Organization	10
	I.2	Infrastructure	12
	I.3	People	15
	I.4	Environment	16

Page

Appendix II – Additional controls for consideration 17
II.1 CSIRT and SOC 17
II.2 Cybersecurity information exchange (CYBEX) 17
Bibliography 18

Supplement 34 to ITU-T X-series Recommendations

ITU-T X.1051 – Supplement on code of practice for information security controls for telecommunication organizations

1 Scope

This Supplement to Recommendation ITU-T X.1051 provides guidance for establishing, implementing, maintaining and continually improving an information and network security management system within the context of an organization. This guidance includes the assessment and treatment of information security risks tailored to the needs of the organization. This guidance is generic and intended to be applicable to all organizations, regardless of size, type or nature.

2 References

The following reference is indispensable for the application of this technical code.

[ITU-T X.1051] Recommendation ITU-T X.1051:ISO/IEC 27011 (2016), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 teleworking: Working from a remote location, e.g., home.

3.2.2 mobile devices: Devices that provide computing and mobility such as mobile phones.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

CISO Chief Information Security Officer

CSIRT Computer Security Incident Response Team

INS Information and Network Security

SOC Security Operation Centre

5 Conventions

None.

6 Methodology

The methodology follows the security requirements as recommended in [ITU-T X.1051] and identified by a methodical assessment of security risks. The results of the risk assessment provide guidance in managing information security risks and the required implementation controls for the organization. Risk management comprises the following activities.

6.1 Organization context

6.1.1 Understanding context of organization

The organization should determine internal and external issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information and network security management system.

6.1.2 Understanding the expectation of interested parties

The organization should determine:

a) interested parties that are relevant to the information and network security management systems; and

b) the requirements of these interested parties relevant to the information and network security.

NOTE – The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

6.1.3 Determining the scope of information and network security management system

The organization should determine the boundaries and applicability of the information and network security management system to establish its scope. The determination of scope should also take the following into consideration:

a) the internal and external issues referred to in clause 6.1;

b) the guidelines referred to in clause 6.2; and

c) interfaces and dependencies between activities performed by the organization and those that are performed by other organizations.

The scope should be available as documented information.

6.1.4 Information and network security management system

The organization should establish, implement, maintain and continually improve an information and network security management system, in accordance with the identified guidelines.

6.2 Risk management

6.2.1 General

When planning for an information and network security management system, the organization should consider the issues referred to in clause 6.1 and determine the risks and opportunities that need to be addressed in order to:

a) ensure the information and network security management system can achieve its intended outcome(s);

b) prevent or reduce undesired results to the business and objectives of the programme; and

c) achieve continual improvement.

The organization should plan:

a) actions to address these risks and opportunities; and

b) how to:

   i) integrate and implement the actions into its information and network security management system processes; and

   ii) evaluate the effectiveness of these actions.

6.2.2 Communication and consultation

Engagement sessions with both internal and external stakeholders should occur throughout the information security risk management process. Communication and consultation with stakeholders is important as stakeholders make judgements based on their perceptions of risk which can vary in values, needs, assumptions, concepts and concerns.

6.2.3 Establish information security risk criteria

The organization should establish the external and internal context of its information security risk management process. This includes the establishment of the information security risk acceptance criteria and the criteria for performing information security risk assessments.

6.2.4 Information security risk assessment

Risk assessment is an integral part of information security risk management. It comprises of risk identification, risk analysis and risk evaluation.

a) A risk assessment should establish and maintain information and network security risk criteria that includes:
   i) the risk acceptance criteria; and
   ii) criteria for performing an information and network security risk assessment;

b) Ensure that repeated information security risk assessments produce consistent, valid and comparable results.

c) Identify the information and network security risks:
   i) Apply the information and network security risk assessment process to identify risks associated with the confidentiality, integrity and availability for information within the scope of the information and network security management system; and
   ii) identify risk owners.

d) Analyse the information and network security risks:
   i) Assess the potential consequences that would result if the risks identified materialize;
   ii) assess the realistic likelihood of the occurrence of the risks identified; and
   iii) determine the level of risks.

e) Evaluate the information and network security risks:
   i) Compare the result of risk analysis with the risk criteria established in clause 6.2.3; and
   ii) prioritize analysed risk for risk treatment.

