TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - MONITORING AND MEASUREMENT OF SECURITY CONTROL OBJECTIVES

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

4 October 2019

MCMC MTSFB TC G021:2019

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)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Committee representation

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

Celcom Axiata Berhad

CyberSecurity Malaysia

Digi Telecommunications Sdn Bhd

KPMG Management & Risk Consulting Sdn Bhd

Maxis Bhd

Measat Broadcast Network Systems Sdn Bhd

MIMOS Berhad

Ministry of Energy, Science, Technology, Environment and Climate Change

Multimedia University

Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia

Telekom Applied Business Sdn Bhd

Telekom Malaysia Bhd

U Mobile Sdn Bhd

Universiti Kuala Lumpur

Universiti Tenaga Nasional

VLAN Technology Sdn Bhd

webe digital sdn bhd

Foreword

This technical code for Information and Network Security - Monitoring and Measurement of Security Control Objectives ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Security, Trust and Privacy Working Group.

This Technical Code is an extension to the document MCMC MTSFB TC G009.

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

INFORMATION AND NETWORK SECURITY - MONITORING AND MEASUREMENT OF SECURITY CONTROL OBJECTIVES

0. Introduction

MCMC MTFSB TC G009 is a Technical Code that has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an Information Security and Network Security (INS) management system within the context of an organisation.

Referring to MCMC MTSFB TC G009, the organisation shall determine the following list when planning to achieve its INS objectives.

a) What will be done?

b) What resources will be required?

c) Who will be responsible?

d) When it will be completed?

e) How the results will be evaluated?

MCMC MTSFB TC G009 also requires the organisation to retain documented information on the INS objectives. Monitoring and measurement are the first step in a process to evaluate performance and effectiveness of security controls.

Monitoring determines the status of a system, a process or an activity in order to meet a specified information need. Measurement is an activity undertaken to determine a value, status or trend in the performance or effectiveness to help identify potential improvement needs. Measurement can be applied to any processes, activities, controls and group of security controls.

The selection of appropriate measurement and effectiveness tests to be performed can be referred to in this Technical Code.

This Technical Code is designed to be used by organisation in:

a) establishing security objectives aligned with the business objectives;

b) developing metrics to monitor the implementation of security controls;

c) evaluating and measuring the effectiveness of security controls;

d) benchmarking or rating the overall security posture of the organisation; and

e) continually improving the INS of the organisation.

1. Scope

This Technical Code provides the appropriate Monitoring and Measurement of Security Control Objectives (MMSCO) as well as provide mechanisms to review and consider improvement initiatives for the existing security controls in order to fulfil the requirements of MCMC MTSFB TC G009.

2. Normative references

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

MCMC MTSFB TC G009, *Requirements for Information and Network Security*

ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*

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

ISO/IEC 27004, *Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation*

Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers, ENISA

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

BCM	Business Continuity Management
BCMS	Business Continuity Management System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CITO	Chief Information and Technology Officer
CTO	Chief Technology Officer
DR	Disaster Recovery
HR	Human Resource
INS	Information and Network Security
ISMS	Information Security Management System
ITD	Information Technology Department
KPI	Key Performance Indicator
MMSCO	Monitoring and Measurement of Security Control Objectives
N/A	Not Applicable
NC	Non-Compliance
SLA	Service Level Agreement
SOP	Standard Operating Procedures
VA	Vulnerability Assessment
PIN	Personal Identification Number

4. Terms and definitions

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

4.1 Frequency

How frequently the data to be collected and reported. There can be a reason for having multiple frequencies.

4.2 Implementation evidence

An evidence that validates the measurement performed. It helps identify possible causes of poor results and provides input to the process. In other words, it is a data that provide input into the formula.

4.3 Justification

To clarify the purpose of setting up such control.

4.4 Measurement

Statement of measurement, generally described using a word such as “percentage”, “number”, “frequency” and “average”.

4.5 Objective

Statement of an intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.

Note: Objectives may also be described as control objectives.

4.6 Performance evaluation

A method of the measure be evaluated, calculated or scored.

4.7 Performance indicator

A method to interpret the performance.

4.8 Responsible parties

The person responsible for gathering and processing the measure.

4.9 Target

Desired result of the measurement, e.g. a milestone or statistical measure or a set of thresholds.

Note: Ongoing monitoring can be required to ensure continued attainment of the target.

5. Structure and overview

This Technical Code is structured to follow the 4 categories of controls (as depicted in Annex A of MCMC MTSFB TC G009) as follows:

a) organisation;

b) infrastructure;

c) people; and

d) environment.

5.1 Clauses

The order of the clauses in this Technical Code does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, therefore each organisation applying this Technical Code shall identify applicable controls, how important these are and their application to individual business processes.

5.2 Security control categories

Each main security control categories contains implementation guidance and example of control and its metrics that can be applied by the organisation.

5.3 Security control measure

For each of security control category, this Technical Code provides monitoring and control measures, metrics and thresholds for organisation when developing the security controls.

The performance metric is calculated based on 4 categories of controls as in Clause 5 is represented in the MMSCO radar chart below.

