MCMC MTSFB TC G009:XXX

TECHNICAL CODE

INFORMATION SECURITY MANAGEMENT - REQUIREMENTS (SECOND REVISION)

Developed by

Registered by

Registered date:

MCMC MTSFB TC G009:XXXX

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact, Cyber 663000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : (+603) 8680 9950
Fax : (+603) 8680 9940
Email : admin@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Information Security Management Sub Working Group under the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

Digi Telecommunications Sdn Bhd

Digital Nasional Berhad

FNS (M) Sdn Bhd

Maxis Broadband Sdn Bhd

Telekom Malaysia Berhad

U Mobile Sdn Bhd

Universiti Kuala Lumpur

Foreword

This technical code for Information Security Management - Requirements ('this Technical Code') was developed pursuant to the Section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Information Security Management Sub Working Group under the Security, Trust and Privacy Working Group.

Major modifications in this revision are as follows:

a) Change of Technical Code Title – INS (Information and Network Security) to ISM (Information Security Management)

b) Inclusion of the newly develop Information Security Management Framework

c) Replacement of Annex A Content - Normative Security Controls replace with Information Security Risk Management Process

d) Add and update Normative Reference (ISO 27001:2022, ISO 27002:2022, ISO 27005:2022, ISO 27011:2016, TC G021, MY CSC TC G00x, TC G029, TC G00155, TC G020)

e) Reposition of Risk Management Process from Clause 5.2.2 to Annex A

This Technical Code replaces the MCMC MTSFB TC G009:2019, *Information Security Management - Requirements (First Revision)*.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INFORMATION SECURITY MANAGEMENT - REQUIREMENTS

1. Scope

This Technical Code provide requirements for establishing, implementing, maintaining and continually improving Information Security Management (ISM) systems which includes the management of information security risk within the context of an organisation. The requirements set out in this Technical Code are generic and intended to be applicable to all organisations, regardless of size, type or nature.

As a result of implementing this Technical Code, organisations will:

a) be able to ensure the confidentiality, integrity and availability of global telecommunications facilities, services and the information handled, processed or stored within global facilities and services;

b) adopt secure collaborative processes and controls ensuring the lowering of risks in the delivery of telecommunications services;

c) be able to deliver information security in an effective and efficient manner;

d) be able to improve the security culture of organizations, raise staff awareness and increase public trust;

e) adopt a consistent and holistic approach of information security; and

f) facilitate adoption of information security requirement and associated technical codes as depicted below.

