MCMC MTSFB TC G016:2023

# TECHNICAL CODE

## INFORMATION AND NETWORK SECURITY - SECURITY POSTURE ASSESSMENT (FIRST REVISION)

**Developed by**

Malaysian Technical Standards Forum Bhd

**Registered by**

MCMC

**Registered date: 23 May 2023**

# MCMC MTSFB TC G016:2023

## 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
https://www.mcmc.gov.my

OR

**Malaysian Technical Standards Forum Bhd (MTSFB**)
MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8680 9950
Fax: +60 3 8680 9940
http://www.mtsfb.org.my

## Contents

Page

Committee representation ..... iii
Foreword ..... iv

0. Introduction ..... 1
1. Scope ..... 1
2. Normative references ..... 2
3. Abbreviations ..... 2
4. Terms and definitions ..... 2
   4.1 Attack surface analysis ..... 2
   4.2 Black-box testing ..... 2
   4.3 White-box testing ..... 2
   4.4 Grey-box testing ..... 2
   4.5 Intelligence gathering ..... 2
   4.6 Risk ..... 3
   4.7 Security Posture Assessment (SPA) exercise ..... 3
   4.8 Security Posture Assessment (SPA) programme ..... 3
   4.9 Security Posture Assessment (SPA) project ..... 3
   4.10 Threat ..... 3
   4.11 Vulnerability ..... 3
5. General requirements ..... 3
   5.1 Security Posture Assessment (SPA) programme ..... 3
   5.2 Vulnerability Assessment and Penetration Test (VAPT) ..... 4
   5.3 Security Baseline Assessment (SBA) ..... 13
   5.4 Important considerations ..... 17
6. Engagement objective, scope and limitation ..... 18
   6.1 Engagement objective ..... 18
   6.2 Scope and Limitation ..... 18
7. Security assessor qualification ..... 19
   7.1 Organisation experience and service records ..... 19
   7.2 Security assessor experience and professional credentials ..... 19
   7.3 Past experience ..... 20
   7.4 Conflict of interest ..... 20
8. Assurance of Confidentiality, Integrity and Availability (CIA) ..... 21
9. Security Posture Assessment (SPA) programme planning and management ..... 21
   9.1 Planning ..... 21
   9.2 Managing Security Posture Assessment (SPA) programme phases ..... 22

10. Project management ..... 23
10.1 Project team structure ..... 23
10.2 Project manager qualification ..... 24
11. Reporting requirements ..... 24
11.1 Security Posture Assessment (SPA) exercise reporting ..... 24
12. Protection of test data and secure information transfer ..... 25
12.1 Protection of test data ..... 25
12.2 Information transfer ..... 26
13. Compliance to legal and contractual requirements ..... 26
13.1 Identification of applicable legislation and contractual requirements ..... 26
13.2 Intellectual property rights ..... 26
13.3 Protection of records ..... 26
13.4 Privacy and personal protection ..... 26
14. Vulnerability category and risk rating ..... 26

Annex A Normative references ..... 28
Annex B Abbreviations ..... 29
Bibliography ..... 32

## Committee representation

This technical code was developed by Trust and Privacy 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:

Deloitte Business Advisory Sdn Bhd

Digi Telecommunication Sdn Bhd

Digital Nasional Berhad

FNS (M) Sdn Bhd

Harvestnet Sdn Bhd

Huawei Technologies (M) Sdn Bhd

Maxis Broadband Sdn Bhd

Provintell Technologies Sdn Bhd

Telekom Malaysia Berhad

TIME dotCom Berhad

U Mobile Sdn Bhd

Universiti Kuala Lumpur

Webe Digital Sdn Bhd

## Foreword

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

This Technical Code is an extension to the MCMC MTSFB TC G009, *Information and Network Security - Requirements,* which establish the technical risk assessment for the risk management requirements.

Major modifications in this revision are as follows:

a) added term and updated definitions on Clause 3, *Terms and definitions*;

b) changed on title of 5.1, *Cyber security assessment programme structure* to 5.1, *Security Posture Assessment (SPA) programme*;

c) modified on 5.2, *Vulnerability Assessment and Penetration Test (VAPT)*;

d) modified on 5.2.2.2, *Static Application Security Test (SAST);*

e) modified on 5.2.3, *Customer Premise Equipment (CPE) security test*;

f) modified on 5.2.4, *Telecommunication and signalling technologies security test,*

g) added and modified on 5.3, *Security Baseline Assessment (SBA)*;

h) added new requirements on 5.3.2, *Container security assessment; and*

i) added new requirements on 5.3.7, *Data security controls review.*

This Technical Code replaces the MCMC MTSFB TC G016:2018, *Information and Network Security - Security Posture Assessment (SPA)*.

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

# INFORMATION AND NETWORK SECURITY - SECURITY POSTURE ASSESSMENT

## 0. Introduction

The emergence of more varied, targeted attack techniques from the malware and hacking communities, combined with growing regulations of organisation security standing and diversity of business processes, have resulted in a climate in which businesses are increasingly being required to assess their technological vulnerabilities and security defence mechanisms on a regular basis.

Many organisations perform regular Security Posture Assessment (SPA) exercise to maintain and improve their cyber security baselines and framework in combating with the latest cyber threats. A SPA programme is designed to regularly assessing the vulnerabilities and threats imposed on the critical infrastructure of an organisation, which comprises of the technologies, people and processes.

SPA provides plenty of benefits to an organisation, which listed as follows but not limited to:

a) reduce the risk of intentional or accidental access to information technology assets and information;

b) proactively identify security vulnerabilities that pose a risk to the information technology infrastructure;

c) prioritise resources to address vulnerabilities based on business risk;

d) improve the overall security state of the organisation's infrastructure by following recommended actions to mitigate identified vulnerabilities;

e) achieve improved compliance with regulations and industry mandates that require security assessments;

f) reduce the time and resources needed to stay current with new and emerging vulnerabilities;

g) potential vulnerabilities in the information technology systems and related controls could be identified from end users' and outsiders' angles; and

h) rectification and improvement of the systems could be conducted when issues are identified.

## 1. Scope

This Technical Code provides practical implementation on the establishment and management of the SPA programme by:

a) supporting an organisation in the planning, implementation, and monitoring of an effective SPA programme for the technical vulnerability management requirements; and

b) providing the important considerations and key success requirements in managing a successful SPA programme.

## 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.

See Annex A.

## 3. Abbreviations

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

See Annex B.

## 4. Terms and definitions

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

### 4.1 Attack surface analysis

Security analysis on the exposure and vulnerability of an organisation's information systems being the source of data breach and service disruption. The activities comprise of various vulnerability and threat intelligence data gathering and analysis to assess the known and unknown risks of an organisation to cyber-attacks.

### 4.2 Black-box testing

An outside-in security testing approach and methodology. The assessor has minimum knowledge and information on the test subject. The objective is to produce a prognostic test result by employing the sophisticated hacking techniques used by a real threat actor.