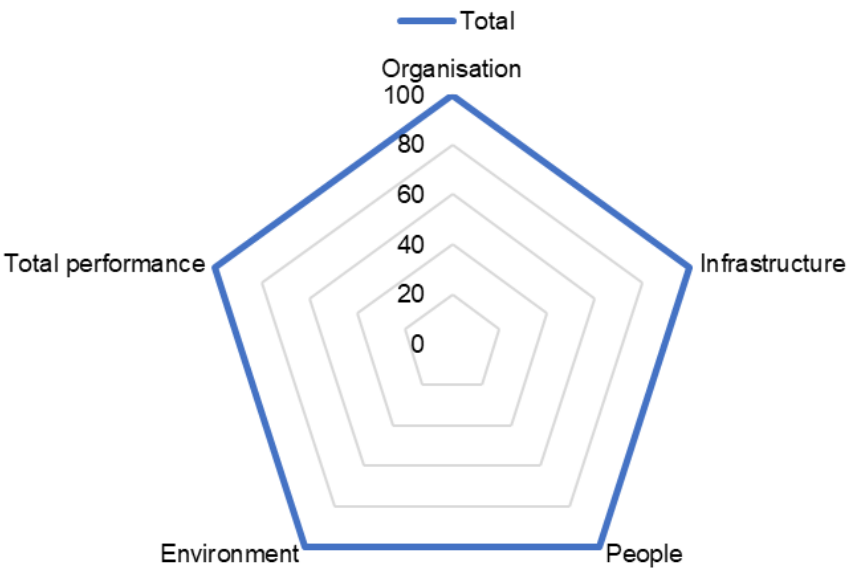

Figure 1. MMSCO radar chart of performance metrics

The metrics tables are regrouped depending on the defined controls categories as follows:

a) organisation: 7 metrics tables;

b) infrastructure: 10 metrics tables;

c) people: 3 metrics tables; and

d) environment: 1 metrics table.

The proposed coefficients of total performance for each control's categories are as follows:

a) organisation: 40 %;

b) infrastructure: 40 %;

c) people: 15 %; and

d) environment: 5 %.

For each of the categories, several metrics are to be measured and the composition score will become the performance score of that category. The sample of the calculation is demonstrated in Annex A. The organisation shall achieve 80% for the overall performance score.

The metrics for controls categories is summarised in the following lists.

a) Organisation

   i) INS and Business Continuity Management (BCM) policies review (see Table B.1).

   ii) INS and BCM awareness session attended (see Table B.2).

   iii) BCM simulation and testing (see Table C.1).

   iv) INS compliance audit (see Table D.1).

   v) Identify critical information (see Table D.2).

   vi) Information security organisation (see Table D.3).

   vii) Information security incident handling management (see Table E.1).

b) Infrastructure

   i) Asset management audit (see Table F.1).

   ii) Storage media management (see Table G.1).

   iii) Access control (see Table H.1).

   iv) Access management and review (see Table I.1).

   v) Malicious software protection coverage (see Table J.1).

   vi) Detection, prevention and recovery controls (see Table J.2).

   vii) Critical system centralised logging (see Table K.1).

   viii) Security event log review (see Table K.2).

   ix) Vulnerabilities Assessment (VA) (see Table L.1).

   x) Information backup and restoration (see Table M.1).

c) People

i) Human Resource (HR) security (see Table N.1).

ii) Information security professional development (see Table O.1).

iii) Supplier relationship (see Table P.1).

d) Environment

i) Physical security (see Table Q.1).

6. Organisation

This clause provides guidance on the monitoring and measurement of security controls within the INS framework related to organisational readiness. Organisations shall have a formal and systematic approach to implementing and maintaining an effective INS programme.

6.1 Information and Network Security (INS) policy

The objective of the policies is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

The organisation shall develop, approve and publish a set of policies for information security and it shall be communicated to employees and relevant external parties.

The monitoring and measurement for each category can be found in the Annex B, where it covers the table metrics below.

a) INS and BCM policies review (see Table B.1)

b) INS and BCM awareness session attended (see Table B.2)

6.2 Business Continuity Management (BCM)

The objectives of having the BCM are to identify critical operations and risks, provide a plan to maintain or restore critical operations during a crisis, and create a plan to communicate with key people during the crisis. The organisation shall embed the INS continuity in the organisation's Business Continuity Management Systems (BCMS).

The monitoring and measurement for each category can be found in the Annex C, where it covers the table metric for BCM on the simulation and testing (see Table C.1).

6.3 Information and Network Security (INS) compliance

The objective of this control category is to avoid breaches of legal, statutory, regulatory or contractual obligations related to INS and of any security requirements. The organisation shall establish and maintain a policy for checking and enforcing the compliance of internal policies against the identified legal requirements and industry best practices and standards, where these policies are reviewed on a regular basis.

If the organisation conducts business in other countries, managers shall consider compliance in all relevant countries. The specific controls and individual responsibilities to meet these requirements shall also be defined and documented.

The monitoring and measurement for each category can be found in the Annex D, where it covers the following table metrics.

a) INS compliance audit (see Table D.1).

b) Identify critical information (see Table D.2).

c) Information security organisation (see Table D.3).

6.4 Information security incident management

The objectives for effective information security incident management is to ensure service operation is restored as quickly as possible with minimum adverse impact on business operation. To ensure this, the organisation shall establish Service Level Agreement (SLA) that defines clearly objective, scope, task and its process flow.

The monitoring and measurement for Information security incident management as in Annex E.