6.2.5 Information and network security risk treatment

The organization should define and apply an information and network security risk treatment process to:

a) Select appropriate information and network security risk treatment options, taking account of the assessment result.

b) Determine all controls that are necessary to implement the information and network security risk treatment option(s) chosen.

   NOTE – Organizations can design controls as required or identify them from any source. Examples of controls are given in Appendix I and Appendix II.

c) Compare the controls determined in clause 6.2.5 b) above with those in Appendix I and verify that no necessary controls have been omitted.

   NOTE 1 – Appendix I contains a comprehensive list of control objectives and controls. Users of this document are directed to Appendix I to ensure that no necessary controls are overlooked.

NOTE 2 – Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Appendix I are not exhaustive and additional control objectives and controls may be needed.

d) Produce a statement of applicability that contains the necessary controls and justifications for inclusions, whether they are implemented or not, and the justification for exclusion of controls from Appendix I.

e) Formulate an information and network security risk treatment plan; and

f) obtain risk owner's approval of the information and network security risk treatment plan and acceptance of the residual information and network security risk.

The organization should retain documented information about the information and network security risk assessment process.

6.3 Information and network security objectives and planning to achieve them

The organization should establish information and network security objectives at relevant functions and levels.

The information and network security objectives should:

a) be consistent with the information and network security policy;

b) be measurable (if applicable);

c) take into account applicable information and network security requirements, and results from risk assessment and risk treatment;

d) be communicated; and

e) be updated as appropriate.

The organization should retain documented information on the information and network security objectives.

When planning how to achieve its information and network security objectives, the organization should determine:

a) what will be done;

b) what resources will be required;

c) who will be responsible;

d) when it will be completed; and

e) how the results will be evaluated.

7 Roles and responsibilities

7.1 Leadership and commitment

Top management should demonstrate leadership and commitment with respect to the information and network security management system by:

a) ensuring the information and network security policy and the objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information and network security requirements into the organization's process;

c) ensuring that the resources needed for the information and network security management system are available;

d) communicating the importance of effective information and network security management and of confirming to the information and network security management requirements;

e) ensuring that the information and network security management system achieves the intended outcome(s);

f) directing and supporting persons to contribute the effectiveness of the information and network security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibilities.

7.2 Policy

Organization leadership should establish a management framework to initiate and control the implementation of information and network security. Management should approve the information and network security policy, assignment of security roles, coordinate and review of the implementation of security across the organization.

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. Reviews include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

Top management should establish an information and network security policy that:

a) is appropriate to the purpose of the organization;

b) includes information and network security objectives or provides the framework for setting the information and network security objectives;

c) includes a commitment to satisfy applicable requirements related to information and network security; and

d) includes a commitment to continual improvement of the information and network security management system.

The information and network security policy should:

a) be available as documented information;

b) be communicated within the organization; and

c) be available to interested parties, as appropriate.

7.2.1 Roles, responsibilities within the organization and authorities

Top management should ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management should assign the responsibilities and authority for:

a) ensuring that the information and network security management system conforms to the guidelines of this Supplement; and

b) reporting on the performance of the information and network security management system to top management.

NOTE – Top management may also assign responsibilities and authorities for reporting the performance of the information and network security management system within the organization.

These functions should be assigned in the applicable organization:

a) regulatory/authority contact;

b) information and network security responsibility such as chief information security officer (CISO); and

c) risk management.

8 Support

8.1 Resources

The organization should determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information and network security management system.

8.2 Competence

The organization should:

a) determine the necessary competence of person(s) doing work under its control that affects the performance of information and network security;

b) ensure that these persons are competent on the basis of appropriate education, training or experience;

c) where applicable, take action to acquire the necessary competence and evaluate the effectiveness of the action taken; and

d) retain appropriate documented information as evidence of competence.

NOTE – Applicable action may include, for example: The provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

8.3 Awareness

Persons doing work under the organization's control should be aware of:

a) information and network security policy;

b) their contribution to the effectiveness of the information and network security management system, including the benefits of improved information and network security performance; and;

c) the implications of not conforming to the information and network security management system.

8.4 Communication

The organization should determine the need for internal and external communications relevant to information and network security management systems including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who should communicate; and

e) the process by which communication should be affected.