The test is conducted based on specific test criteria along with tools and techniques requirements to be managed the assessor. Normally, it requires a longer test period with intricate test results. Due to the limitation and complexity in managing the quality of the test result, many organisations nowadays replace the black-box testing with intelligence-led testing that is driven by various threat modelling and attack surface analysis techniques in planning the objectives and values of the test.

### 4.3 White-box testing

An inside-out security testing approach and methodology. The assessor is provided with the full knowledge and information on the test subject. The objective is to provide an in-depth and credible test result within a manageable timeline.

### 4.4 Grey-box testing

A combination of white-box and black-box security testing methodologies that provide a comprehensive security test in identifying the security vulnerability by utilising the inside-out and outside-in testing techniques.

### 4.5 Intelligence gathering

The collection and analysis of reliable cyber threat data and information from various external and internal data sources to identify the current and impending cyber threats against an organisation, which provides the useful information to the security assessor in defining the test requirements.

### 4.6 Risk

The exposure to cyber threat and vulnerability exploitation that would result in cyber-attack and data breach of an organisation.

### 4.7 Security Posture Assessment (SPA) exercise

A specific security assessment approach and methodology aim to identify and evaluate security vulnerabilities or security baselines of a particular information asset based on risk assessment requirements of an organisation.

### 4.8 Security Posture Assessment (SPA) programme

A series of planned SPA exercises that employ the enterprise risk assessment approach to identify and manage the cyber threats and vulnerabilities that are affecting information systems, information security processes and ultimately the people of an organisation, which are known as the attack surface of an organisation.

### 4.9 Security Posture Assessment (SPA) project

A full or partial SPA programme that is managed by a third-party security assessor with a specific project goal and service delivery requirements.

### 4.10 Threat

A security event or condition that has the potential of causing disruption, data breach and undesirable consequences of an information system.

### 4.11 Vulnerability

A weakness, flaw or error found within an information system that has the potential to be exploited by a threat agent, which may result in harm to an information system or data breach of an organisation.

## 5. General requirements

### 5.1 Security Posture Assessment (SPA) programme

The SPA programme aims to regularly assess and provides the attestation of the underlying cyber security risks, vulnerabilities and threats that are affecting the critical infrastructure of an organisation.

A successful SPA programme shall be carefully planned and managed to meet the assessment objectives, business and regulatory compliance requirements and most importantly ensuring that the risk mitigation actions are taken to improve the external and internal security posture of the organisation over time.

The general requirements for SPA programme shall include the data network and communications infrastructure security compliance requirements, where the network equipment provider to produce the security certifications of the data network equipment and telecommunication infrastructure.

For example, router, switch, firewall and 4th Generation (4G) or 5th Generation (5G) base station should obtain the following security certifications based on the organisation's security baseline and policy compliance requirements.

a) Common Criteria Recognition Arrangement (CCRA) EAL+; or

b) Global System for Mobile Communications (GSMA) Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme (NESAS-CCS); or

c) any equivalent conformity.

**Table 1. SPA programme structure**

| Data network and telecommunication infrastructure | Security baseline and policy compliance |
|---|---|
| **Vulnerability Assessment and Penetration Test (VAPT)** | **Security Baseline Assessment (SBA)** |
| a) Infrastructure penetration test<br>b) Application security test<br>c) Customer Premise Equipment (CPE) security test<br>d) Telecommunication and signalling technologies security test<br>e) Smart card system security test | a) Host Operating System Configuration and Vulnerability Assessment (HA)<br>b) Container security assessment<br>c) Perimeter Security Device Configuration and Vulnerability Assessment (PDA)<br>d) Database Configuration and Vulnerability Assessment (DBA)<br>e) Security Policy Review (SPR) and Gap Analysis<br>f) Physical security controls review<br>g) Data security controls review |

### 5.2 Vulnerability Assessment and Penetration Test (VAPT)

#### 5.2.1 Infrastructure penetration test

Network security assessment and penetration test on the external and internal networks infrastructure are to improve the network security controls and security configurations of the information assets. This is to prevent data breach, financial and reputation loss due to cyber threats.

The purpose of this test is to perform the intrusive and non-intrusive vulnerability assessment and vulnerability exploitation techniques against the network infrastructure. This is to identify the underlying security vulnerabilities and configuration weaknesses that are affecting the confidentiality, integrity and availability of the information assets.

This test shall cover internal and external network infrastructure for both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) addressing implementation.

##### 5.2.1.1 External Penetration Test (EPT)

VAPT on the external network infrastructure to identify and remediate the vulnerabilities and security configuration weaknesses that are exposed to the external threat actors.

An overview of the key activities for the External Penetration Test (EPT) exercise are as follows:

a) Pre-assessment phase 1 - Scope and objectives

   i) Define and document the engagement objective, business goal and assessment scope.

   ii) Stakeholders' engagement on the roles and responsibilities, project management and reporting requirements. Establish information security requirements for the protection of test data and secure communication.

   iii) Define the test approach and methodology required such as white-box, black-box or grey-box based on the business goal and engagement objective. Specify clearly on the tolerance of service disruption as part of the test requirements.

   iv) Confirm the assessment scope and specifications, project schedule and service contract by the stakeholders and security assessor.

b) Pre-assessment phase 2 - Intelligence gathering and attack surface analysis

   i) Target network and information assets profiling via network Reconnaissance (RECONS) and intelligence gathering techniques are not limited to network Autonomous System Number (ASN), external Internet Protocol (IP) address, domain and email services.

   ii) Analyse the exposure risk and cyber hygiene of the target network and information assets based on the intelligence gathering results obtained from external data sources.

   iii) Identify the attack surface of the target network and information assets based on the exposure risk, identify and suggest the test requirements as part of the assessment scope.

   iv) Document and communicate the test requirements to the stakeholders and system owners.

c) Assessment phase - Vulnerability assessment, security testing, and risk analysis

   i) Identify all remotely accessible services running on the target network and information assets using reliable port scanners for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports scanning, banner grabbing and Enumeration (ENUM) tools.

   ii) Identify the cleartext protocols used and services that are susceptible to brute force and credentials stuffing attacks.

   iii) Perform vulnerability assessment scans on the target network and information assets using multiple vulnerability assessment tools to identify the outdated and vulnerable components and services.

   iv) Prepare and execute the vulnerability exploitation programs and Proof of Concept (PoC) techniques based on the tolerance of service disruption defined. Analyse the remotely exploitable vulnerabilities and the security risks and not limited to the following categories:

      1) Denial of service (DoS).

      2) Weak Password (PWD).

      3) Privileged User Access (PUA).

      4) Database Information (DBI) disclosure.

      5) Man-in-the-Middle (MiTM).

6) Susceptible to Brute Force (BRUF).

7) Weak system Configuration (CONF).

8) ENUM.

