TECHNICAL CODE

SECURITY POSTURE ASSESSMENT (SPA)

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

MCMC MTSFB TC TXXX:2017

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.skmm.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia,
Jalan Impact
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 Trust and Privacy Sub Working Group which supervised 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

Kementerian Sains, Teknologi dan Inovasi (MOSTI)

Malaysian Communications and Multimedia Commission

Malaysian Technical Standards Forum Bhd (Secretariat)

Provintell Technologies

Telekom Applied Business Sdn Bhd

Telekom Malaysia Bhd

TIME dotCom Bhd

Universiti Kuala Lumpur (UniKL)

webe digital sdn bhd

Foreword

This technical code for Security Posture Assessment (SPA) for Communication and Multimedia Industry (CMI) *(*'this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd ('MTSFB') via its Trust and Privacy Sub Working Group under the supervision of Security, Trust and Privacy Working Group.

Security Posture Assessment (SPA) for Communications and Multimedia Industry (CMI) is a Cyber Security Assessment Program that is specifically developed to provide the CMI with a structured security risk and vulnerability assessment approach and methodology to support the SPA Objectives of the CMI's organisations.

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

SECURITY POSTURE ASSESSMENT (SPA) FOR COMMUNICATIONS AND MULTIMEDIA INDUSTRY (CMI)

0. Introduction

The emergence of more varied, targeted attack techniques from the malware and hacking communities, combined with growing regulations of organisational 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 periodic security posture assessments to maintain a current picture of their vulnerabilities, allowing them to prioritise remediation activities based on available resources and business risk. Thus, Security Posture Assessment (SPA) is essential for every organisation. This exercise shall examine and test confidentiality, integrity and availability (CIA) of the information infrastructure used by the organisation.

Security posture assessment provides plenty of benefits to an organisation, as listed below 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.

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 a successful SPA program by:

a) Supporting the CMI organisations to conduct effective, value-for-money security testing and assessment as part of the technical security assurance framework. It is designed to enable the CMI organisations to prepare for the security testing, conduct actual testing in a consistent, competent manner and follow up tests effectively.

b) Provide overview of the key concepts the CMI organisations need to understand to conduct a well-managed SPA Program, the evaluation criteria and the 4process to employ an external Security Assessor in supporting the SPA Program.

The Technical Code is applicable to CMI's organisations of all sizes, budgets, and industries.

2. Normative reference

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.

ISO/IEC 22300, *Societal security - Terminology*

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

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

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

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

ISO/IEC 31010, *Risk management - Risk assessment techniques*

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

Open Web Application Security Project (OWASP), the OWASP Foundation

Center of Internet Security (CIS) Controls (Version 6.1) and CIS Benchmarks

3. Terms and definitions

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

3.1 Risk

Effect of uncertainty on objectives.

NOTES:

1. An effect is a deviation from the expected: positive and/or negative.
2. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process).
3. Risk is often characterised by reference to potential events, and consequences, or a combination of these.
4. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
5. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

3.2 Threat

Potential cause of unwanted incident, which may result in harm to a system or organisation.

3.3 Vulnerability

Intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.

4. Abbreviations

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

CMI	Communication and Multimedia Industry
CPE	Customer Premise Equipment
DAST	Dynamic Application Security Test
DBA	Database Configuration and Vulnerability Assessment
DNS	Domain Name Server
DNSBL	DNS Blacklist/Blocklist
EPT	External Penetration Test
HA	Host Operating System Configuration and Vulnerability Assessment
ICT	Information Communications Technology
IP	Internet Protocol
IPT	Internal Penetration Test
RBL	Realtime Blackhole Lists
SAST	Static Application Security Test
SBA	Security Baseline Assessment
SPA	Security Posture Assessment
SPR	Security Policy Review and Gap Analysis
URIBL	Uniform Resource Identifier Blacklist
VAPT	Vulnerability Assessment and Penetration Test

5. General requirements

5.1 Cyber security assessment program structure for CMI

A SPA program aims to provide the CMI's organisations with the insights and visibilities on the underlying security risks, vulnerabilities and weaknesses on the infrastructure and recommendations for short term and long-term security improvements involving the technology, people and process. The comprehensive results obtained from a successful SPA program (see Table 1) shall be measurable through assurance process to oversee the testing, monitoring performance against requirements and ensuring appropriate actions are being taken.