8.5 Documented information

8.5.1 General

The organization's information and network security management should include:

a) documented information required by this document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information and network security management system.

The extent of documented information for an information and network security management system can differ from one organization to another due to:

a) size and type of activities, processes, products and services of an organization;

b) the complexity of processes and their interactions; and

c) the competence of the persons.

8.5.2 Creating and updating

When creating and updating documented information the organization should ensure appropriate:

a) identification and description (e.g., title, date, author or reference number);

b) format (e.g., language, software version, graphics) and media (e.g., paper, electronic); and

c) review and approval for suitability and adequacy.

8.5.3 Control of documented information

Documented information required by the information and network security management system and by this document should be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g., from loss of confidentiality, improper use or loss of integrity).

For the control of documented information, the organization should address the following activities as applicable:

a) distribution, access, retrieval and use;

b) storage and preservation, including the preservation of legibility;

c) control of changes (e.g., version control); and

d) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information and network security management system, should be identified as appropriate and controlled.

NOTE – Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

9 Operation

9.1 Operational planning and control

The organization should plan, implement and control the processes needed to meet information and network security requirements, and to implement the actions determined in clause 6.1. The organization should also implement plans to achieve the information and network security objectives determined in clause 6.3.

The organization should keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization should control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization should ensure that outsourced processes are determined and controlled.

10 Performance evaluation

10.1 Monitoring, measurement, analysis and evaluation

The organization should evaluate the information security performance and the effectiveness of the information and network security management system.

The organization should determine:

a) what needs to be monitored and measured, including information and network security processes and controls; and

b) the methods for monitoring, measurement, analysis and evaluation, as applicable to ensure valid results.

NOTE – The methods selected should produce comparable and reproducible results to be considered valid.

The organization should retain appropriate documented information as evidence of the monitoring and measurement results.

10.2 Internal audit

The organization should conduct internal audits at planned intervals to provide information on whether the information and network security management system:

a) conforms to:

   i) the organization's own requirements for its information and network security management system; and

   ii) the requirements of this Supplement;

b) is effectively implemented and maintained.

The organization should:

a) plan, establish, implement and maintain an audit programme(s), including the frequency, method, responsibilities, planning requirements and reporting. The audit programme(s) should take into consideration the importance of the processes concerned and the result of the previous audit;

b) define the audit criteria and scope of each audit;

c) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

d) ensure that the results of the audits are reported to the relevant management; and

e) retain documented review information as evidence of the audit programme(s) and the audit results.

10.3 Management review

Top management should review the organization's information and network security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review should include considerations of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information and network security management system;

c) feedback on the information and network security performance, including trends in:

   i) nonconformity and corrective actions;

   ii) monitoring and measurement results;

iii) audit results; and

iv) fulfilment of information and network security objectives;

d) feedback from interested parties;

e) results of risk assessment and status of a risk treatment plan; and

f) opportunities for continual improvement.

The outputs of the management review should include decisions related to continual improvement opportunities and any need for changes to the information and network security management system.

The organization should retain documented information evidence of the results of management reviews.

11 Improvement

11.1 Nonconformity and corrective action

When nonconformity happens, the organization should:

a) react to the nonconformity, and as applicable:

i) take action to control and correct it; and

ii) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere by:

i) reviewing the nonconformity;

ii) determining the causes of the nonconformity; and

iii) determining if similar nonconformity exists or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information and network security management system, if necessary.

Corrective actions should be appropriate to the effects of the nonconformity encountered. The organization should retain documented information as evidence of:

a) the nature of the nonconformity and any subsequent actions taken; and

b) the results of any corrective action.

11.2 Continual improvement

The organization should continually improve the suitability, adequacy and effectiveness of the information and network security management system.

Appendix I

Reference to applicable controls and how they can be applied

Controls

The following controls apply based on identified risks in line with clause 6.2.5. These controls, illustrated in Figure I.1 are divided into four families of controls.

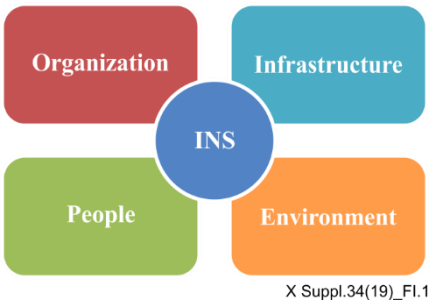

Figure I.1 – Families of control

I.1 Organization

This family of control focuses on organizational readiness for information and network security. A business should have a formal and systematic approach to implementing and maintaining an effective information and network security programme.