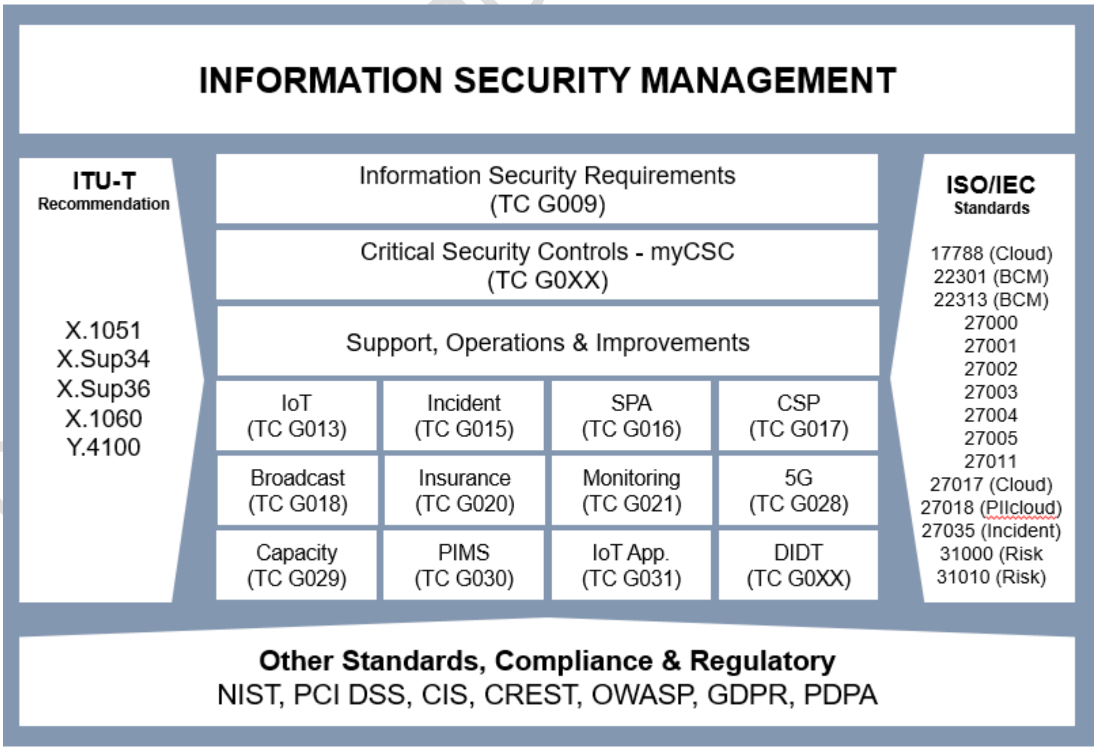

Figure 1. ISM framework

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated reference, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

ISO/IEC 27000:2018 Information technology- Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ISO/IE 27002:2022 Information security, cybersecurity and privacy protection — Information security controls

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

ISO/IEC27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations *(version 2022 under development, to be released in Jun 2023*)

3. Abbreviations

CISO	Chief Information Security Officer
ISM	Information Security Management
IP	Internet Protocol
OWASP	Open Web Application Security Project
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

4. Terms and definitions

For the purposes of this Technical Code, the definition as stated in ISO/IEC 27000 is referred.

5. Information Security Management Organisation Context & Planning

5.1 Organisation context

5.1.1 Understanding context of organisation

The organisation shall determine internal and external issues that are relevant to its purpose and that affects its ability to achieve the intended outcomes of its ISM.

5.1.2 Understanding the expectation of interested parties

The organisation shall determine:

a) interested parties that are relevant to the ISM;

b) the requirements of these interested parties relevant to the ISM; and

c) which requirements will be addressed through the ISM.

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

5.1.3 Determining the scope of Information Security Management (ISM)

The organisation shall determine the boundaries and applicability of the ISM management system to establish its scope. The determination of scope shall take the following into consideration:

a) the internal and external issues referred in 5.1.1;

b) the requirements referred in 5.1.2; and

c) interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations.

The scope shall be available as documented information.

5.1.4 Information Security Management (ISM) methodology

The organisation shall establish, implement, maintain and continually improve an ISM system, in accordance with the requirements of this Technical Code.

5.2 Policy

Organisation leadership shall establish a management framework to initiate and control the implementation of ISM. Management shall approve the ISM policy, assignment of security roles, coordinate and review of the implementation of security across the organisation.

Each policy shall 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 organisation’s policies and approach in managing information security in response to changes to the organisational environment, business circumstances, legal conditions or technical environment.

Top management shall establish an ISM policy that:

a) is appropriate to the purpose of the organisation;

b) includes ISM objectives or provide the framework for setting the ISM objectives;

c) includes a commitment to satisfy applicable requirements related to ISM; and

d) include a commitment to continual improvement of the ISM management system.

The ISM policy shall:

a) be available as documented information;

b) be communicated within the organisation; and

c) be available to interested parties, as appropriate.

5.3 Planning for information security risk management

5.3.1 General

When planning for the ISM management system, the organisation shall consider the issues referred in 5.1.1 and 5.1.2 and determine the following risks and opportunities that need to be addressed:

a) security management system can achieve its intended outcomes;

b) enhance desirable effects;

c) prevent or reduce undesired effects; and

d) achieve continual improvement.