Table 1. SPA program structure for CMI

Data Network and Telecommunication Infrastructure	Security Configuration and Policy Compliance
Vulnerability Assessment and Penetration Test (VAPT) a) Infrastructure Penetration Test b) Application Security Test c) Customer Premise Equipment (CPE) Security Test d) Telecommunication and Signaling Technologies Security Test e) Subscriber Identification Card (SIM) and Smart Card Security Test	**Security Baseline Assessment (SBA)** a) Operating System Configuration and Vulnerability Assessment b) Perimeter Security Device Configuration and Vulnerability Assessment c) Database Configuration and Vulnerability Assessment d) Security Policy Review and Gap Analysis

5.2 Vulnerability Assessment and Penetration Test (VAPT)

5.2.1 Infrastructure penetration test

a) This test shall cover internal and external network infrastructure of the CMI organisation for both IPv4 and IPv6 addressing implementation.

b) The purpose of this test is to perform either intrusive or non-intrusive vulnerability assessment and exploitation techniques toward the CMI network infrastructure to identify the underlying security vulnerabilities and weaknesses that may disrupt the security goals in terms of availability, integrity and confidentiality of the CMI network infrastructure.

c) Requirements:

i) External Penetration Test (EPT)

1) Vulnerability assessment and exploitation activities toward the CMI's external network infrastructure by simulating various vulnerability assessment and exploitation techniques to idenatity the underlying security vulnerabilities and weaknesses that are exposed to the external attacker. Security testing and risk are analysed from the external perspective.

2) The main activities for EPT shall include but not limited to the followings:

Step 1: Intelligence gathering

- Internet foot-printing, such as Internet registry check, dns, web, mail and other common Internet services checks, multi RBLs such as DNSBL and URIBL checks;
- Network reconnaissance and identify perimeter security mechanisms such as firewalls, IDS or IPS;
- Identify the remote operating system types;
- Identify remotely accessible services, type and version;
- Identify clear-text protocols used.

Step 2: Vulnerability assessment

- Vulnerability scanning using multiple commercial vulnerability scanning tools;
- Vulnerability analysis to identify default system and services configuration and remotely exploitable vulnerability;
- Prepare vulnerability exploitation test plan which describes the exploitation tools and techniques;
- Identify and describe the possible system impact on the exploitation techniques used.

Step 3: Security testing and risk analysis

- Conduct vulnerability exploitation and Proof-of-Concept (POC);
- Identify the remotely exploitable vulnerability types such as Denial-of-Service (DOS);
- Weak Password (PWD), Privileged User Access (PUA), Database Information Disclosure (DBI), Man-in-the-Middle (MITM), Susceptible to Brute Force (BRUF), Weak System Configuration (CONF), Enumeration (ENUM), Reconnaissance (RECONS), to name a few;
- Analyse the vulnerability's risk level based on the CMI's risk assessment methodology.

Step 4: Reporting and presentation of findings

- Documentation of the security evidences and findings;
- Vulnerability research to provide the security recommendations based on the latest security trends and best practices;
- Management and technical reports preparation, review and finalisation;
- Conduct technical and management presentations on the findings such as the vulnerability and risk overview to the CMI's top management and risk owners, the detailed technical findings and recommendations to the system owners for vulnerability remediation.

Step 5: Vulnerability Retest and Verification (Post Assessment)

- Vulnerability retest and verification shall be performed upon the completion of the vulnerability remediation activities by the system owners within the stipulated time frame;
- Vulnerability retest shall focus and prioritise on the remediation activities that are associated with the high risk vulnerabilities and to be completed within one (1) month of the vulnerability discovery;
- Update of the vulnerability status and risk level;
- Preparation, review and finalisation of the Post Assessment report.

ii) Internal Penetration Test (IPT)

1) Vulnerability assessment and exploitation activities toward the CMI's internal network infrastructure such as the server farm networks, by simulating various vulnerability assessment and exploitation techniques to identity the underlying security vulnerabilities and weaknesses that are exposed to the internal users. Security testing and risk are analysed from the internal perspective.