I.1.1 Information and network security policy

The information and network security policy encompasses information security requirements that provide the management direction and intent based on business requirements hich are:

a) guided by relevant laws and regulatory requirements; and

b) reviewed at planned intervals to ensure congruence towards the dynamic landscape of business, appropriateness based on current technologies and effectiveness of controls and requirements.

I.1.2 Business continuity management

Organization survival depends on having a solid business continuity plan. This plan needs to incorporate the information and network security elements to ensure completeness and comprehensiveness of the plan, in line with the organization's information and network security programme, including the following:

a) Establish, maintain and implement effective plans for emergency response and post-disaster recovery to ensure availability and continuity of operations in emergency situations; and

b) review, verify and evaluate the plans at regular intervals to ensure effectiveness and validity.

c) Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

I.1.3 Information and network security compliance

Organizations are bound by the laws of the land, which require compliance by identifying and understanding the legal, statutory and contractual obligations pertaining to information and network security, given below.

a) Identify, document and keep up to date applicable legal, statutory and contractual obligations.

b) Protect records/information, personal and sensitive data in accordance with legal, regulatory, contractual and business requirements.

c) Procedures should be established in relation to management of intellectual property rights and use of proprietary software products.

d) Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.

e) Privacy and personally identifiable information should be ensured as required in relevant legislation and regulation, where applicable.

f) The organization's approach to managing information and network security and its implementation should be reviewed independently at planned intervals or when significant changes occur.

g) Managers of the organization should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

h) Information systems should be regularly reviewed for compliance with the organization's information and network security policies and standards.

I.1.4 Organization of information security

a) Establish a management framework to initiate and control the implementation and operation of information security within the organization, including:

   i) information security roles and responsibilities;

   ii) segregation of duties;

   iii) contact with authorities;

   iv) contact with special interest groups; and

   v) information security in project management.

b) Ensure the security of teleworking and use of mobile devices with:

   i) a mobile device policy; and

   ii) teleworking.

I.1.5 Information security incident management

a) Security incident management will assist in responding appropriately to security incidents, including applying appropriate remedies and future prevention measures.

b) Security events and weaknesses are communicated in a manner allowing timely corrective action to be taken.

c) Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents.

d) Incidents related to information and network security should be reported through appropriate management channels as quickly as possible.

e) Evidence relating to a security violation must be properly collected, documented and preserved.

f) All incidents must be properly investigated and analysed. Corrective action must be taken to recover from security violations. Subsequently, preventative measures must be taken to avoid the reoccurrence of the incident. Reviews must be done on a periodic basis (as part of operational procedural review) to evaluate the effectiveness of the controls, lessons learned and disciplinary action taken.

g) Knowledge gained from incidents should be used to reduce the likelihood or impact of future incidents.

I.2 Infrastructure

Managing the security of infrastructure of information security is one of the control focuses on the organization's readiness in managing information and network security. This is due to growing information security risks; organizations must also continually monitor and effectively manage the security of their computing infrastructure to ensure the confidentiality, integrity and availability of their information assets**.**

I.2.1 Asset management

Business performance relies on its assets. Business assets may comprise of physical or virtual elements, network equipment, server hardware and human capital.

a) Assets pertaining to information and processing should be identified.

b) Assets should be drawn and maintained in an inventory with the owners identified, returned upon termination of employment, contract or agreement; and

c) acceptable use of asset rules should be identified, documented and implemented.

I.2.2 Information management

a) Information should be classified, labelled and handled in accordance with value, sensitivity, criticality and legality.

b) Procedures should be implemented for the management of information life cycle including asset handling.

c) Test data should be carefully selected, protected and controlled; and

d) test data derived from production data should be protected as equivalent to production data.

I.2.3 Media management

a) Procedures should be implemented for the management and disposal of storage media based on the classification scheme; and

b) media containing information should be protected against unauthorized access, misuse or corruption.

I.2.4 Access control

a) An access control policy should be drawn up, documented and reviewed based on business and information and network security requirements; and

b) access to network and services should only be provided for those who have been specifically authorized to do so.