7. Infrastructure

The clause provides guidance on the monitoring and measurement of security controls within the INS framework related to asset and infrastructure management. Organisations shall have a formal and systematic approach to manage end to end security requirements in their operations, acquisition, development, service delivery, maintenance and support.

7.1 Asset management

The objective of having asset management is to identify organisational assets and define appropriate protection responsibilities. To ensure the objective is achieved, the organisation shall ensure on the following items.

a) Identify the assets associated with information and information processing facilities and drawn up and maintained an inventory of these assets.

b) Identify the assets relevant in the lifecycle of information and document their importance. The lifecycle of information shall include creation, processing, storage, transmission, deletion and destruction. Documentation shall be maintained in dedicated or existing inventories as appropriate.

c) The asset inventory shall be accurate, up to date, consistent and aligned with other inventories.

The monitoring and measurement for asset management audit can be found in Annex F.

7.2 Information management

The objective for effective information management is to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation. To ensure the objective is achieved, the organisation shall ensure on the following items.

a) To classify the information in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

b) To develop and implement an appropriate set of procedures for information labelling in accordance with the information classification scheme adopted by the organisation.

c) To have an appropriate classification label for the output from systems containing information that is classified as being sensitive or critical.

The monitoring and measurement for information management is as in Table D.2, and for media management as in Annex G.

7.3 Access control

The objective of this control category is to limit access to information and information processing facilities. To ensure the objective is achieved, the organisation shall ensure on the following items.

a) To establish, document and review the access control policy based on business and information security requirements.

b) The asset owner to determine the appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

c) To provide the users and service providers a clear statement of the business requirements to be met by access controls by considering both logical and physical access controls.

d) To provide users with access to the network and network services that they have been specifically authorised to use.

The monitoring and measurement for access control is as in Annex H.

7.4 User access management

The objective of effective user access management is to ensure authorised user access and to prevent unauthorised access to systems and services. The organisation shall ensure that a formal user registration and de-registration process be implemented to enable assignment of access rights.

Selection of monitoring and measurement for user access management as in Annex I.

7.5 Malicious software protection

The objective for having malicious software protection is to ensure that information and information processing facilities are protected against malware. The organisation shall ensure that the detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

The monitoring and measurement for each category can be found in the Annex J, where it covers the following table metrics.

a) Malicious software protection coverage (see Table J.1).

b) Detection, prevention and recovery controls (see Table J.2).

7.6 Logging and monitoring

The objective of this control category is to record events and generate evidence.

The organisation shall produce, store and regularly review the event logs that record user activities, exceptions, faults and information security events. Event logging sets the foundation for automated monitoring systems, which are capable of generating consolidated reports and alerts on system security.

The monitoring and measurement for logging and monitoring as in Annex K, where it covers the following table metrics.

a) Critical system centralised logging (see Table K.1).

b) Security event log review (see Table K.2).

7.7 Technical vulnerability management

The objective of effective technical vulnerability management is to prevent exploitation of technical vulnerabilities.

The organisation shall ensure that information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. A current and complete inventory of assets is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organisation responsible for the software.

The monitoring and measurement of technical vulnerability management as in Annex L.

7.8 Backup

The objective of this control category is to protect against loss of data. To achieve the objective, the organisation shall ensure on the following items.

a) Backup copies of information, software and system images to be taken and tested regularly in accordance with an agreed backup policy.

b) To establish a backup policy to define the organisation's requirements for backup of information, software and systems.

c) To define the retention and protection requirements for the backup policy.

d) To provide an adequate backup facility to ensure that all essential information and software can be recovered following a disaster or media failure.

The monitoring and measurement for information backup are details in Annex M.

8. People

This clause provides guidance on the selection of measurement and effectiveness tests for applicable controls within the INS framework related to people. Organisations shall have a formal and systematic approach to ensure that employees, contractors and suppliers are aware of their security responsibilities and maintain compliance to security policies and procedures.

8.1 Screening

The objective of the control category is to ensure individual who is hired for a specific information security role has the necessary competence to perform the security role and can be trusted to take on the role, especially if the role is critical for the organisation.

Verification shall take into account all relevant privacy, protection of personally identifiable information and employment legislation, and shall, where permitted, include the following items:

a) availability of satisfactory character references, e.g. one business and one personal;

b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;

c) confirmation of claimed academic and professional qualifications;

d) independent identity verification (passport or similar document); and

e) more detailed verification, such as credit review (insolvency) or review of criminal records.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and, in particular, if these are handling confidential information, e.g. financial information or highly confidential information, the organisation shall also consider further, more detailed verifications.

Procedures shall define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out.

A screening process shall also be ensured for contractors. In these cases, the agreement between the organisation and the contractor shall specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

Information on all candidates being considered for positions within the organisation shall be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates shall be informed beforehand about the screening activities.

The monitoring and measurement for HR security as in Annex N.