9) RECONS.

v) All findings shall be communicated to the stakeholders and system owners during the test to allow timely security remediation and to ensure the awareness of the findings to be reported in the assessment.

vi) Full assessment report shall be provided to the stakeholders and system owners, which include the following important information for security improvement, threat defence and response:

1) Affected information assets.

2) Affected network ports and services.

3) Common vulnerabilities and exposures identification (cve id).

4) Common vulnerability scoring system (cvss) score.

5) Vulnerability severity and descriptions.

6) Mitre adversarial tactics, techniques and common knowledge (mitre att&ck) mapping for threat analysis.

7) Exploitation evidence, include date and time of the execution.

8) Reliable recommendations for vulnerability remediation.

d) Post-assessment phase - Vulnerability retest and status advisory

i) Vulnerability retest and verification shall be conducted upon the completion of vulnerability remediation activities by the system owners within the stipulated time frame.

ii) System owners shall immediately prioritise on the remediation activities that are associated with the high severity findings reported.

iii) Post assessment report shall be provided to the stakeholders and system owners which include the following important information:

1) Latest vulnerability status.

2) Remediation activities by system owners.

3) Retest and exploitation evidence, include the date and time of the execution.

4) Additional recommendations for vulnerability remediation, if required.

#### 5.2.1.2 Internal Penetration Test (IPT)

VAPT on the internal network infrastructure to identify and remediate the vulnerabilities and security configuration weaknesses to minimise the risk of insider threat.

An overview of the key activities for the Internal Penetration Test (IPT) exercise is summarised below.

a) Pre-assessment phase 1 - Scope and objectives

The requirements specified in (a) of 5.2.1.1 shall be applied.

b) Pre-assessment phase 2 - Intelligence gathering and attack surface analysis

The requirements specified in (b) of 5.2.1.1 shall be applied except item (i).

In addition, the target network and information assets profiling via network reconnaissance and intelligence gathering techniques used are not limited to the network diagram review, network assets discovery and network packets capturing for cleartext communications.

During this phase, the cleartext protocols used and services that are susceptible to brute force and credentials stuffing attacks shall be identified.

c) Assessment phase - Vulnerability assessment, security testing and risk analysis

The requirements specified in (c) of 5.2.1.1 shall be applied except item (ii) as it is identified during the pre-assessment phase 2.

d) Post-assessment phase - Vulnerability retest and status advisory

The requirements specified in (d) of 5.2.1.1 shall be applied.

### 5.2.2 Application security test

The application security test shall include the Dynamic Application Security Test (DAST) and Static Application Security Test (SAST) requirements to ensure the quality of the web application security design and development to prevent data breach, financial and reputation loss due to cyber threats.

The purpose of in-depth and secure by design in application security test requirements on the web application modules and web services are to identify and remediate the security vulnerabilities due to the weak application security design and programming techniques used.

This test shall incorporate the black-box or grey-box testing methodology (i.e. DAST) and white-box testing methodology (i.e. SAST) on the web application modules, web services and application programming interface (API) based on the criticality of the web application in collecting, processing and storing sensitive information.

#### 5.2.2.1 Dynamic Application Security Test (DAST)

DAST is a process of testing an application or software product in its operating state. The objective of this exercise is to identify, test and evaluate the security vulnerabilities and design weaknesses of the application components with reference to the OWASP Top 10 application vulnerabilities.

a) Pre-assessment phase 1 - Scope and objectives

The requirements specified in (a) of 5.2.1.1 shall be applied.

b) Pre-assessment phase 2 - Intelligence gathering and threat modelling

i) Ensure the readiness and accessibility of the application's staging or test environment. Any production and sensitive data are removed or sanitised in the application test environment.

ii) Application flowcharting and intelligence gathering to identify the application modules and components used such as the Software Bill of Materials (SBoM) that shall be included in the assessment scope.

iii) Identify the attack surface and high-risk application components such as data collection modules and components for processing, storing and delivering sensitive information are included as part of the assessment scope.

iv) Define the application threat modelling technique and risk categories to be included in the test requirements for the OWASP Top 10 vulnerabilities.

v) Document and communicate the test requirements to the stakeholders and system owners. Review and update the assessment scope and project schedule, if required.

c) Assessment phase - Vulnerability assessment, security testing and risk analysis

i) Perform vulnerability assessment scans on the target application using multiple web application security scanners to identify the outdated and vulnerable components and services.

ii) Execute the manual security analysis and tests based on the risk categories as defined in the application threat modelling requirement.

iii) Analyse the vulnerabilities and security risk based on the following OWASP Top 10 vulnerabilities and risk rating methodology:

1) Broken access control.

2) Cryptographic failures.

3) Injection.

4) Insecure design.

5) Security misconfiguration.

6) Vulnerable and outdated components.

7) Identification and authentication failures.

8) Software and data integrity failures.

9) Security logging and monitoring failures.

10) Server-side request forgery.

iv) Analyse the vulnerabilities and security risk based on the following API Security Top 10 vulnerabilities.

1) Broken object level authorisation.

2) Broken user authentication.

3) Excessive data exposure.

4) Lack of resources and rate limiting.

5) Broken function level authorisation.

6) Mass assignment.

7) Security misconfiguration.

8) Injection.

9) Improper assets management.

10) Insufficient assets management.

v) The overview of the risk rating methodology summarised as the following.

1) Step 1 - Identify a security vulnerability and risk that need to be rated based on the threat agent, attack technique and possible business impact.

2) Step 2 - Estimate the likelihood of a successful attack based on threat agent and vulnerability factors.

3) Step 3 - Estimate the business impact and technical impact of a successful attack.

4) Step 4 - Determine the severity of the risk by estimating the likelihood and impact levels.

vi) All findings shall be communicated to the stakeholders and system owners during the test to allow timely security remediation and to ensure the awareness of the findings to be reported in the assessment.

vii) Full assessment report shall be provided to the stakeholders and system owners which include the following important information for security improvement, threat defence and response.

1) Affected application modules and services.

2) Regulatory compliance issues (if applicable).

3) Common Weakness Enumeration ID (CWE ID) (if applicable).

4) Common Weakness Scoring System (CWSS) score (if applicable).

5) Vulnerability severity and descriptions.

6) MITRE ATT&CK mapping for threat analysis.

7) Exploitation evidence, include the date and time of the execution.

8) Reliable recommendations for vulnerability remediation.

d) Post-assessment phase - Vulnerability retest and status advisory

The requirements specified in (d) of 5.2.1.1 shall be applied.

#### 5.2.2.2 Static Application Security Test (SAST)

SAST is a white box testing approach, which to identify the security vulnerabilities in the application source code and programming techniques used by utilising the automated source code analysis tools and manual testing methods.

a) Pre-assessment phase 1 - Scope and objectives

The requirements specified in (a) of 5.2.1.1 shall be applied.

b) Pre-assessment phase 2 - Intelligence gathering and threat modelling

The requirements specified in (b) of 5.2.2.1 shall be applied except item (i).