2) The main activities for IPT shall include but not limited to the followings:

Step 1: Intelligence gathering

- Network reconnaissance and identify the local network topology of IP or non-IP based network infrastructure;
- Identify internal network's packet filtering mechanisms such as firewall, IDS or IPS;
- Identify target hosts' operating system types;
- Identify locally accessible services, type and version;
- Identify clear-text protocols used.

Step 2: Vulnerability Assessment

- Vulnerability scanning using multiple commercial vulnerability scanning tools;
- Vulnerability analysis to identify default system and services configuration and remotely exploitable vulnerability;
- Network packets sniffing for clear-text passwords and other useful information;
- Prepare vulnerability exploitation test plan which describes the exploitation tools and techniques;
- Identify and describe the possible system impact on the exploitation techniques used.

Step 3: Security Testing and Risk Analysis

- Conduct vulnerability exploitation and Proof-of-Concept (POC);
- Identify the remotely exploitable vulnerability types such as Denial-of-Service (DOS), Weak Password (PWD), Privileged User Access (PUA), Database Information Disclosure (DBI), Man-in-the-Middle (MITM), Susceptible to Brute Force (BRUF), Weak System Configuration (CONF), Enumeration (ENUM), Reconnaissance (RECONS), to name a few;
- Analyse the vulnerability's risk level based on the CMI's risk assessment methodology.

Step 4: Reporting and Presentation of Findings

- Documentation of the security evidences and findings;
- Vulnerability research to provide the security recommendations based on the latest security trends and best practices;

- Management and technical reports preparation, review and finalisation;

- Conduct technical and management presentations on the findings such as the vulnerability and risk overview to CMI's top management and risk owners, the detailed technical findings and recommendations to the system owners for vulnerability remediation.

Step 5: Vulnerability Retest and Verification (Post Assessment)

- Vulnerability re-test and verification shall be performed upon the completion of the vulnerability remediation activities by the system owners within the stipulated time frame.

- Vulnerability retest shall focus and prioritise on the remediation activities that are associated with the high risk vulnerabilities and to be completed within one (1) month of the vulnerability discovery;

- Update of the vulnerability status and risk level;

- Preparation, review and finalisation of the Post Assessment report.

5.2.2 Application security test

a) This test covers the various applications used by the CMI organisation for both CMI side and subscriber side such as web application, mobile application and client based application.

b) The purpose of this test is to perform a thorough security test toward the CMI's multifaceted application modules for possible vulnerabilities and weakness that may disrupt the security goals in terms of availability, integrity and confidentiality of the CMI's business critical applications.

c) Requirements:

i) Dynamic Application Security Test (DAST)

The Dynamic Application Security Test (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's Top 10 application vulnerabilities and security risk rating methodology. This is to ensure that the risk mitigation controls recommended to the CMI are in line with the latest industry trend and best practices.

The main activities of DAST shall include but not limited to the item in Table 2.

Table 2. DAST activities

Vulnerability Types	Descriptions
Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorisation.
Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

Table 2. DAST activities *(continued)*

Vulnerability Types	Descriptions
Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorised data.
Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorisation.
Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorised pages.

ii) Static Application Security Test (SAST)

The Static Application Security Test (DAST) is a white-box testing approach which can help to accurately identify and analyse both the server-side and client-side application vulnerabilities. The main objective of the SAST exercise is to identify, test and evaluate the security vulnerabilities in the application design and programming codes by utilising the automated and manual source codes testing and analysis methods. Besides the usual web and mobile application codes, SAST can be applied to code in also in embedded systems and other locations.

The main activities of SAST shall include but not limited to the Table 3.