8.2 Awareness, education and training

The objective of an information security awareness programme is to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

To achieve the objective, the organisation shall ensure the following items.

a) To establish an information security awareness programme in line with the organisation's information security policies and relevant procedures. This is by taking into consideration the organisation's information to be protected and the controls that have been implemented to protect the information.

b) To include a number of awareness-raising activities such as campaigns and issuing booklets or newsletters in the awareness programme.

c) To plan the awareness programme by taking into consideration the employees' roles in the organisation, and, where relevant, the organisation's expectation of the awareness of contractors.

d) To schedule the awareness programme over time, preferably regularly, so that the activities are repeated and cover new employees and contractors.

e) To update the awareness programme regularly so it stays in line with organisational policies and procedures, and shall be built on lessons learnt from information security incidents.

f) To perform the awareness training performed as required by the organisation's information security awareness programme. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others.

Information security education and training shall take place periodically. Initial education and training apply to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and shall take place before the role becomes active.

The organisation shall develop the education and training programme in order to conduct the education and training effectively. The programme shall be in line with the organisation's information security policies and relevant procedures, taking into consideration the organisation's information to be protected and the controls that have been implemented to protect the information. The programme shall consider different forms of education and training, e.g. lectures or self-studies.

The monitoring and measurement for information security professional development as in Annex O.

8.3 Disciplinary process

The objective of disciplinary process is to ensure correct and fair treatment for employees who are suspected of committing breaches of information security. To achieve the objective, the organisation shall ensure the following items.

a) Not to commence the disciplinary process without prior verification that an information security breach has occurred.

b) To provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

c) To be used as a deterrent to prevent employees from violating the organisation's information security policies and procedures and any other information security breaches. Deliberate breaches may require immediate actions.

The monitoring and measurement as in Annex N.

8.4 Supplier relationships

The objective is to assess level of supplier's performance against the agreed Key Performance Indicator (KPI) and SLA. The reviews are a key component of supplier performance management, which seeks to measure and monitor the performance of suppliers in reducing costs, mitigating risks and driving continuous improvement.

Monitoring of supplier performance will help organisation, among others in:

a) observing compliance of supplier performance with agreed KPIs and SLAs;

b) identifying performance gaps and areas where they fail to meet expectations;

c) pre-empting issues that lead to underperformance; and

d) identifying required actions when dealing with performance failures.

The monitoring and measurement for supplier relationship as in Annex P.

9. Environment

This clause provides guidance on the monitoring and measurement of security controls within the INS framework related to environment. Organisations shall have a formal and systematic approach to ensure that physical security controls are implemented for information processing and storage facilities.

9.1 Physical and environmental security

The objective of this security control category is to prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

The organisation shall ensure the following items.

a) The date and time of entry and departure of visitors shall be recorded, and all visitors shall be supervised unless their access has been previously approved. Visitors shall only be granted access for specific, authorised purposes and shall be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors shall be authenticated by an appropriate means.

b) Access to areas where confidential information is processed or stored shall be restricted to authorised individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret Personal Identification Number (PIN).

c) A physical log book or electronic audit trail of all access shall be securely maintained and monitored.

d) All employees, contractors and external parties shall be required to wear some form of visible identification and shall immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.

e) External party support service personnel shall be granted restricted access to secure areas or confidential information processing facilities only when required; this access shall be authorised and monitored.

f) Access rights to secure areas shall be regularly reviewed and updated, and revoked when necessary.

The monitoring and measurement for physical security as in Annex Q.

Annex A
(informative)

Calculation of performance evaluation

A.1. Evaluation scale and coefficient controls

All metrics are measured using scale 1 to 5 as in the performance evaluation formula and performance indicator. The proposed weightage to calculate the total performance are as follows:

a) organisation: 40 %;

b) infrastructure: 40 %;

c) people: 15 %; and

d) environment: 5 %.

A.2. Performance evaluation formula

The calculation of performance evaluation is as the following steps.

a) Step 1: Find the Organisation points (refer formula below).

$$Organisation\ points = \frac{\sum\ (B.1 + B.2 + C.1 + D.1 + D.2 + D.3 + E.1)}{7\ metrics\ tables \times 5\ points} \times 40$$

b) Step 2: Find the Infrastructure points (refer formula below).

$$Infrastrucure\ points = \frac{\sum\ (F.1 + G.1 + H.1 + I.1 + J.1 + J.2 + K.1 + K.2 + L.1 + M.1)}{10\ metrics\ tables \times 5\ points} \times 40$$

c) Step 3: Find the People points (refer formula below).

$$People\ points = \frac{\sum\ (N.1 + O.1 + P.1)}{3\ metrics\ tables \times 5\ points} \times 15$$

d) Step 4: Find the Environment points (refer formula below).

$$Environment\ points = \frac{Q.1}{5\ points} \times 5$$

e) Step 5: Calculate the total points (refer formula below).

$$Total\ performance\ evaluation\ points = \sum points\ (Organisation + Infrastructure + Environment + People)$$

The Table A.1 shows the example of performance evaluation been calculated.