In addition, the programming languages, source code analysis tools and regulatory compliance requirements for code analysis shall be identified.

c) Assessment phase - Vulnerability assessment, security testing and risk analysis

The requirements specified in (c) of 5.2.2.1 shall be applied except item (i) and (v)(7). The following is the addition.

i) Perform source code analysis using code scanning tools (where applicable) and manual code review based on recommended security coding guidelines and best practices such as Open Web Application Security Project (OWASP), to validate whether secure programming practices are implemented within the system or host or application.

ii) Perform binary analysis at the binary code level and it analyses raw binaries that compose a complete application when there is no access to the source code. The binary code analysis evaluates stripped binary code. Hence the software can be audited without presence of vendor or coder.

iii) For Commercial Off-The-Shelf (COTS) software, where source code analysis and binary code analysis are not possible due to intellectual property rights of the provider, the following controls shall be performed and reviewed but not limited to:

1) testing reports of the software;

2) third-party attestation or audit reports; and

3) identify the COTS components (optional).

iv) Analyse the common issues on the programming language used that may affect the stability and availability of the application in the adverse conditions.

v) Assess the SBoM to identify and document the in-house software, open-source software and third-party components in a codebase such as the following but not limited to versions and patch status, to reduce the code opacity and identify the security risks.

vi) Full assessment report shall be provided to the stakeholders and system owners as defined in (c)(vii) of 5.2.2.1 with addition of reference to the faulty lines of code, including date and time of the review.

d) Post-assessment phase - Vulnerability retest and status advisory

The requirements specified in (d) of 5.2.1.1 shall be applied.

### 5.2.3 Customer Premise Equipment (CPE) security test

This test covers the security testing of the CPE device supplied to the organisation. This is to ensure the CPE provider undergone or conducted thorough security testing for the CPE. The organisation shall develop a standard security requirement tailored for each CPE supply by the organisation to the customers.

The general requirements for SPA programme shall include the data network and telecommunication infrastructure security compliance where the network equipment provider to produce cybersecurity certification of the target network component. The supplier should provide a regular certification report based on the following standards but not limited to:

a) CCRA EAL+.

b) GSMA NESAS-CCS;

c) CPE shall need to be tested and certified by authority body; or

d) any equivalent conformity.

The purpose of this test is to ensure all vulnerabilities have been mitigated for every firmware release. The test shall focus but not be limited to the following components.

a) Web interface integrity protection.

b) Authentication or authorisation.

c) Authentication and authorisation (or Two-Factor Authentication (2FA)).

d) Network services.

e) Network security zone design with zone isolation.

f) Wireless and transport encryption.

g) Privacy concerns.

h) Cloud interface.

i) Mobile interface.

j) Security configurability.

k) Software or firmware.

l) Physical security.

#### 5.2.4 Telecommunication and signalling technologies security test

Telecommunication and signalling technologies have evolved from non-IP switching technology to IP based technology. By leveraging the principal of all IP network, the threat agents have more opportunities to utilise various publicly available tools to conduct attacks towards the data network and telecommunication infrastructure of the organisation.

The infrastructure offered by the organisation should conform to the related certifications and standards developed by but not limited to the following organisations:

a) MCMC MTSFB TC G028.

b) International Organisation for Standardisation (ISO)

   i) ISO 22301.

   ii) ISO/IEC 15408.

   iii) ISO/IEC 18000-3.

   iv) ISO/IEC 21878.

   v) ISO/IEC 27001.

   vi) any equivalent.

c) International Telecommunication Union - Standardisation (ITU-T).

d) 3rd Generation Partnership Project (3GPP).

e) GSMA NESAS or common criteria.

f) European Telecommunications Standards Institute (ETSI).

g) National Institute of Standards and Technology (NIST).

h) Any other internationally recognised standards.

The security tests on the telecommunication and signalling technologies should focus on the end user, access network, core network, service application and generic security enablers but not limited to the following areas:

a) Evolved packet core, 4G, 5G and beyond cellular network technology.

b) Legacy telecommunication technology Signalling System 7 (SS7), diameter, Secure Transfer Protocol (STP), Short Message Service (SMS) gateway, packet switching and circuit switching technology.

c) High speed broadband network.

d) Short range wireless communication technology.

The security test shall meet the following objectives:

a) Identify and evaluate the known threat and vulnerability in the telecommunication (international and domestic traffic) and signalling technology.

b) Identify and evaluate dos scenario that caused service disruption.

c) Identify and evaluate the eavesdropping on data and voice communication technology.

d) Identify and evaluate the possibility of identity spoofing for fraudulent purposes.

e) Identify and evaluate the possibility of text messages interception.

f) Identify and evaluate the possibility of location tracking.

#### 5.2.5 Smart card system security test

This test covers in-depth security testing and analysis on the smart card system's security mechanism and the information transfer process to identify vulnerabilities that may cause information leakages and forgeries.

The security tests on the smart card system shall cover the front-end and back-end systems infrastructure which involve detailed security testing and analysis on the cryptographic functions used, authentication systems workflow, data security and communication protocols used with reference to the latest industry standards and best practices.

The security test shall cover but not limited to the followings:

a) Smart card technology implementation and information transfer processes analysis.

b) Smart card cryptographic functions and authentication systems workflow analysis including the data transfer between the front-end and back-end systems and the communication protocols used.

c) In-depth security testing and analysis on the smart card system's' authentication mechanism, encryption standard and communication protocol used, mainly to identify the possible information leakages and forgery vulnerabilities.

d) End to end review of the smart card provisioning and termination processes.

### 5.3 Security Baseline Assessment (SBA)

#### 5.3.1 Host Operating System Configuration and Vulnerability Assessment (HA)

Detailed operating systems security configuration and vulnerability assessment as per Centre for Internet Security (CIS) controls, organisation security policies and other industry best practices in protecting the Confidentiality, Integrity and Availability (CIA) of the organisation information assets.

The purpose of this test is to identity operating systems' configuration weaknesses and vulnerabilities as well as to identify areas for improvement and security hardening requirements.

The Operating Systems' (OS) configuration review and vulnerability assessment shall cover and not limited to the followings:

a) System update and software update.

b) Filesystem configuration.

c) Secure boot setting.

d) System process setting.

e) OS services setting.

f) Network configuration and firewall.

g) Logging and auditing.

h) System access, authentication and authorisation.

i) User and group settings.

j) System file permission.

k) OS's vulnerability assessment for known vulnerabilities and outdated system packages.

l) Physical security.

#### 5.3.2 Container security assessment

The use of containers is beneficial in terms of speed and flexibility. However, just like any new technology, containers are not immune to security issues. It is essential to adhere to the following security controls, but not limited to the followings:

a) Secure the containers that supports the micro services-based architecture.

b) Validate the images to ensure it originates from a trusted registry.

c) Reduce the containers' potential attack surface with baselining and behaviour signature detection.

d) Harden containers' image according to the CIS standards.

e) Define an effective vulnerability assessment process.

f) Isolate resource and enforce least privilege.

g) Automatic analysis of cluster operation and application traffic to reduce the attack surface.

h) Implement real-time threat detection and incident response.

i) Scan configuration files for security and compliance checks in Continuous Integration (CI).

j) Lock down the OS.

k) Use centralised policies to restrict which containers can run in the cluster including policies to restrict privileged containers.

l) Rotate encryption keys that are used for communication between orchestrator components.