Table 3. SAST activities

Vulnerability Types	Descriptions
Input Validation	This type of vulnerability includes cross site scripting, sql injection, Xpath injection, LDAP injection, cross site request forgery and buffer overflow.
Source Code Design	This type of vulnerability reflects the security flaw in source code starts from design and from the choices made before starting to code such as insecure field scope, insecure method scope, insecure class modifiers, unused external references and redundant code.
Information Leakage And Improper Error Handling	This type of vulnerability contains security check families about how source code manage errors, exception, logging and sensitive information. The following families are as information leakage and improper error handling, unhandled exception, routine return value usage, NULL Pointer reference and insecure logging.
Direct Object Reference	This type of vulnerability refers to the attacker's capability to interact with application internals supplying an ad hoc crafted parameter. The families contained in this category are direct object reference database data, file system and to memory.
Resource Usage	This type of vulnerability is related to all the unsafe ways a source code can request operating system managed resources. Most of the vulnerability families contained here, if exploited, will result in some kind of denial of service. Resources can be file system objects memory, CPU, network bandwidth. The families included are resource usage Insecure file creation, file modifying, and file deletion, race condition, memory leak and unsafe process creation.
API Usage	This type of vulnerability reflects the APIs provided by the system or by the framework in use that can be used in a malicious way. In this category you can identify the insecure database calls, random number creation, improper memory management calls, insecure HTTP session handling and insecure strings manipulation.
Best Practices Violation	This type of vulnerability reflects the miscellaneous security violations that don't fit in the previous categories. Most, but not all, of these contain warning-only source code best practices. This category includes insecure memory pointer usage, NULL pointer reference, pointer arithmetic, variable aliasing, unsafe variable initialisation missing comments and source code documentation.
Weak Session Management	This type of vulnerability is associated with the weak session management which is not invalidating session upon an error occurring, not checking for valid sessions upon HTTP request, not issuing a new session upon successful authentication and passing cookies over non SSL connections (no secure flag).
Usage Of HTTP GET Query Strings	This type of vulnerability allows the payload data is logged if contained in query strings. This information can be logged in all nodes between client/browser and server. Passing sensitive information using a query string and HTTP GET is a mortal sin. SSL does not even protect you here. Passing sensitive data over URL or query string.

5.2.3 Customer Premise Equipment (CPE) Security Test

5.2.3.1 Descriptions

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

5.2.3.2 Objectives

The purpose of this test is to ensure all vulnerabilities have been mitigated for every firmware release.

5.2.3.3 Requirements

The test shall focus and may not be limited to the following components:

a) web interface;

b) authentication/authorisation;

c) network services;

d) transport encryption;

e) privacy concerns;

f) cloud interface;

g) mobile interface;

h) security configurability;

i) software/firmware;

j) physical security.

5.2.4 Telecommunication and Signalling Technologies Security Test

5.2.4.1 Descriptions

Telecommuncation and Signalling technology has evolved from non-IP switching technology to IP based technology. By leveraging the principal of all IP network, threat agent has the freedom to use more publicly available tools to conduct attacks towards the CMI services and infrastructure. The security test for telecommunication and signaling technologies will enable the CMI to uncover threats in their environment.

5.2.4.2 Objectives

The purpose of this test is to ensure to identify vulnerability and weaknesses that may lead to data interception, privacy violation, denial-of-service, acquiring sensitive data, spoofing, data tampering, and unauthorised access to the CMI infrastructure.

5.2.4.3 Requirements

a) The security tests on Telecommunication and Signaling Technologies shall focus and may not be following on the following areas:

   i) evolved packet core and 4G cellular network technology;

   ii) legacy telecommunication technology - SS7, packet switching and circuit switching technology;

   iii) high speed Broadband network.

b) The security test shall meet the following objectives:

i) uncover known threat and vulnerability in the telecommunication and signaling technology;

ii) uncover denial-of-service scenario that caused service disruptions;

iii) uncover eavesdropping on data and voice communication technology;

iv) uncover possibility of identity spoofing for fraudulent purposes;

v) uncover possibility of text messages interception.