Table A.1. Example of performance evaluation

Category of controls	Annex	Metrics table	Points	Category of controls points
Organisation (40 %)	B	B.1	5	$\frac{5+5+5+5+5+4+4}{7\times 5}\times 40$ $\frac{33}{35}\times 40 = 37.71\ points$
		B.2	5	
	C	C.1	5	
	D	D.1	5	
		D.2	5	
		D.3	4	
	E	E.1	4	
Infrastructure (40 %)	F	F.1	4	$\frac{4+5+5+4+5+5+5+5+5+5}{10\times 5}\times 40$ $\frac{48}{50}\times 40 = 38.40\ points$
	G	G.1	5	
	H	H.1	5	
	I	I.1	4	
	J	J.1	5	
		J.2	5	
	K	K.1	5	
		K.2	5	
	L	L.1	5	
	M	M.1	5	
People (15 %)	N	N.1	4	$\frac{4+4+4}{3\times 5}\times 15$ $\frac{12}{15}\times 15 = 12.00\ points$
	O	O.1	4	
	P	P.1	4	
Environment (5 %)	Q	Q.1	4	$\frac{4}{5}\times 5 = 4.00\ points$
Total performance evaluation points (%)				$37.71 + 38.40 + 12.00 + 4.00 = 92.11\ \%$

The overall performance evaluation is presented in radar chart as in Figure A.1.

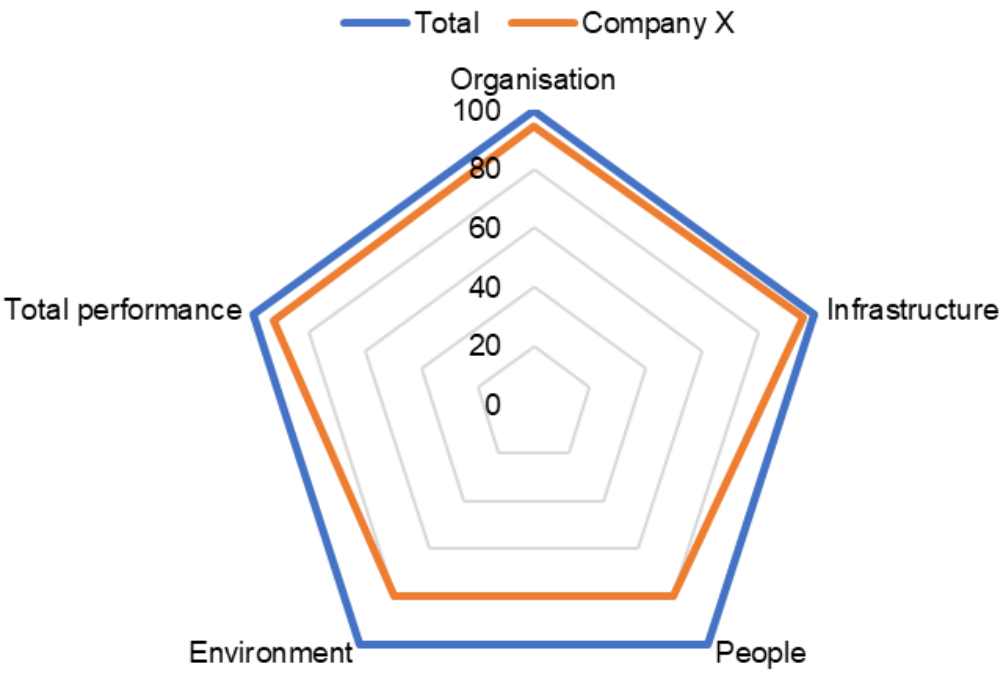

Figure A.1. Example of radar chart for overall performance evaluation

Annex B
(normative)

Monitoring and measurement of Information and Network Security (INS) and Business Continuity Management (BCM) policies

Table B.1. INS and BCM policies review

Information	Description
Objective	To evaluate whether the policies for INS and BCM are reviewed at planned intervals or if significant changes occurred.
Justification	To ensure suitability towards the dynamic landscape of business, appropriateness/ adequacy based on current technologies and effectiveness of controls and requirements.
Measurement	Policy and Standard Operating Procedures (SOP) exist and reviewed at planned intervals or if significant changes occur.
Performance evaluation	The policy should be reviewed as per agreed by the management. $\frac{\text{Number of policy and SOP reviewed}}{\text{Total number of policies and SOPs}} \times 100$
Target	100 % policy and SOP conformance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) Minutes of Meeting and record of management review. b) Document listing indicating date of last review. c) Document history that mentioning review of document.
Frequency	As per policy.
Responsible parties	a) Information Security Management System (ISMS) manager; or b) Internal auditor; or c) Chief Information Security Officer (CISO) or equivalent.

Table B.2. INS and BCM awareness session attended

Information	Description
Objective	To communicate the INS and BCM policy to employees and relevant stakeholders.
Justification	a) To help employees and relevant stakeholders understand the importance of INS and BCM, and how it benefits them in their daily works. b) To ensure employees and relevant stakeholders are aware about the security policy as ignorance and lack of understanding are major contributor to security breaches.
Measurement	% of employees and stakeholders that participate in awareness sessions.
Performance evaluation	The relevant employees and stakeholders should participate at least one session per latest version. $\frac{\text{Number of participation}}{\text{Total number of employees and stakeholders}} \times 100$
Target	100 % participation for INS and BCM awareness sessions.

Performance indicator	The final performance is calculated based on the average of INS and BCM awareness score. It should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) Document listing on the communications. b) Document history that mentioning about the communications. c) Minutes of Meeting of management review.
Frequency	As per policy.
Responsible parties	a) Information Security Governance; b) BCM Manager; or c) HR or equivalent.