### 5.3.3 Perimeter Security Device Configuration and Vulnerability Assessment (PDA)

Detailed technical assessment on the perimeter device configuration as per the organisation's security policies and industry standards in protecting the CIA of organisation's information assets.

The purpose of this test is to identify the perimeter security device configuration weaknesses and vulnerabilities to identify areas for improvement and security hardening requirements which shall cover the device's configuration and network packets filtering policies.

The perimeter security device configuration review and vulnerability assessment shall cover and not limited to the followings:

a) Operations security.

b) Physical security.

c) Access control.

d) Communications security.

e) OS's vulnerability assessment for known vulnerabilities and outdated system packages.

### 5.3.4 Database System Configuration and Vulnerability Assessment (DBA)

Detailed technical assessment on the database system configuration as per the organisation's security policies and industry standards in protecting the CIA of organisational information assets.

The purpose of this test is to conduct a detailed technical assessment on the database's system configuration as per the CIS benchmarks and relevant industry standards in protecting the CIA of the organisation information assets.

The main activities of DBA shall include but not limited to the followings:

a) Operating system level configuration.

b) File system permission.

c) General database configuration.

d) Database permission.

e) Auditing and logging.

f) Authentication and authorisation.

g) Network.

h) Database replication.

i) Vulnerability assessment for known vulnerabilities and outdated database software packages.

j) Physical security.

### 5.3.5 Security Policy Review (SPR) and gap analysis

SPR exercise aims to identify the gap in the organisation's information security policies and controls implementation that is based on the ISO/IEC 27001, the international standard for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the contexts of information security management of the organisation.

The objective of the SPR exercise is to identify the security gaps in the current information security policies and controls of the organisation to provide recommendations on the areas for improvement.

The main activities of the SPR exercise shall include but not limited to the followings:

a) Pre-assessment survey and scope definition.

b) Planning and preparation.

c) Security documents, processes, and controls review.

d) Gap analysis.

e) Reporting.

### 5.3.6 Physical security controls review

Detailed technical assessment on the physical security as per the organisation's security policies and industry standards to protect the physical security perimeter in organisation.

The purpose of this review is to conduct an assessment on the physical security posture against the benchmarks and relevant industry standards in protecting the organisation physical perimeter.

The main activities of physical security assessment shall include but not limited to the followings:

a) Access control and authorisation.

b) Surveillance and intrusion detection.

c) Logging and monitoring.

d) Auditing and reviewing.

e) Isolation and segregation of critical assets.

f) Environmental components.

g) Clean desk and clear screen policy.

h) Secure disposal of assets.

i) Secure physical facilities.

The physical security offered by the organisation should conform to the related certifications and standards developed by but not limited to the following organisations:

a) Uptime Institute Tier III design and constructed.

b) Fire suppression as stipulated in TIA-942.

c) Payment Card Industry Data Security Standard (PCI DSS).

d) ISO 9001.

e) ISO/IEC 27001.

f) NIST.

g) Green Mark or equivalent.

h) Risk Management in Technology (RMiT) compliance.

#### 5.3.7 Data Security Controls Review

Securing and protecting the data based on data classification is the responsibility for the organisation to ensure the confidentiality, integrity and availability. Data security controls review shall include but not limited to the following:

a) Need-to-know.

b) Least privilege.

c) Data in transit encryption.

d) Data in rest encryption.

e) Data masking.

f) Tokenisation.

g) Data anonymisation.

### 5.4 Important considerations

The important considerations for ensuring a smooth, cost effective and successful SPA programme delivery include:

a) security assessor's industry experience with proven businesses and operational processes in managing SPA programme requirements;

b) certified security professionals and subject matter experts with proven good experience in managing SPA programme; and

c) reliable security assessment tools and techniques used, and the results obtained are in line with the latest industry standards and best practices.

The general requirements that shall be considered by the organisation prior to engaging the SPA programme are as follows:

a) engagement objective, scope and limitation;

b) security assessor qualification and conflict of interest consideration; and

c) assurance of CIA.

## 6. Engagement objective, scope and limitation

### 6.1 Engagement objective

In general, the benefits realisation of a well-managed SPA programme would contribute many significant values to the organisation growth and sustainability.

The recognised objectives of a successful SPA programme for the organisation include:

a) well-structured approaches and methodologies in the ID of the security vulnerabilities and risks that are associated with the organisation's Information and Communication Technology (ICT) infrastructure;

b) well-managed security risks from the technical and operational perspectives for ensuring the confidentiality, integrity, availability and auditability of the ICT infrastructure;

c) access to professional and top-notch security advisory on the risk mitigation, vulnerability remediation and security controls improvement; and

d) established security roadmap for security baseline improvement of the organisation's network, system and application infrastructure with reference to the latest industry standards and best practices.

### 6.2 Scope and Limitation

The scope for SPA program shall cover the following:

a) Systems that store, process and transmit personal data.

b) Core network and telecommunication systems.

c) Critical business applications.

The type of tests may include the following questions:

a) What are the types of tests required against business requirements and test approach technique to consider such as white-box, black-box or grey-box?

b) Who shall conduct the test?

c) What are the risks and constraints that we shall be concerned about?

d) How do we decide which external service provider to choose?

# 7. Security assessor qualification

## 7.1 Organisation experience and service records

The companies shall provide its past experiences and records for the past SPA projects performed for the last 3 years, including:

a) name and address of the organisation;

b) value of the project;

c) duration of the project; and

d) contact person.

Appropriate penetration testing experience and qualifications cannot be met by certifications alone. Therefore, confirmation of additional criteria is necessary. For example, review of the extent of actual assessments that have been performed and relevant work experience are important considerations when selecting a security assessor or team.

The following questions are examples for assessing the qualifications and competency of a security assessor or companies but not limited to the followings.

a) Is the company specialising in penetration testing or SPA?

b) How many years has the organisation that employs the security assessor been performing penetration tests?

c) Have the company been recognised with any industry awards and recognitions?

d) Does any security violations or breaches that are associated with the company and its members exist?

e) Is there any form or condition in which the company or its members are in a conflict of interest with the penetration testing or SPA exercise?

## 7.2 Security assessor experience and professional credentials

The security assessor may perform the SPA if they are organisationally independent. The security assessor should be organisationally separate from the management of the target systems. For example, in situations where a third-party company is performing the SPA for the organisation, that party cannot perform the SPA if they were involved in the installation, maintenance or support of target systems for the organisation.

In selecting a security assessor or team to understand their qualifications to perform SPA, the certifications held by them may be an indication of the skill level and competence of a potential security assessor or company. While these are not required certifications, they can indicate a common body of knowledge held by the candidate.