I.2.5 User access management

a) A formal process for user registration and de-registration should be implemented to enable assignment of accounts and access rights.

b) A formal process for user access provisioning should be implemented to assign or revoke access rights for all types of users, systems and services.

c) The allocation and use of privileged access rights should be restricted and controlled.

d) The allocation of secret authentication information should be controlled through a formal management process.

e) Users should be required to adhere to an organization's practices in the use and management of secret authentication information.

f) The allocation and use of privileged access rights should be restricted and controlled.

g) Asset owners should formally review user's access rights at regular intervals; and

h) a formal process to remove access rights of all employees and external party users to information, systems, infrastructure and services upon termination of their employment, contract or agreement, or adjust upon change is implemented and managed.

I.2.6 Systems, services and application access control

a) Access to systems, services and applications should be restricted in accordance with the access control policy of the organization.

b) Access to systems, services and applications should be controlled by a secure log-on procedure where required by the access control policy.

c) When passwords are used a password management system should be interactive and should ensure quality/strong passwords; and

d) use of privileged systems which provide capabilities to override system and application controls should be restricted and tightly controlled.

e) Programme source code access should be restricted.

I.2.7 Cryptography

a) A policy on the use of cryptographic controls for the protection of information should be developed and maintained, based on legal/regulatory obligations and other industry requirements.

b) A cryptographic key management policy on the use, protection and lifetime should be developed and implemented to manage its life cycle; and

c) cryptographic controls should be used in compliance with all relevant legislations, regulations and contracts/agreements and should be in accordance with industry best practices.

I.2.8 Information and network security in operations

a) Operating procedures should be documented and made available.

b) Changes made in the operations environment should be controlled, managed and documented.

c) Resources used in operations should be monitored, tuned and protections made of future capacity requirements to ensure meeting the required system performance; and

d) Environments of development, testing and operations should be kept separate to reduce risks of unauthorized access or changes.

I.2.9 Malicious software protection

a) Sufficient detection, prevention and recovery controls to protect against malware should be implemented; and

b) awareness of malware should be made to all organization users.

I.2.10 Logging and monitoring

a) Event logs should be enabled to record system activities, exceptions, faults and security events.

b) Event logs should be kept and regularly reviewed.

c) Logs and logging facilities should be protected against unauthorized access and tampering.

d) Clocks of all relevant systems/ information and infrastructure should be synchronized to an organization authorized reference time source; and

e) administrative and operator access should be logged and the logs regularly reviewed and sufficiently protected.

I.2.11 Control of operational software

Installation of software on operational systems should be controlled based on installation and implementation procedures.

I.2.12 Technical vulnerability management

a) Information about technical vulnerabilities of systems/networks/infrastructure should be obtained in a timely manner, to ensure that exposure to such vulnerabilities are evaluated and necessary measures taken to address the risk; and

b) procedures governing the installation of software by users should be established and implemented.

I.2.13 Information and network audit

Activities involving the verification of operational systems and audit requirements should be planned and agreed to minimize disruption to business processes.

I.2.14 Backup

Backup copies of information and required software should be taken and tested regularly according to an agreed backup policy.

I.2.15 Network communications security management

a) Networks should be managed and controlled to protect information in systems, applications and services.

b) Network service agreements for both in-source and outsourced environments should contain requirements of security mechanisms, service levels and management of all network services; and

c) networks should be segregated based on groups of information services, users and systems.

I.2.16 Information transfer

a) Formal policies, procedures and controls should be in place to protect information transfer through the use of all types of communication facilities.

b) Formal agreements should address the secure transfer of information between an organization and external parties.

c) Electronic messaging that contains information for the organization should be protected; and

d) non-disclosure or confidentiality agreements reflecting the need of the organization to protect information should be identified, regularly reviewed and documented.

I.2.17 Security requirements of systems

a) Information and network security related requirements should be included in the requirements for new systems or existing system enhancements; and

b) information pertaining to application service and service transactions should be protected to maintain confidentiality, integrity and availability.