Annex C
(normative)

Monitoring and measurement of Business Continuity Management (BCM)

Table C.1. BCM simulation and testing

Information	Description
Objective	To ensure simulation and testing for BCM and/or Disaster Recovery (DR) plans are conducted periodically.
Justification	To ensure BCM and/or DR plans are valid and effective during an adverse situation.
Measurement	Simulations or test conducted as planned.
Performance evaluation	$\frac{\text{Number of simulation and testing conducted}}{\text{Number of simulation and testing planned}} \times 100$
Target	100 % BCM and/or DR plans were conducted.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) Documented information e.g., findings, test results. b) Report from management review.
Frequency	As per stated in organisation scheduled/as per BCM policy. For critical system, the simulation shall be successfully tested at least twice a year.
Responsible parties	a) BCM Manager. b) Internal audit. c) CISO or equivalent.

Annex D
(normative)

Monitoring and measurement of Information and Network Security (INS) compliance

Table D.1. INS compliance audit

Information	Description
Objective	To measure the level of compliance.
Justification	To avoid breaches of legal, statutory, regulatory or contractual obligations related to INS and of any security requirements.
Measurement	INS compliance audit conducted as planned.
Performance evaluation	$\frac{\text{Number of internal audit conducted}}{\text{Number of internal audit planned}} \times 100$
Target	100 % compliance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	Audit programme documented information, e.g. audit plan, audit attendance list, audit report.
Frequency	Annually.
Responsible parties	Top management.

Table D.2. Identify critical information

Information	Description
Objective	To identify and classify critical information in an organisation.
Justification	To avoid breaches of legal, statutory, regulatory or contractual obligations related to INS and of any security requirements.
Measurement	Critical data inventory is updated at least once a year.
Performance evaluation	N/A.
Target	Data inventory exist and up-to-date.
Performance indicator	Performance should be interpreted as follows: a) Data inventory exist and up-to-date = 5 points; b) Data inventory exist not up-to-date = 3 points; and c) Data inventory non-existent = 1 point.
Implementation evidence	Data inventory report.
Frequency	Annually.
Responsible parties	Data Owner.

Table D.3. Information security organisation

Information	Description
Objective	To assess the effectiveness of information security organisation.
Justification	To establish a management framework to initiate and control the implementation of information security.
Measurement	Regular review of information security performance and reports.
Performance evaluation	N/A.
Target	Approved management report.
Performance indicator	Performance should be interpreted as follows: a) annual review = 5 points; b) bi-annual review = 3 points; and c) tri-annual review = 1 point.
Implementation evidence	Documented information.
Frequency	Annually.
Responsible parties	Top management.

Annex E
(normative)

Monitoring and measurement of incident management

Table E.1. Information security incident management

Information	Description
Objective	To assess the effectiveness of information security incident management.
Justification	To obtain level of effectiveness for continuous improvement.
Measurement	SOP exist for incident identification, notification, escalation, containment and mitigation in target timeframe: a) define target response timeframes for different security incident categories; b) define target resolution timeframes for each security incidents; and c) define indicator thresholds for security incidents exceeding the timeframe stated in b).
Performance evaluation	% of information security incidents not resolve within SLA. $\frac{\text{Number of incident not resolved within SLA}}{\text{Number of security incident}} \times 100$
Target	95 % conformance.

Performance indicator	Performance should be interpreted as follows:
	a) more than 90 % = 5 points;
	b) more than 80 % = 4 points;
	c) more than 70 % = 3 points;
	d) 60 % = 2 points; and
	e) 50 % = 1 point.

Implementation evidence	SOP documented information.
Frequency	As per define by the organisation.
Responsible parties	CISO or equivalent.

Annex F
(normative)

Monitoring and measurement of asset management

Table F.1. Asset management audit

Information	Description
Objective	To control and maintain the availability of incoming, storing, movement and issuing of fixed and digital assets.
Justification	Assets pertaining to information and processing are identified and maintained in an inventory.
Measurement	Regular update of inventory records in terms of: a) hardware; b) software; c) IP addresses; d) asset locations; e) URL, hostname/computer name, domain or workgroup; and f) asset owners.
Performance evaluation	The accuracy of assignment of the assets.
Target	Record exists and up-to-date.
Performance indicator	Performance should be interpreted as follows: a) data exist and up-to-date = 5 points; b) data exist not up-to-date = 3 points; and c) data non-existent = 1 point.
Implementation evidence	Documented information.
Frequency	Record updated annually.
Responsible parties	Asset management team or equivalent.

Annex G
(normative)

Monitoring and measurement of information management

Table G.1. Storage media management

Information	Description
Objective	To ensure that the procedures for the full life cycle of a storage media based on the classification criteria (e.g. critical, non-critical) are implemented and shall be protected against unauthorized access, misuse or corruption.
Justification	To ensure the storage media life cycle management is handled according to the policy.
Measurement	SOP for storage media life cycle management is available which includes: a) media protection including hardware and software; b) encryption or access control for media intended to handle sensitive information; and c) disposal management.
Performance evaluation	$\frac{\text{Total number of storage media fulfilled the SOP requirement}}{\text{Total number of storage media}} \times 100$
Target	100 % SOP conformance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) SOP documentation. b) Disposal record.
Frequency	Annually.
Responsible Parties	a) Chief Information and Technology Officer (CITO); or b) Chief Information Officer (CIO); or c) Chief Technology Officer (CTO); or d) Head of Information Technology Department (ITD) or equivalent.