The organisation shall plan the actions to address these risks and opportunities and identify the following items:

a) integrate and implement the actions into its ISM system processes; and

b) evaluate the effectiveness of these actions.

5.3.2 Information security risk management

Guidelines for establishing information security risk management process referred to Annex A.

5.4 Objectives and planning

The organisation shall establish ISM objectives at relevant functions and levels. The ISM objectives shall consider the following items:

a) be consistent with the ISM policy;

b) be measurable (if feasible);

c) take into account applicable ISM requirements and results from risk assessment and risk treatment;

d) be monitored;

e) be consulted and communicated; and

f) be available as documented information and updated as appropriate.

The organisation shall retain documented information on the ISM objectives.

When planning on how to achieve its ISM objectives, the organisation shall determine the following questions:

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.

When the organisation determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

6. Roles and responsibilities

6.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the ISM management by:

a) appointing a Chief Information Security Officer (CISO) or equivalent who is an independent authority and reports to board of directors, that is responsible for the overall ISM for the organisation;

b) ensuring the IS policy and the objectives are established and are compatible with the strategic direction of the organisation;

c) ensuring the integration of the ISM requirements into the organisation's process;

d) ensuring that the resources needed for the ISM system are available;

e) communicating the importance of effective ISM and of confirming to the ISM requirements;

f) ensuring that the ISM system achieves the intended outcomes;

g) directing and supporting persons to contribute the effectiveness of the ISM system;

h) promoting continual improvement; and

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

6.2 Roles, responsibilities within the organisation and authorities

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

Top management shall assign the responsibilities and authority for:

a) ensuring that the ISM conforms to the requirements of this Technical Code; and

b) reporting on the performance of the ISM to top management based on MCMC MTSFB TC G021.

NOTE: Top management may also assign responsibilities and authorities for reporting performance of the ISM within the organisation.

These functions shall be assigned in the applicable organisation:

a) regulatory/ authority contact;

b) ISM responsibility; and

c) risk management.

7. Support

7.1 Resources

The organisation shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the Information Security Management.

7.2 Competence

The organisation shall:

a) determine the necessary competence of persons doing work under its control that affects the performance of ISM;

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 effectiveness of the action taken; and

d) retain appropriate documented information as evidence of competence.

NOTE: Applicable action may include i.e. the provision of training to, the mentoring of, the re-assignment of current employees, the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organisation's control shall be aware of:

a) IS policy;

b) their contribution to the effectiveness of the ISM system, including the benefits of improved ISM performance; and

c) the implications of not conforming to the ISM system.

7.4 Communication

The organisation shall determine the need for internal and external communications relevant to ISM system including:

a) what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who shall communicate; and

e) the process by which communication shall be affected.

7.5 Documented information

7.5.1 General

The organisation’s ISM shall include:

a) documented information required by this Technical Code; and

b) documented information determined by the organisation as being necessary for the effectiveness of the ISM system.

The extent of documented information for an ISM system can differ from one organisation to another due to:

a) size and type of activities, process, products and services of an organisation;

b) the complexity of processes and their interactions; and

c) the competence of the persons.

7.5.2 Creating and updating

When creating and updating documented information, the organisation shall 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.

7.5.3 Control of documented information

Documented information required by the ISM system and by this Technical Code shall 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 organisation shall 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 organisation to be necessary for the planning and operation of the ISM system shall 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.

8. Operations

8.1 Operational planning and control

The organisation shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 5.4 by:

a) establishing criteria for the processes; and

b) implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

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

The organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

The implementation for incident management, security continuity, monitoring and other relevant information security requirements should be referred to the TC as stated in the ISM framework in Figure 1.

8.2 Information security risk

The organisation shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 5.1.2. The organisation shall retain documented information of the results of the information security risk assessments.