I.2.18 Security requirements for development and support processes

a) A procedure for the development of systems, software and services should be established and applied to developments within the organization;

b) Changes to systems, software and services within the development life cycle should be controlled through a formal change control procedure.

c) Business critical applications, software and services should be reviewed and tested to ensure there is no adverse impact on operations or security when operating platforms have been changed.

d) All changes to systems, software and services should be strictly controlled; modifications to packages should be discouraged and limited to necessary changes.

e) Secure systems engineering principles should be established, documented, maintained and applied to any implementation efforts.

f) A procedure for establishing and protecting a secure development environment for development and integration efforts that cover the entire system development life cycle should be drawn up.

g) Security functionality testing should be carried out during development.

h) Organizations should supervise and monitor activities of outsourced system development; and

i) acceptance testing criteria and programmes should be established for new systems, upgrades and new versions.

I.2.19 Systems acquisition, development and maintenance

a) All security requirements should be identified and analysed at the requirements phases of a project and justified, agreed, documented, tested and delivered as part of the overall business case for an information system; and

b) project and support environments should be strictly controlled. A designated owner should be responsible for the security elements of the project or support processes.

I.3 People

As technology is considered to be an essential part of securing information assets, the people are responsible for the design, implementation and operation of the technology. The people may be the driving factor or the restraining forces in the effectiveness of the information security management system.

I.3.1 Human resource security

a) The organization should ensure employees and contractors understand and comply with their responsibilities and are suitable for the roles for which they are assigned; and

b) the organization should adhere to its security-related responsibilities in personnel-related processes, inclusive of:

   i) screening;

   ii) terms and conditions of employment;

   iii) management responsibilities;

   iv) information security awareness, education and training;

   v) disciplinary process; and

   vi) termination or change of employment responsibilities.

I.3.2 Supplier relationships

a) The organization should ensure that its suppliers and partners are aware of their security obligations, and that these suppliers and partners maintain a security standard that is suitable to prevent breaches in security.

b) The supplier agreements should include requirements for information and network security and address information and network security risks associated with information technology services and product supply chains.

c) Organizations should regularly monitor, review and audit supplier service delivery.

d) Changes to the provision of services by suppliers, including maintaining and improving existing information and network security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.

I.4 Environment

The environment and physical security is another essential factor in protecting people, data, equipment, systems, facilities and company assets. The information security of environment and physical security need to work jointly to achieve and to maintain the confidentiality, integrity and availability of information and information processing facilities including telecommunication systems and infrastructure. The environment and physical security also need to protect against cybercrime, fraudulent activities, information loss and other security risks and threats.

I.4.1 Physical and environmental security

a) The organization should ensure that physical and environmental security controls are identified, and these controls are implemented.

b) Physical and environmental security measures should prevent unauthorized physical access, damage and interference to the organization's premises and information.

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

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

e) All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or security overwritten prior to disposal or reuse.

Appendix II

Additional controls for consideration

II.1 CSIRT and SOC

Organizations should consider the establishment of an organizational computer security incident response team (CSIRT) and security operation centre (SOC) to continuously monitor and mitigate security risks, threats and vulnerabilities.

II.2 Cybersecurity information exchange (CYBEX)

Organizations should also consider the adoption of cybersecurity information exchange (CYBEX) techniques to enhance cybersecurity information exchange and infrastructure protection. CYBEX provide structured information exchange for known assurance levels of systems, devices, vulnerabilities, incidents, etc.

The Recommendation ITU-T X.1500 series provides the cybersecurity information exchange specification in detail e.g., threat sharing expression, attack pattern enumeration and malware description format.

Bibliography

[b-ITU-T X.1500] ITU-T X.1500 (2012), *Overview of cybersecurity information exchange*.

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

[b-ISO/IEC 27005] ISO/IEC 27005:2011, *Information technology – Security technique – Information security risk management*.

[b-NIST SP 800-100] NIST SP 800-100 (2006), *Information Security Handbook: A Guide for Managers*.

[b-NIST SP-800-39] NIST SP-800-39 (2011), *Managing Information Security Risk: Organization, Mission, and Information System View*.

[b-NIST SP-800-53] NIST SP-800-53 (2017), *Security and Privacy Controls for Information Systems and Organization, Revision 5*.

[b-Act 709] Act 709 (2010), *Personal Data Protection Act, Malaysia*.

[b-MCMC TC G009] MCMC MTSFB TC G009 (2016), *Requirements of Information and Network Security, Malaysia*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
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, and associated measurements and tests
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, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019