The following are some of the examples of common penetration testing certifications.

a) Certified Information Systems Security Professional (CISSP).

b) Certified in Risk and Information Systems Control (CRISC).

c) Certified Ethical Hacker (CEH) by International Council of E-Commerce Consultant (EC-Council).

d) Offensive Security Certified Professional (OSCP) by Offensive Security.

e) Global Information Assurance Certification (GIAC) Certifications

   i) GIAC Certified Security Assessor (GPEN).

   ii) GIAC Web Application Security Assessor (GWAPT).

   iii) GIAC Exploit Researcher and Advanced Security Assessor (GXPN).

   iv) Any equivalent.

f) Council of Registered Security Testers (CREST)

   i) CREST registered penetration tester.

   ii) CREST certified web application tester.

   iii) CREST certified infrastructure tester.

   iv) Any equivalent.

### 7.3 Past experiences

Appropriate experience and qualifications cannot be met by certifications alone. Therefore, confirmation of additional criteria is necessary. For example, review of the extent of actual assessments that have been performed and relevant work experience are important considerations when selecting a security assessor or team.

The following questions are examples for assessing the qualifications and competency of a security assessor or companies but not limited to the followings.

a) How many years' experiences do the security assessor have?

b) Has the security assessor performed assessments against organisations of similar size and scope?

c) What penetration testing experience has the security assessor or team had with the technologies in the target environment (e.g. OS, hardware, web applications, highly customised applications, network services, protocols, etc.)?

d) Any previous reports of security violations, breaches or criminal records that are associated with the security assessor?

e) Involvement in the local or international hackers' communities?

### 7.4 Conflict of interest

The organisation shall avoid to engage the security assessor's company that has potential tendency to be in conflict of interest with SPA objectives of the organisation.

## 8. Assurance of Confidentiality, Integrity and Availability (CIA)

The organisation shall ensure the followings are adhered prior, during and after SPA programme:

a) Confidentiality

All sensitive information shared shall be properly managed by the appointed security assessor and/or subject matter expert.

b) Integrity

The security assessor shall ensure the sensitive information is protected from unauthorised modification.

c) Availability

The security assessor shall manage SPA exercise in a controlled environment to ensure there is no disruption to the business and system operations.

Security services outsourcing may be, for some, best for their situation. As such, it's a good idea to bring a fresh view from the outside periodically to conduct the SPA programme for the organisation, which shall not be a one-time exercise to analyse vulnerabilities, fix security issues and safeguard sensitive data.

The organisation shall ensure the requirements in clause 8 are met when the SPA programme is outsourced to a third party.

## 9. Security Posture Assessment (SPA) programme planning and management

The security assessor shall provide in detail on the methodology that shall be used for the SPA programme. For ensuring a successful implementation and management of a SPA programme, there are several activities and processes to be considered beyond the testing itself. This clause provides guidance for these activities and organised by phases which include:

a) Phase 1 - Pre-assessment;

b) Phase 2 - Assessment; and

c) Phase 3 - Post assessment.

### 9.1 Planning

The main considerations in the planning of a SPA programme shall include:

a) define assessment goals;

b) select assessment team;

c) pre-assessment meeting to review network and system diagrams, define assessment scope;

d) risk assessment on the CIA of the organisation information assets; and

e) establish assessment plan such as SPA plan to clearly specify the assessment scope, approach and methodology, tools and techniques, test system definition, rules of engagement and points of contact.

The SPA programme and its exercises shall be planned, managed and executed at least once a year depending on the regulatory and compliance requirements, nature of business and risk profile of the organisation in alleviating the dynamic cyber security threats that may have direct impact to the business.

### 9.2 Managing Security Posture Assessment (SPA) programme phases

The followings are the main SPA programme activities and prerequisites that need to be carefully managed for ensuring the CIA of information assets.

#### 9.2.1 Phase 1 - Pre-assessment

During the pre-assessment phase, all activities are concentrated on preparing and gathering information for the assessment phase. The organisation shall ensure the process of security clearance through signing of Non-Disclosure Agreement (NDA), letter of approval to conduct assessment are completed prior to start assessment.

The information that shall be gathered include:

a) network diagrams;

b) host information;

c) information security policies, network, system and application documentations;

d) physical security access requirements for onsite activities; and

e) primary and secondary personnel contacts for each site as the points of liaison during the assessment stage.

The deliverables for this phase shall include SPA plan and scope of work documents that clearly describes the assessment requirements, scope and details of the target systems, technical approach and methodology, tools and techniques to be used, limitation and constraints, special test requirements and reporting requirements.

#### 9.2.2 Phase 2 - Assessment

During the assessment phase, all SPA programme activities shall be conducted based on the agreed scope of work as specified in the SPA plan and scope of work documents. The SPA project activities and status updates shall be provided on regular basis.

All activities shall be performed in a controlled environment and shall be conducted based on the structured procedures as per the technical approach and methodology defined. The tools and techniques used and their possible impact to the system shall be clearly communicated and agreed upon.

In this phase, the SPA project team would require the full support and commitment from all the respective members assigned at the SPA project and ensure the following SPA project requirements are being managed in due time.

a) Information and documentations requested for the SPA exercise are provided on time.

b) Ensuring the availability of the system, network and application administrators to assist our consultants especially when performing the onsite activities.

c) Ensuring that any issues and concerns are rectified in due time.

d) Ensuring effective communications among the project team members and the respective personnel involved in the SPA exercises.

Upon the successful completion and submission of the SPA programme exercise reports and deliverables, a management review meeting shall be organised to present the overall of findings and risks to management personnel of the organisations. The respective system owners are required to perform the remediation on any high-risk vulnerabilities within the stipulated time frame prior to the post assessment phase.

The deliverables for this phase shall include:

a) SPA programme exercise reports that clearly specify the security vulnerabilities and risks, areas for improvement and detailed technical recommendations;

b) management and technical presentation materials on the security vulnerabilities and risks identified;

c) recommendations for both short-term and long-term security improvements; and

d) useful information to provide decision making inputs to management on the level of technical complexity, remediation cost and duration, required resources.

#### 9.2.3 Phase 3 - Post assessment

In this phase, the full support and commitment are required from the SPA project team and the respective system owners of the organisations to perform the vulnerability remediation activities within the stipulated time. System owners shall carefully plan and perform the vulnerability remediation which can be based on risk level, technical complexity, duration and local resources availability.

Once the vulnerabilities remediation activities are completed, the security assessor shall conduct the post assessment exercises to verify the presence of the vulnerabilities reported and to ensure that the vulnerabilities have been successfully remediated. The deliverables of this phase shall include:

a) post assessment exercise reports that clearly specify the security vulnerabilities and risks, areas for improvement and detailed technical recommendations; and

b) useful information to provide decision making inputs to management on the risk level, possible business impact, remediation cost and duration, required resources.