The organisation shall implement the information security risk treatment plan. The organisation shall retain documented information of the results of the information security risk treatment. The selection of information security controls from MYCSC (TC G0xx) is dependent upon organisational decisions based on the criteria for information security risk acceptance, risk treatment options and the information security risk management approach applied to all organisations, additionally the selection should be subject to all relevant national and international legislation and regulations.

Management of information security risk assessment and treatment referred to appendix A.

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organisation shall determine:

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

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated;

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results. The organisation shall evaluate the information security performance and the effectiveness of the information security management.

Monitoring and measurement information security referred to MCMC MTSFB TC G021.

9.2 Internal audit

9.2.1 General

The organisation shall conduct internal audits at planned intervals to provide information on whether the information security management:

a) conforms to;

  i) the organisation’s own requirements for its information security management system;

  ii) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organisation shall plan, establish, implement and maintain an audit programmes, including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programmes, the organisation shall consider the importance of the processes concerned and the results of previous audits.

The organisation shall:

a) define the audit criteria and scope for each audit;

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

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

Documented information shall be available as evidence of the implementation of the audit programmes and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organisation's information security management at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the ISM system;

c) changes in needs and expectations of interested parties that are relevant to the ISM system;

d) feedback on the information security performance, including trends in:

   i) nonconformities and corrective actions;

   ii) monitoring and measurement results;

   iii) audit results;

   iv) fulfilment of information security objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management.

Documented information shall be available as evidence of the results of management reviews.

10. Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organisation shall:

a) react to the nonconformity, and as applicable:

   i) Take action to control and correct it.

   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.

   iii) Determining if similar nonconformities exist, 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 security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of:

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

b) the results of any corrective action.

10.2 Continual improvement

The organisation shall continually improve the suitability, adequacy and effectiveness of the ISM.

Annex A
(Normative)

A.1. Risk Management process

The main purpose of the risk management process is to enable the organisation to assess the existing or potential risks that may be faced, evaluate the risks by comparing the risk analysis results with the established risk criteria, and treat such risks using the risk treatment options. The organisation shall use such a process when making decisions.

Figure A.1 shows the steps involved in a risk management process and are as follows:

a) Communication and consultation

b) Context establishment

c) Risk assessment;

   i) Risk identification;

   ii) Risk analysis; and

   iii) Risk evaluation.

c) Risk treatment;

d) Documented information (recording and reporting); and

e) Monitoring and review.

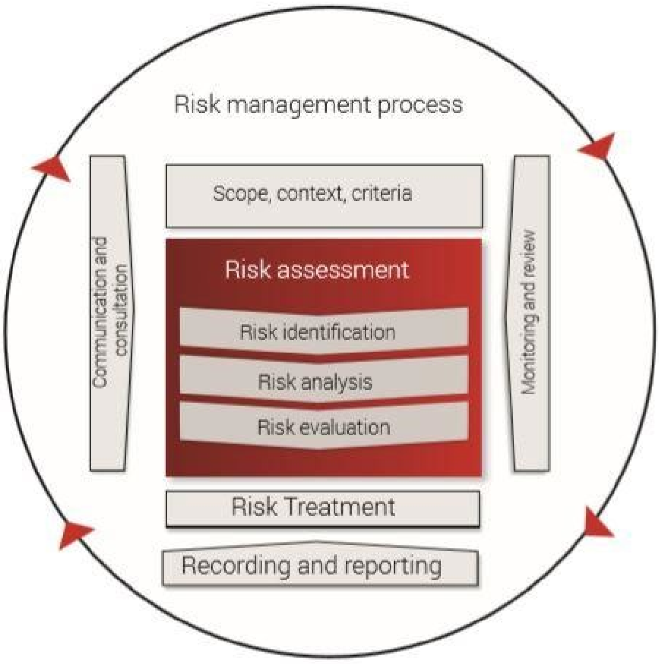

Figure A.1. Risk management process

A.2. Communication and consultation

Proper risk management requires structured and on-going communication and consultation with those affected by the organisation’s operations This should happen at every step of the risk management process, with the relevant interested parties.

