TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - SECURITY POSTURE ASSESSMENT (SPA)

Developed by

Registered by

Registered date:

15 October 2018

MCMC MTSFB TC G016:2018

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
Cyber 6
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

Provintell Technologies Sdn Bhd

Telekom Applied Business Sdn Bhd

Telekom Malaysia Berhad

TIME dotCom Berhad

Universiti Kuala Lumpur

webe digital sdn bhd

Foreword

This technical code for Information and Network Security - Security Posture Assessment (SPA) ('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.

This technical code served as a supplement document to part 4 of 'MCMC MTSFB TC G009 - Requirements for information and network security' to establish the technical risk assessment for the risk management requirements.

Security Posture Assessment (SPA) is a cyber security assessment programme that is specifically developed to provide the structured security risk and vulnerability assessment approach and methodology to support the SPA objectives.

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

INFORMATION AND NETWORK SECURITY - SECURITY POSTURE ASSESSMENT (SPA)

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 (SPA) to maintain a current picture of their vulnerabilities, allowing them to prioritise remediation activities based on available resources and business risk. Thus, SPA is essential for every organisation. This exercise will examine and test Confidentiality, Integrity and Availability (CIA) of the information infrastructure used by the organisation.

SPA 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; 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 the 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 organisations to prepare for the security testing, conduct actual testing in a consistent, competent manner and follow up tests effectively.

b)   Providing overview of the key concepts the organisations need to understand in order to conduct a well managed SPA programme, the evaluation criteria and the process to employ an external security assessor in supporting the 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.

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

Center of Internet Security (CIS) Controls (Version 6.1), CIS benchmarks

Personal Data Protection Act (PDPA) 2010

3. Terms and definitions

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

3.1 Black-box testing

No information is provided to the assessor prior to the security assessment; to simulate external attacks with no prior knowledge of the target environment - and understand what is possible for an uninformed attacker to achieve.

3.2 Grey-box testing

Limited information is provided to the assessor prior to the security assessment, eg. login credentials to a system or visitor access to a site; to understand the degree of access that authorised users of a system can obtain – and the possible damage caused by insider or privileged attacks with some knowledge of the target environment.

3.3 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.

3.4   SPA exercise

The security assessment activities that identify and evaluate the vulnerabilities of the particular components that are used to process organisational information assets.

3.5   SPA programme

A series of planned SPA exercises that employ the enterprise risk assessment approach and include all stakeholders to ensure that all aspects of the IT organisation are addressed, including hardware and software, employee awareness, and business processes.

3.6   SPA project

A full or partial SPA program that is outsourced to third party for execution in an agreed time interval shall be managed as a project to meet the intended outcome.

3.7   Threat

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

3.8   Vulnerability

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

3.9   White-box testing

Full information is provided to the assessor prior to the security assessment, for example application source code, network maps and access to development staff; to support a more targeted test on a system that requires a test of as many vulnerabilities and attack vectors as possible.

4.   Abbreviations

For the purposes of this Technical Code, the abbreviations in Annex A apply.

5.   General requirements

5.1   Cyber security assessment programme structure

The SPA programme aims to provide the 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 programme as shown in Table 1. The results shall meet the testing objective, business requirements, regulatory compliance and ensuring appropriate actions are being taken.

Table 1. SPA programme structure

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) Host operating system configuration and vulnerability assessment (HA) b) Perimeter security device configuration and vulnerability assessment (PDA) c) Database configuration and vulnerability assessment (DBA) d) Security Policy Review (SPR) and gap analysis

5.2 Vulnerability Assessment and Penetration Test (VAPT)

5.2.1 Infrastructure penetration test

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

The purpose of this test is to perform either intrusive or non-intrusive vulnerability assessment and exploitation techniques toward the 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 network infrastructure.

5.2.1.1 External Penetration Test (EPT)

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

The main activities for External Penetration Test (EPT) shall include but not limited to the followings:

a) Step 1 (intelligence gathering)

   i)   internet footprinting, such as internet registry check, Domain Name Server (DNS), website, mail and other common internet services checks, multi Realtime Blackhole Lists (RBLs) such as DNS Blacklist/Blocklist (DNSBL) and Uniform Resource Identifier Blaclist (URIBL) checks;

   ii) network reconnaissance and identify perimeter security mechanisms such as firewalls, Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS);

   iii) identify the remote operating system types;

   iv) identify remotely accessible services, type and version; and

v)   identify cleartext protocols used.

b)   Step 2 (vulnerability assessment)

i)   vulnerability scanning using multiple commercial vulnerability scanning tools;

ii)   vulnerability analysis to identify default system and services configuration and remotely exploitable vulnerability;

iii)   prepare vulnerability exploitation test plan which describes the exploitation tools and techniques; and

iv)   identify and describe the possible system impact on the exploitation techniques used.

c)   Step 3 (security testing and risk analysis)

i)   conduct vulnerability exploitation and Proof of Concept (POC);

ii)   identify the remotely exploitable vulnerability types such as:

   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)   Enumeration (ENUM); and

   9)   Reconnaissance (RECONS).

iv)   analyse the vulnerability's risk level based on the risk assessment methodology.

d)   Step 4 (reporting and presentation of findings)

i)   documentation of the security evidences and findings;

ii)   vulnerability research to provide the security recommendations based on the latest security trends and best practices;

iii)   management and technical reports preparation, review and finalisation; and

iv)   conduct technical and management presentations on the findings such as the vulnerability and risk overview to top management and risk owners, the detailed technical findings and recommendations to the system owners for vulnerability remediation.

e)   Step 5 (vulnerability retest and verification (post assessment))

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

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

iii) update of the vulnerability status and risk level; and

iv) preparation, review and finalisation of the post assessment report.