5.2.5 Subscriber Identification Card (SIM) and Smart Card Security Test

5.2.5.1 Descriptions

This test covers in-depth security testing and analysis on the Smart Card systems' security mechanisms and the information transfer process to identify vulnerabilities that may cause data leakage and forgery.

5.2.5.2 Objectives

The security tests on Smart Card technology shall cover the front-end and back-end Smart Card 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 including but not limited to the ISO 7816, PC/SC, X509, Open OS, FIPS 140 and Common Criteria.

5.2.5.3 Requirements

The security test on Smart Card system shall cover but may not limited to the followings:

a) Smart Card technology implementation and information transfer processes analysis;

b) cryptographic functions and authentication systems workflow analysis including the data transfer between Smart Card, Reader and Backend Systems and the communication protocols used;

c) in-depth security testing and analysis on the Smart Card systems' authentication mechanisms, encryption standards and communication protocols used, mainly to identify possible data leakage and card forgery vulnerabilities.

5.3 Security Baseline Assessment (SBA)

5.3.1 Operating System Configuration and Vulnerability Assessment (HA)

5.3.1.1 Descriptions

Detailed operating systems security configuration and vulnerability assessment as per Internet Security's (CIS) Security Benchmarks, organisation security policies and other industry best practices in protecting the confidentiality, integrity and availability of the CMI's information assets.

5.3.1.2 Objectives

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.

5.3.1.3 Requirements

The operating systems' configuration review and vulnerability assessment shall cover but 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) operating system's vulnerability assessment for known vulnerabilities and outdated system packages;

l) physical security.

5.3.2 Perimeter Security Device Configuration and Vulnerability Assessment (PDA)

5.3.2.1 Descriptions

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

5.3.2.2 Objectives

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.

5.3.2.3 Requirements

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

a) operations security;

b) physical security;

c) access control;

d) communications security;

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

5.3.3 Database System Configuration and Vulnerability Assessment (DBA)

5.3.3.1 Descriptions

Detailed technical assessment on the database system configuration as per the CMI organisation's security policies and industry standards in protecting the confidentiality, integrity and availability of CMI's information assets.

5.3.3.2 Objectives

The purpose of this test is to conduct a detailed technical assessment on the database's system configuration as per the Center of Internet Security's (CIS) Security Benchmarks and relevant industry standards in protecting the confidentiality, integrity and availability of the CMI's information assets.

5.3.3.3 Requirements

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 authorization;

g) network;

h) database replication;

i) vulnerability assessment for known vulnerabilities and outdated database software packages;

j) physical security.

5.3.4 Security Policy Review (SPR) and Gap Analysis

5.3.4.1 Descriptions

Security Policy Review (SPR) exercise aims to identify the gap in the CMI organisation's information security policies and controls implementation that is based on the ISO/IEC 27001:2013, the international standard for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the contexts of information security management of the organisation.

5.3.4.2 Objectives

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

5.3.4.3 Requirements

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.

5.4 Important considerations

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

a) Security Assessor's industry experience with proven businesses and operational processes in managing SPA Program requirements for CMI.

b) Certified security professionals and subject matter experts with proven good experience in managing SPA Program for CMI;

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 should be considered by the CMI's organisations prior to engaging the SPA Program shall include the followings:

a) engagement objective, scope and limitation;

b) security assessor qualification and conflict of interest Consideration;

c) assurance of confidentiality, integrity and availability.

6. Engagement objective, scope and limitation

6.1 Engagement Objective

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

The recognised objectives of a successful SPA Program for CMI include:-

a) well-structured approaches and methodologies in the identification of the security vulnerabilities and risks that are associated with the CMI's ICT infrastructure;

b) well-managed security risks from the technical and operational perspectives for ensuring the confidentiality, integrity, availability and auditability of CMI's 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 CMI's organisation network, system and application infrastructure with reference to the latest industry standards and best practices.

6.2 Scope and limitation

The scope for CMI shall cover:

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 vs. business requirements? Test approach and 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 three (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 (this is not an exhaustive list):

a) Is the company specialising in Penetration Testing/Security Posture Assessment?

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

c) Have the company being 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 / Security Posture Assessment exercise?