Annex H
(normative)

Monitoring and measurement of access control

Table H.1. Access control

Information	Description
Objective	To ensure that access to information, network and services are provided only for those who have been specifically authorised to do so.
Justification	To avoid unauthorised access to information, network and services.
Measurement	Policy and SOP exist to regularly review user access.
Performance evaluation	$\frac{\text{Number of review for user access}}{\text{Number of user access review planned}} \times 100$
Target	100 % policy and SOP conformance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) Policy and SOP documentation. b) Review report.
Frequency	Quarterly.
Responsible parties	a) CITO. b) CISO. c) HR manager. d) Relevant parties.

Annex I
(normative)

Monitoring and measurement of user access management

Table I.1. Access management and review

Information	Description
Objective	To ensure proper access rights for re-designated, resigned and terminated employees and contractors.
Justification	To ensure that the access rights which are no longer in use (e.g. unused, backup, temporary accounts) are disabled within timeframe in the system or else may be misused for illegal access.
Measurement	To add, remove or disable, re-designated, resigned or terminated employees and contractors according to policy and SOP.
Performance evaluation	$\frac{\text{Number of access right updated}}{\text{Total number of request for access right changes}} \times 100$
Target	100 % policy and SOP conformance.
Implementation evidence	Policy, SOP documentation and documented information.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Frequency	Quarterly.
Responsible parties	a) HR manager. b) System admin. c) Relevant parties.

Annex J
(normative)

Monitoring and measurement of malicious software protection

Table J.1. Malicious software protection coverage

Information	Description
Objective	To assess the protection system coverage against malicious software attack.
Justification	To ensure that information and information processing facilities are protected against malicious software.
Measurement	Number of devices* protected.
Performance evaluation	$\frac{\text{Number of devices* having malicious software protection}}{\text{Total number of devices* or systems*}} \times 100$ *registered in company inventory
Target	100 % software protection installed and 95 % up-to-date.

Performance indicator	Performance should be interpreted as follows:
	a) installed and 95% up-to-date = 5 points;
	b) installed and 85% up-to-date = 4 points;
	c) installed and 75% up-to-date = 3 points;
	d) installed but not up-to-date = 2 points; and
	e) non-existent = 1 point.

Implementation evidence	Record of devices protected using the malicious software protection in the inventory list.
Frequency	a) Monthly report. b) Quarterly measurement revision.
Responsible parties	a) ITD. b) CISO.

Table J.2. Detection, prevention and recovery controls

Information	Description
Objective	To assess the effectiveness of the detection, prevention and recovery controls against malicious software attack incident.
Justification	To ensure that information and information processing facilities are up to date and protected against malicious software attack incident.
Measurement	Policy and SOP exist to remove and recover from known and unknown malicious software attack incident. It should include: a) prevention mechanism; b) detection mechanism; and c) recovery mechanism.
Performance evaluation	$\frac{\text{Number of incidents conform to the SOP}}{\text{Number of total incident}} \times 100$
Target	100 % policy and SOP conformance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) Policy and SOP documentation. b) Documented information.
Frequency	When necessary.
Responsible parties	a) ITD b) CISO.

Annex K
(normative)

Monitoring and measurement of logging and monitoring

Table K.1. Critical system logging

Information	Description
Objective	To ensure logging is enabled for critical systems.
Justification	Event logs shall be enabled to record system activities, exceptions, faults and security events.
Measurement	Number of critical systems with logging enabled.
Performance evaluation	$\frac{\text{Number of critical systems with logging enabled}}{\text{Total number of critical systems}} \times 100$
Target	100% critical systems with logging enabled.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	System log report.
Frequency	As per define by the organisation.
Responsible parties	ITD.

Table K.2. Security event log review

Information	Description
Objective	To ensure event logs are regularly reviewed and appropriate action is taken accordingly.
Justification	To ensure that the security threats are captured and prevented.
Measurement	Policy and SOP exist to monitor and review logs.
Performance evaluation	$\frac{\text{Number of security event log reviewed}}{\text{Number of security event log review planned}} \times 100$
Target	100 % Policy and SOP conformance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) Policy and SOP documentation. b) Documented information.
Frequency	As per policy and SOP.
Responsible Parties	a) ITD. b) CISO.

Annex L
(normative)

Monitoring and measurement of technical vulnerability

Table L.1. Vulnerabilities assessment (VA)

Information	Description
Objective	To identify potential vulnerabilities and evaluate the effectiveness of various security controls by performing regular VA.
Justification	To prevent exploitation of technical vulnerabilities.
Measurement	All critical systems must undergo VA scan.
Performance evaluation	$\frac{\text{Number of critical systems undergoing VA scan}}{\text{Total number of critical systems}} \times 100$
Target	100 % scanned.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) VA schedule/plan. b) VA report.
Frequency	As per policy and SOP.
Responsible parties	a) ITD. b) CISO.

Annex M
(normative)

Monitoring and measurement of backup and restoration

Table M.1. Information backup and restoration

Information	Description
Objective	To ensure information are backup and tested regularly according to an agreed backup policy and SOP.
Justification	To ensure all information backup are restorable for business continuity.
Measurement	Policy and SOP exist to conduct information backup and restoration testing.
Performance evaluation	$\frac{\text{Number of backup and restoration test done}}{\text{Number of backup and restoration test planned}} \times 100$
Target	100 % policy and SOP conformance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) Policy and SOP documentation. b) Documented information.
Frequency	As per policy and SOP.
Responsible parties	ITD.