The communication seeks to promote awareness and understanding of risk and the means to respond to it. Risk communication should be carried out to:

a) provide assurance of the outcome of the organisation’s risk management;

b) collect risk information;

c) share the results from the risk assessment and present the risk treatment plan;

d) avoid or reduce both the occurrence and consequence of information security breaches due to the lack of mutual understanding among risk owners and interested parties;

e) support risk owners;

f) obtain new information security knowledge;

g) coordinate with other parties and plan responses to reduce the consequences of any incident;

h) give a sense of responsibility to risk owners and other parties with a legitimate interest at risk; and

i) improve awareness.

Consultation involves obtaining feedback and information to support decision-making. Some of the objectives of the consultation activities are as follows:

a) bringing different areas of expertise together for each step of the risk management process;

b) ensuring different views are considered when defining risk criteria and evaluating risks;

c) providing sufficient information to facilitate risk oversight and decision-making; and

d) building a sense of inclusiveness and ownership among those affected by risk.

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

A.3. Context establishment

When establishing the context, the organisation shall take into account the organisation’s external context (political, social, etc.) and internal context (objectives, strategies, structures, ethics, discipline, etc.) for the management of information security risks.

The organisation’s context must be understood before the full range of risks can be identified, assessed and treated.

The key steps involved in establishing the organisation’s context for risk management would involve:

a) Organisational considerations such as risk appetite (defined as the amount of risk an organisation is willing to pursue or accept), risk owners and their responsibilities.

b) Identifying basic requirements of interested parties as well as the status of compliance with these requirements.

c) Applying risk assessment within many different processes such as project management, incident management, vulnerability management or even when they are required on an adhoc basis.

d) Establishing and maintaining information security risk criteria which should include:

   i) the risk acceptance criteria - used to determine whether a risk is acceptable or not, defined based on the risk appetite; and

   ii) criteria for performing information security risk assessments which specifies how the significance of a risk is determined in terms of its consequences, likelihood and level of risk.

e) Choosing the appropriate risk management method to ensure consistency, comparable results when performed for different risks and produces results that are as close as possible with reality.

A.4. Information security risk assessment process

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

A.4.1. Risk identification

Risk identification is about the creation of a comprehensive list of risks (both internal and external) that the organisation faces, and can involve input from sources such as historical data, theoretical analysis, expert options, and stakeholder's needs.

The identification of risks shall be a formal, structured process that includes risk sources, events, their causes and their potential consequences.

The organisation shall establish and maintain security risk criteria that includes:

a) the risk acceptance criteria; and

b) criteria for performing ISM risk assessment.

The organisation shall ensure that repeated information security risk assessments produce consistent, valid and comparable results.

The organisation shall identify ISM risks by:

a) applying the ISM risk assessment process to identify risks associated with the confidentiality, integrity and availability for information within the scope of the ISM management system; and

b) identifying risk owners.

A.4.2. Risk analysis

The organisation shall analyse each risk that was identified in the 5.2.5.1. Based on the level of risk that is determined after the risk analysis, the organisation is able to define whether the risk is acceptable or not. As so, if the risk turns out to be unacceptable, the organisation can take actions to modify the risk to correspond to the acceptable level of risk.

The organisation shall use a formal technique to consider the consequence and likelihood of each risk, and these techniques can be qualitative, semi-quantitative, quantitative, or a combination thereof, based on the circumstances and the intended use.

Analyse the ISM risks includes:

a) assess the potential consequences (impact) that would result if the risks identified materialise;

b) assess the realistic likelihood of the occurrence of the risks identified; and

c) determine the level of risks.

A.4.3. Risk evaluation

This step offers the organisation the opportunity to have a mechanism that helps them rank the relative importance of each risk, so that a treatment priority can be established.

Evaluate the ISM risks:

a) compare the result of risk analysis with the risk criteria established in 5.2.4; and

b) prioritise analysed risk for risk treatment.