7.2 Security Assessor experience and professional credentials

The security assessor may perform the security posture assessment as long as 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 security posture assessment for the CMI, that party cannot perform the security posture assessment if they were involved in the installation, maintenance, or support of target systems for the CMI. The following guidelines may be useful when selecting a Security Assessor (or team) to understand their qualifications to perform security posture assessment:

Certifications held by Security Assessor (or team) 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);

b) Certified Ethical Hacker (CEH) by EC-Council;

c) Offensive Security Certified Professional (OSCP) by Offensive Security;

d) Global Information Assurance Certification (GIAC) Certifications (e.g., GIAC Certified Security Assessor (GPEN), GIAC Web Application Security Assessor (GWAPT), or GIAC Exploit Researcher and Advanced Security Assessor (GXPN));

e) CREST Certified Testers (CREST Certified Tester Application (CCT-APP), CREST Certified Tester Infrastructure (CCT-INF)).

7.3 Past Experience

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 (this is not an exhaustive list):

a) How many years' experience does 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 (i.e., operating systems, 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

CMI shall avoid to engage the Security Assessor's company that has potential tendency to be in conflict of interest with SPA objectives of the CMI's organisations.

8. Assurance of Confidentiality, Integrity and Availability

A SPA Program constitutes a special type of project, where it is often a challenge for CMI's organisation to ensure of the followings and not limited to:-

a) Confidentiality - such as sensitive information is shared prior, during and after the project is being properly managed by the appointed Security Assessor and/or subject matter expert;

b) Integrity - the fact that the Security Assessor shall likely be exposed to CMI's organisation sensitive information and/or have administrator (super user) access to the business critical information systems;

c) Availability - the Security Assessor may require to execute harmful test vulnerability exploits and test programs that mimicking a real attack that often harmful and may cause disruption to the business and system operations if they are not being managed in a controlled environment.

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 Program for the CMI organisation, which shall not be a one-time exercise to analyse vulnerabilities, fix security issues and safeguard sensitive data.

However, outsourcing security in which a service provider is called in might increase certain risk. CMI's organisations need to be cautious when outsourcing the SPA Program services as it requires implicit trust in the third-party Security Assessor and its ability to vet employees and provide trustworthy, trained, experienced consultants. Security Assessors have necessarily access to large amount of information and, theoretically, could leave backdoors and vulnerabilities in the system during their testing.

Therefore, before the CMI's organisation allows the third party Security Assessor to install software on the target systems to do more in-depth probing, it is important to check for proven customer service and an excellent track record.

9. SPA program planning and management

The Security Assessor shall provide in details on the methodology that shall be used for the SPA program for CMI. For ensuring a successful implementation and management of a SPA Program, there are several activities and processes to be considered beyond the testing itself. This section provides guidance for these activities and organised by phases which include:

a) phase 1 (pre-assessment);

b) phase 2 (assessment);

c) phase 3 (post-assessment).

9.1 Planning

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

   i) define assessment goals;

   ii) select assessment team;

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

   iv) risk assessment on the risks of confidentiality, integrity and availability of CMI's information assets;

   v) 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.

b) The SPA Program and its exercises for CMI 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 SPA program phases

The followings are the main SPA program activities and prerequisites that need to be carefully managed for ensuring the confidentiality, integrity and availability 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. CMI 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.

Some of 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;

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 program 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; and

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 Program exercise reports and deliverables, a Management Review Meeting shall be be organised to present the overall of findings and risks to management personnel of the CMI's 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 program 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, to name a few

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 CMI's 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, to name a few.

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;

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

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 :

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

b) name(s).

10.2 Qualification of project manager

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 is 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 can 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.

The following guidelines may be useful when selecting a project manager to understand their qualifications to manage the security posture assessment project:

Certifications

As project managers work with various methodologies, preferably certified or qualified in the required competencies. These methodologies or techniques allow project managers to resolve complex problems in fast-paced, dynamic environments. It is recommended for the project manager to have qualifications specific to the industry, such as PRINCE2®, PMP or ITIL.