## 10. Project management

The companies shall provide a detailed timeline for the SPA project in Gantt chart format.

### 10.1 Project team structure

The companies shall provide the project structure for the SPA service, including but not limited to the followings.

a) roles and responsibilities (i.e. project manager, security assessor, document controller (if any)).

b) name(s).

### 10.2 Project manager qualification

Responsibility and accountability for the SPA project are necessary to complete the project on time. As such, the role of the project managers to coordinate and deliver projects according to defined timelines, budgets and outcomes are very vital. Effective utilisation of the available resources, effective managing risks and finding the correct solutions are the characteristics of an effective project management.

Managing the penetration testing project requires a thorough understanding of all the individual parts of the scope process. Once these scope objectives have been cleared, the project manager should coordinate with the penetration testing process to develop a formal outline that defines the project plan and schedule. This is important because the test execution requires careful allotment of the timescale that shall not exceed the declared deadline. Once the proper resources have been identified and allocated to carry certain tasks during the assessment period, it becomes necessary to draw a timeline depicting all those resources with their key parts in the penetration testing process.

Project managers should work with various methodologies, preferably certified or qualified in the required competencies in ensuring them capable to resolve complex problems in fast-paced and dynamic environments. It is recommended for the project manager to have qualifications specific to the industry, such as Projects In Controlled Environments (PRINCE2), Project Management Professional (PMP) or Information Technology Infrastructure Library (ITIL).

The following skills and experience are also considered as essential for a project manager in ensuring the success of the SPA project for the organisation but not limited to the followings.

a) Client presentations.

b) Effective communication (oral and written).

c) Leadership.

## 11. Reporting requirements

Comprehensive and consistent reporting is a critical phase of a SPA. This section provides guidelines on common contents of an industry standard SPA. It shall be noted that these are only suggested outlines and do not define specific reporting requirements for the SPA. Testers may have different sections, alternative titles and/or report format, etc. This Technical Code represents data gathered from a number of penetration testing providers and the desires of customers.

### 11.1 Security Posture Assessment (SPA) exercise reporting

The report provided for each SPA exercise shall meet the following minimum requirements as stated in Table 2.

**Table 2. Reporting requirements**

| Items | Minimum requirements |
|---|---|
| Executive summary | High level summary of the SPA scope and major findings. |
| Scope of works | A detailed definition of the scope of the network and systems tested as part of the assessment:<br>a) clarification systems or segments that are considered during the test; and<br>b) ID of critical systems and explanation of why they are included in the test as targets. |

**Table 2. Reporting requirements** *(continued)*

| Items | Minimum requirements |
|---|---|
| Statement of methodology | Details on the methodologies used to complete the testing (e.g. port scanning, map etc.). |
| Limitations | Document any restrictions imposed on testing such as designated testing hours, bandwidth restrictions, special testing requirements for legacy systems, etc. |
| Findings | a) Whether or how the systems or host or application may be exploited using each vulnerability.<br>b) PoC and exploitation evidence.<br>c) Risk ranking or severity of each vulnerability.<br>d) Targets affected.<br>e) References (if available)<br>i) CVE, CWE, Bugtraq ID (BID), Open Source Vulnerability Database (OSVDB), etc.; and/or<br>ii) vendor and/or researcher.<br>f) Description of finding.<br>g) Remediation status. |
| Tools used | Tools and techniques used |
| Appendix | Intelligence gathering and threat modelling techniques |

## 12. Protection of test data and secure information transfer

### 12.1 Protection of test data

Test data shall be selected carefully, protected and controlled.

The use of operational data containing personally identifiable information or any other confidential information for testing purposes shall be avoided. If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content shall be protected by removal or modification.

The following requirements shall be applied to protect operational data, when used for testing purposes.

a) The access control procedures, which apply to operational application systems, shall also apply to test application systems.

b) There shall be separate authorisation each time operational information is copied to a test environment.

c) Operational information shall be erased from a test environment immediately after the testing is complete.

d) The copying and use of operational information shall be logged to provide an audit trail.

### 12.2 Information transfer

Appropriate security controls shall be in place to protect the transfer of information through the use of all types of communication facilities. Information involved in electronic messaging such as email shall be appropriately protected (e.g. using file encryption software or password protected).

## 13. Compliance to legal and contractual requirements

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

### 13.1 Identification of applicable legislation and contractual requirements

All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.

### 13.2 Intellectual property rights

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

### 13.3 Protection of records

Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislator, regulatory, contractual and business requirements.

### 13.4 Privacy and personal protection

Privacy and protection of personally identifiable information shall comply with Act 709 or at least with MCMC MTSFB TC G030.

## 14. Vulnerability category and risk rating

The organisation shall implement or adopt its own risk rating methodology to effectively determine the risk level and business impact of the various types of vulnerabilities identified by the SPA programme.

The severity levels that are associated with the common vulnerabilities identified in a SPA programme is listed in Table 3 below.

**Table 3. Common vulnerability categories and severity level**

| Vulnerability type | Severity | Descriptions |
|---|---|---|
| DoS | High | This type of vulnerability if exploited would cause service disruption to a single or multiple system functions. |
| Weak PWD | High | This type of vulnerability would allow attacker to easily gain access directly to the system by password guessing. |
| Gain PUA | High | This type of vulnerability would allow the attacker to gain administrative access to the system due to the weaknesses of the user authentication and/or authorisation mechanisms. |

**Table 3. Common vulnerability categories and severity level** *(continued)*

| Vulnerability type | Severity | Descriptions |
|---|---|---|
| DBI disclosure | High | This type of vulnerability would allow the attacker to obtain the valuable information from the system database, via exploitation to the database system configuration weaknesses or via complex Structured Query Language (SQL) injection attacks. |
| MiTM | Medium | This type of vulnerability is associated with the clear text packet transmissions over the network that can be easily obtained via sniffing tools by the attacker or due to weak network encryption mechanisms. |
| Susceptible to BRUF | Medium | This type of vulnerability is associated with the user authentication mechanism on a system that supports multiple user logins and does not have user account lockout control for failed login attempts. |
| Weak system CONF | Medium | This type of vulnerability is reported when the remote system appears to be in default configuration state with one or more of the 'unused' services that can accessed remotely. The unused services running on the system provide the attacker with more opportunities to compromise the system. The system is running on old version software that is susceptible to multiple vulnerabilities. |
| ENUM | Low | This type of vulnerability is not considered as an actual attack to the system, but more towards information gathering for further launching of a real attack. The types of information gathered via ENUM are the network resources and shares, users and groups, system and application services, etc. |
| RECONS | Low | This type of vulnerability is associated with the publicly accessible information on the network services that provide the attacker an insight of the targeted network topology and the perimeter security design. |

# Annex A
(normative)

## Normative references

Act 709, *Personal Data Protection Act (PDPA) 2010*

MCMC MTSFB TC G028, *IMT-2020 (Fifth Generation) - Security Requirements*

MCMC MTSFB TC G030, *Information Network Security - Personal Information Management Systems*