Annex N
(normative)

Monitoring and measurement of Human Resources

Table N.1. HR security

Information	Description
Objective	To ensure employees and contractors related to INS understand and comply with their roles and responsibilities and are suitable for the roles for which they are assigned.
Justification	To ensure competency, level of integrity and suitability of potential candidates related to INS for the organisation.
Measurement	Policy and SOP exist to conduct personnel-related processes, inclusive of: a) screening; b) terms and conditions of employment; c) education and training; d) disciplinary process; and e) after employment processes such as exit interview, return of all company assets, remove all software access and etc.
Performance evaluation	$\frac{\text{Number of employees and contractors related to INS following the SOP}}{\text{Number of employees and contractors related to INS}} \times 100$
Target	100 % of policy and SOP conformance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	a) Policy and SOP documentation. b) Documented information.
Frequency	As per policy and SOP.
Responsible parties	HR manager.

Annex O
(normative)

Monitoring and measurement of information security education and training

Table O.1. Information security professional development

Information	Description
Objective	To measure effectiveness of INS education and training conducted.
Justification	To ensure INS personnel are equipped with the latest information and knowledge to perform their duties.
Measurement	Staff development plan for INS training exist.
Performance evaluation	$\frac{\text{Number of employee with INS roles attended}}{\text{Total number of employer with INS roles}} \times 100$
Target	100 % of employees and with information security roles shall attend.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	Documented information.
Frequency	As per policy.
Responsible parties	a) HR manager. b) ISMS manager.

Annex P
(normative)

Monitoring and measurement of supplier relationship

Table P.1. Supplier relationship

Information	Description
Objective	To ensure the INS related suppliers have implemented the security practices comparable to this Technical Code.
Justification	To minimise risk and reduce cost for continuous improvement on security practices.
Measurement	Security compliance requirements are met and included in supplier contract.
Performance evaluation	$\frac{\text{Number of supplier contract related to INS having security compliance requirements}}{\text{Number of supplier contract related to INS}} \times 100$
Target	100 % compliance.

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	Documented information.
Frequency	Per award.
Responsible parties	Procurement manager.

Annex Q
(normative)

Monitoring and measurement of physical security

Table Q.1. Physical security

Information	Description
Objective	To ensure that only authorised personnel are allowed to access INS facilities.
Justification	To ensure that all secure areas shall be protected by appropriate entry controls.
Measurement	Policy exists to monitor access rights and existence of appropriate security mechanisms and procedures.
Performance evaluation	$\frac{(\text{Total access to the area} - \text{number of breach})}{\text{Total access to the area}} \times 100$
Target	100 %

Performance indicator	Performance should be interpreted as follows:
	a) 100 % = 5 points;
	b) 90 % = 4 points;
	c) 80 % = 3 points;
	d) 70 % = 2 points; and
	e) 60 % = 1 point.

Implementation evidence	Policy documentation, access control logs and documented information.
Frequency	As per policy.
Responsible parties	Physical security officer.

Acknowledgements

Members of Security, Trust and Privacy Working Group

Mr Thaib Mustafa (Chairman)	Telekom Applied Business Sdn Bhd
Prof Dr Shahrulniza Musa (Vice Chairman)	Universiti Kuala Lumpur
Ms Norkhadhra Nawawi/ Ms Nor Iratul Munirah Mazani (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Mohamed Nabil Zolkefly	Celcom Axiata Berhad
Mr Ahmad Dahari Jarno/ Mr Ahmad Khabir Shuhaimi/ Mr Shahrin Baharom	CyberSecurity Malaysia
Mr Gunasegaran Amaristayah	Digi Telecommunications Sdn Bhd
Mr Azlan Mohamed Ghazali	KPMG Management & Risk Consulting Sdn Bhd
Mr Muhd Dawud Saifullah Fadlullah Mr Wong Chup Woh	Maxis Bhd
Mr Choo Seng Yew	Measat Broadcast Network Systems Sdn Bhd
Ms Faridah Ibrahim	Ministry of Energy, Science, Technology, Environment and Climate Change
Mr Alwyn Goh/ Mr Ng Kang Siong	MIMOS Berhad
Mr Khairil Anuar/ Dr Khazaimatol Shima Subari	Multimedia University
Mr Syarifuddin Palawi	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Mr Arief Khalid Supian/ Ms Patrina Nasiron	Telekom Malaysia Bhd
Ms Lisa Lim/ Ms Nurul Shahida Samsul Azlan	U Mobile Sdn Bhd
Dr Ahmad Shahrafidz Khalid/ Dr Amna Saad/ Ms Herny Ramadhani/ Mr Muhammad Azmin Mohamed Ghazali/ Ms Norhaiza Ya Abdullah/ Ms Roziyani Rawi	Universiti Kuala Lumpur
Assoc Prof Dr Mohd Ezanee Rusli/ Dr Norziana Jamil	Universiti Tenaga Nasional
Mr Mohd Zikre Ahmad Puad	VLAN Technology Sdn Bhd
Mr Mohd Nadzree Karim	webe digital sdn bhd