Nevertheless, the followings skills and experience are also considered as essential (including but not limited to) for a project manager in ensuring the success of the SPA project for the CMI:

a) client presentations;

b) effective communication (oral & written);

c) leadership.

11. Reporting requirements

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

11.1 Outline of SPA reports

The reports provided for each SPA exercises shall meet the following minimum requirements as Table 4 below:

Table 4. Reports requirement

Executive Summary	Brief high-level summary of the security posture assessment scope and major findings.
Scope of Works	A detailed definition of the scope of the network and systems tested as part of the assessment : a) Clarification systems or segments that are considered during the test b) Identification of critical systems and explanation of why they are included in the test as targets
Statement of Methodology	Details on the methodologies used to complete the testing (port scanning, nmap 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/how the systems / host / application may be exploited using each vulnerability. b) Proof of concept / Evidences c) Risk ranking/severity of each vulnerability d) Targets affected e) References (if available) i. CVE, CWE, BID, OSBDB, etc. ii. Vendor and/or researcher f) Description of finding
Tools Used	In additional to manual scripting techniques, the assessment tools utilized that comprises freeware (open source), commercial and proprietary tools, must be listed.
Appendix	

11.2 Outline of post assessment report

The security posture assessment findings shall require remediation and retesting , a post remediation report must also be provided.

All remediation efforts shall be completed and retested within a reasonable period of time after the original security posture assessment report was provided. It is expected that the post remediation report shall cover all identified/exploitable vulnerabilities that require remediation.

The following is an example of the sections to include in a post remediation report as (but not limited to):

a) executive summary;

b) date of original test;

c) date of re-test;

d) original findings;

e) results of re-test.

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

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

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

a) 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.

b) 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.

c) Protection of records

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

d) Privacy and protection of personally identifiable information such as PDPA.

14. Vulnerability category and risk rating

CMI 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 program.

Table 5 can be used as a reference in the determining the risk level that are associated with the common vulnerabilities identified in a SPA program.

Table 5. Vulnerability category and risk rating

Reference	Risk Rating	Descriptions
Denial-of-Service (DOS)	High	This type of vulnerability if exploited would cause service disruption to a single or multiple system functions.
Weak Password (PWD)	High	This type of vulnerability would allow attacker to easily gain access directly to the system by password guessing.
Gain Privileged User Access (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 authorization mechanisms.
Sensitive Information Disclosure (DBI)	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 SQL injection attacks.
Man-in-the-Middle (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 Brute Force (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 Configuration (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.

Table 5. Vulnerability category and risk rating *(continued)*

Reference	Risk Rating	Descriptions
Enumeration (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 enumeration are the network resources and shares, users and groups, system and application services, etc.
Reconnaissance (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.

Acknowledgements

Members of the Trust and Privacy Sub Working Group

Mr Yew Seng Ong (Chairman)	Provintell Technologies
Ms Humairah Ahmad Nasir/ (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Ahmad Taufik Nik Nor Azlan	
Mr Azlan Mohamed Ghazali	Celcom Axiata Berhad
Ms Faridah Ibrahim	Kementerian Sains, Teknologi dan Inovasi (MOSTI)
Mr Azleyna Ariffin/	Malaysian Communications and Multimedia
Mr Ruzamri Ruwandi/	Commission
Ms Wan Rosmawarni Wan Sulaiman	
Mr Nicholas Ng	Provintell Technologies
Mr Thaib Mustafa	Telekom Applied Business Sdn Bhd
Mr Mohd Azrin Muhamad Nor/	Telekom Malaysia Berhad
Mr Mohd Shahrul Azamer Rumli/	
Ms Rafeah Omar/	
Mr Mohamad Azhar Abdullah	
Mr Wan Ahmad Ezani Wan Mohamed	TIME dotCom Bhd
Prof Dr Shahrulniza Musa	Universiti Kuala Lumpur
Mr Shadil Akimi Zainal Abidin/	
Ms Roziyani Rawi	
Ms Farah Nuamirha Mohamad/	webe digital sdn bhd
Mr Haizam Abu Hassan	