A.5. Risk treatment

The organisation shall define and apply an ISM risk treatment process to:

a) select appropriate ISM risk treatment options, taking account of the assessment result;

NOTE: There are 4 options available for risk treatment options: risk modification, risk retention, risk avoidance and risk sharing.

b) determine all controls that are necessary to implement the ISM risk treatment option(s) chosen;

NOTE: Organisations can design controls as required or identify them from MCMC MTSFB TC G0xx (MYCSC) or any source.

c) formulate an ISM risk treatment plan; and

d) obtain risk owner’s approval of the ISM risk treatment plan and acceptance of the residual ISM risk.

A.6. Documented information

The organisation shall retain documented information about the ISM risk assessment and risk treatment processes.

Documented information about the risk assessment process should contain:

a) a definition of the risk criteria (including the risk acceptance criteria and the criteria for performing information security risk assessments).

b) reasoning for the consistency, validity and comparability of results.

c) a description of the risk identification method (including the identification of risk owners)

d) a description of the method for analysing the information security risks (including the assessment of potential consequences, realistic likelihood and resultant level of risk)

e) a description of the method for comparing the results with the risk criteria and the prioritisation of risks for risk treatment

Documented information about the information security risk treatment process should contain descriptions of:

a) the method for selecting appropriate information security risk treatment options

b) the method for determining necessary controls and identification of the necessary controls

c) where appropriate and available, evidence that these necessary controls act to modify risks, so as to meet the organisation's risk acceptance criteria

d) the method used to determine that necessary controls have not been inadvertently overlooked

e) how risk treatment plans are produced

f) how risk owners' approval is obtained

Documented information about the information security risk assessment results should contain:

a) the identified risks, their consequence and likelihood

b) the identity of the risk owner(s)

c) the results of applying the risk acceptance criteria

d) the priority for risk treatment.

A.7. Monitoring and review

Organisation shall monitor and review the risk treatment plan by:

a) examining the progress of treatment plans; and

b) monitoring the established controls and their effectiveness.

Monitoring and reviewing factors influencing risks such as value of assets, consequences, threats, vulnerabilities, likelihood of occurrence; to identify any changes in the context of the organisation at an early stage, and to maintain an overview of the complete risk picture.

Bibliography

[1] ITU-T X.1051, ISO/IEC 27011, *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations*.

[2] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*.

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

[4] ISO/IEC 27005, *Information technology - Security technique - Information security risk management*.

[5] NIST SP 800-37 Rev.2, *Risk Management Framework for Information System and Organisations: A System Life Cycle Approach for Security and Privacy*.

[6] NIST SP-800-39, *Managing Information Security Risk: Organisation, Mission, and Information System View*.

[7] NIST SP-800-53, *Security and Privacy Controls for Information Systems and Organisation, Revision 5*.

[8] NIST SP 800-100, *Information Security Handbook: A Guide for Managers*.

[9] Centre for Internet Security (CIS), *Critical Security Controls 20 V7.0*.

[10] *Personal Data Protection Act*, 2010.

Acknowledgements

Members of the Information Security Management Sub Working Group

Ms Azrina Ibramsha (Chair/Draft Lead)	Telekom Malaysia Berhad
Ms Rafeah Omar (Vice Chair)	Telekom Malaysia Berhad
Mr Khairul Ekhwan Kamarudin (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Thaib Mustafa/ Mr Radhilutfi Madehi	FNS (M) Sdn Bhd
Dr Amna Saad	Universiti Kuala Lumpur
Mr Mohd Hafiz Mat Tabrani	Cybersecurity Malaysia
Mr Yasdy Md Yasin	Maxis Broadband Sdn Bhd
Mr Navinkumar Palani Velu	Digital Nasional Berhad
Mr Parag Barua	Digi Telecommunications Sdn Bhd
Mr Myke Chia	U Mobile Sdn Bhd

By invitation:

Ts Nurul Husna Mohamad Kasim	Jabatan Penyiaran Malaysia