ISO 9001, *Quality management systems - Requirements*

ISO 22301, *Security and resilience - Business continuity management systems - Requirements*

ISO/IEC 15408, *Information technology - Security techniques - Evaluation criteria for IT security*

ISO/IEC 18000-3, *Information technology - Radio frequency identification for item management - Part 3: Parameters for air interface communications at 13,56 MHz*

ISO/IEC 21878, *Information technology - Security techniques - Security guidelines for design and implementation of virtualized servers*

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

BNM/RH/PD 028-98, *Risk Management in Technology (RMiT)*

TIA-942, *Telecommunications Infrastructure Standard for Data Centers*

OWASP Top Ten, the OWASP foundation

# Annex B
(informative)

## Abbreviations

| | |
|---|---|
| 2FA | Two-Factor Authentication |
| 3GPP | 3rd Generation Partnership Project |
| 4G | 4th Generation |
| 5G | 5th Generation |
| API | Application Program Interface |
| ASN | Autonomous system number |
| BID | Bugtraq ID |
| BRUF | Brute Force |
| CCRA | Common Criteria Recognition Arrangement |
| CEH | Certified Ethical Hacker |
| CI | Continuous Integration |
| CIA | Confidentiality, Integrity and Availability |
| CIS | Centre of Internet Security |
| CISSP | Certified Information Systems Security Professional |
| CONF | Configuration |
| COTS | Commercial Off-The-Shelf |
| CPE | Customer Premise Equipment |
| CREST | Council of Registered Security Testers |
| CRISC | Certified in Risk and Information Systems Control |
| CVE | Common Vulnerabilities and Exposures |
| CVSS | Common Vulnerability Scoring System |
| CWE | Common Weakness Enumeration |
| CWSS | Common Weakness Scoring System |
| DAST | Dynamic Application Security Test |
| DBA | Database Configuration and Vulnerability Assessment |
| DBI | Database Information |
| DoS | Denial of Service |
| EC-Council | International Council of E-Commerce Consultant |
| ENUM | Enumeration |
| EPT | External Penetration Test |
| ETSI | European Telecommunications Standards Institute |
| GIAC | Global Information Assurance Certification |
| GPEN | GIAC Certified Security Assessor |

| | |
|---|---|
| GSMA | Global System for Mobile Communications |
| GWAPT | GIAC Web Application Security Assessor |
| GXPN | GIAC Exploit Researcher and Advanced Security Assessor |
| HA | Host Operating System Configuration and Vulnerability Assessment |
| ICT | Information and Communications Technology |
| ID | Identification |
| IP | Internet Protocol |
| IPT | Internal Penetration Test |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| ITIL | Information Technology Infrastructure Library |
| ITU-T | International Telecommunication Union - Standardisation |
| MiTM | Man-in-the-Middle |
| MITRE ATT&CK | MITRE Adversarial Tactics, Techniques and Common Knowledge |
| NDA | Non-Disclosure Agreement |
| NESAS-CCS | Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme |
| NIST | National Institute of Standards and Technology |
| OS | Operating System |
| OSCP | Offensive Security Certified Professional |
| OSVDB | Open Source Vulnerability Database |
| OWASP | Open Web Application Security Project |
| PCI DSS | Payment Card Industry Data Security Standard |
| PDA | Perimeter Security Device Configuration and Vulnerability Assessment |
| PMP | Project Management Professional |
| PoC | Proof of Concept |
| PRINCE2 | Projects In Controlled Environments |
| PUA | Privileged User Access |
| PWD | Password |
| RECONS | Reconnaissance |
| RMiT | Risk Management in Technology |
| SAST | Static Application Security Test |
| SBA | Security Baseline Assessment |
| SBoM | Software Bill of Materials |
| SMS | Short Message Service |
| SPA | Security Posture Assessment |
| SPR | Security Policy Review |
| SQL | Structured Query Language |

| | |
|---|---|
| SS7 | Signalling System 7 |
| STP | Secure Transfer Protocol |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| VAPT | Vulnerability Assessment and Penetration Test |

## Bibliography

[1] ISO/IEC 22300, *Societal security - Terminology*

[2] ISO/IEC 27000, *Information technology - Security techniques - Information security management system - Overview and vocabulary*

[3] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*

[4] ISO/IEC 27017, *Information technology - Security techniques - Code of Practice for information security controls based on ISO/IEC 27002 for cloud services*

[5] ISO/IEC 31010, *Risk management - Risk assessment techniques*

[6] *Open Source Security Testing Methodology Manual (OSSTMM),* the Institute for Security and Open Methodologies (ISECOM)

[7] *Web Security Testing Guide Version 4.2*, the OWASP foundation

[8] *PTES Technical Guidelines*, the pentest-standard organization

## Acknowledgements


**Members of the Trust and Privacy Sub Working Group**

| | |
|---|---|
| Mr Nicholas Ng (Vice Chair/Draft lead) | Provintell Technologies Sdn Bhd |
| Ms Norkhadhra Nawawi (Secretariat) | Malaysian Technical Standards Forum Bhd |
| Mr Azlan Mohamed Ghazali | Deloitte Business Advisory Sdn Bhd |
| Mr Parag Barua | Digi Telecommunication Sdn Bhd |
| Ms Nur Hidayah Mohd Mustapha | Digital Nasional Berhad |
| Mr Thaib Mustafa/ | FNS (M) Sdn Bhd |
| Mr Wan Ameer Ruzman Wan Salaidin | |
| Mr Nyou Wei Fung/ | Harvestnet Sdn Bhd |
| Ms Siti Nur Baiti Abdul Rahim | |
| Mr Dikhwan Hadi Darnalis | Huawei Technologies (M) Sdn Bhd |
| Mr Ahmad Fahmi Mohd Haris/ | Maxis Broadband Sdn Bhd |
| Mr Cheong Gze Wei/ | |
| Mr Mohd Adlan Abd Wahab/ | |
| Mr Muhd Dawud Saifullah Fadlullah/ | |
| Ms Russell - Md Ifthekharul Alam/ | |
| Mr Yasdy Md Yasin | |
| Mr Mohammad Hairul Isnin | Telekom Malaysia Berhad |
| Mr Bhavesh Kaul | TIME dotcom Berhad |
| Mr See Chun Siong | U Mobile Sdn Bhd |
| Dr Amna Saad/ | Universiti Kuala Lumpur |
| Mr Shadil Akimi Zainal Abidin/ | |
| Prof Dr Shahrulniza Musa | |
| Mr Teo Beng Seon | Webe Digital Sdn Bhd |

**By invitation:**

| | |
|---|---|
| Ms Darishini Manimaran/ | Carsome Sdn Bhd |
| Mr Yuwanthiran Sukalingam | |
| Mr Mohd Ridhwan Mohd Salleh | Celcom Axiata Berhad |
| Ms Dania Syahirah Zakry | CyberSecurity Malaysia |