5.2.1.2   Internal Penetration Test (IPT)

Vulnerability assessment and exploitation activities toward the 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.

The main activities for Internal Penetration Test (IPT) shall include but not limited to the followings:

a)   Step 1 (intelligence gathering)

i) network reconnaissance and identify the local network topology of Internet Protocol (IP) or non-IP based network infrastructure;

ii) identify internal network's packet filtering mechanisms such as firewall, IDS or IPS;

iii) identify target hosts' operating system types;

iv) identify locally accessible services, type and version; and

v) identify cleartext protocols used.

b)   Step 2 (vulnerability assessment)

i) vulnerability scanning using multiple commercial vulnerability scanning tools;

ii) vulnerability analysis to identify default system and services configuration and remotely exploitable vulnerability;

iii) network packets sniffing for cleartext passwords and other useful information;

iv) prepare vulnerability exploitation test plan which describes the exploitation tools and techniques; and

v) identify and describe the possible system impact on the exploitation techniques used.

c)   Step 3 (security testing and risk analysis)

i) conduct vulnerability exploitation and POC;

ii) identify the remotely exploitable vulnerability types such as:

1) DOS;

2) weak PWD;

3) PUA;

4) DBI disclosure;

       5)   MITM;

       6)   susceptible to BRUF;

       7)   weak system CONF;

       8)   ENUM; and

       9)   RECONS.

    iii)   analyse the vulnerability's risk level based on the risk assessment methodology.

d)   Step 4 (reporting and presentation of findings)

    i)   documentation of the security evidences and findings;

    ii)   vulnerability research to provide the security recommendations based on the latest security trends and best practices;

    iii) management and technical reports preparation, review and finalisation; and

    iv) conduct technical and management presentations on the findings such as the vulnerability and risk overview to top management and risk owners, the detailed technical findings and recommendations to the system owners for vulnerability remediation.

e)   Step 5 (vulnerability retest and verification (post assessment))

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

    ii)   vulnerability retest shall focus and prioritise on the remediation activities that are associated with the high risk vulnerabilities and to be completed immediately upon the vulnerability discovery;

    iii) update of the vulnerability status and risk level; and

    iv) preparation, review and finalisation of the post assessment report.

5.2.2   Application security test

This test covers the various applications used by the organisation and its subscriber side such as web application, mobile application and client based application.

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

The requirements shall be as folllows:

a)   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 organistion 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 Structured Query Language (SQL), operating system, and Lightweight Directory Access Protocol (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.
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 User Interface (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 Hyper Text Transfer Protocol (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.

b) Static Application Security Test (SAST)

The Static Application Security Test (SAST) 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 activities as in 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, CSRF 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 DOS. Resources can be file system objects memory, Central Processing Unit (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.
Application Program Interface (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 do not 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 Secure Sockets Layer (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 Uniform Resource Locator (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 organisation. This is to ensure the CPE provider undergone/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.

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; and

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 services and infrastructure offered by the organisation. The security test for telecommunication and signaling technologies will enable the organisation to uncover threats in their environment.

5.2.4.2 Objectives

The purpose of this test is to identify vulnerability and weaknesses that may lead to data interception, privacy violation, DOS, acquiring sensitive data, spoofing, data tampering and unauthorised access to the organisation's infrastructure.

5.2.4.3 Requirements

The security tests on telecommunication and signaling technologies shall focus and may not be limited to the following areas:

a) evolved packet core and 4th Generation (4G) cellular network technology;

b) legacy telecommunication technology Signaling System 7 (SS7), packet switching and circuit switching technology; and

c) high speed broadband network.

The security test shall meet the following objectives:

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

b) uncover DOS scenario that caused service disruptions;

c) uncover eavesdropping on data and voice communication technology;

d) uncover possibility of identity spoofing for fraudulent purposes; and

e) 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.

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; and

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 Host Operating System Configuration and Vulnerability Assessment (HA)

5.3.1.1 Descriptions

Detailed operating systems security configuration and vulnerability assessment as per Center for Internet Security (CIS) controls, organisation security policies and other industry best practices in protecting the CIA of the organisational 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; and

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 organisation's security policies and industry standards in protecting the CIA of organisational 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; and

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 organisation's security policies and industry standards in protecting the CIA of organisationl 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 CIS benchmarks and relevant industry standards in protecting the CIA of the organisational information assets.

5.3.3.3 Requirements

The main activities of Database System Configuration and Vulnerability Assessment (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; and

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 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.

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 the organisation 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; and

e)   reporting.

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 organisational growth and sustainability.

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

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

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 (this is not an exhaustive list):

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 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 or SPA exercise?

7.2 Security assessor experience and professional credentials

The security assessor may perform the SPA 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 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.

The following items may be useful when selecting a security assessor (or team) to understand their qualifications to perform SPA:

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);

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

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

e) 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)); and/or

f) 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

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 7 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 details 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 section 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 risks of CIA of the organisational 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; 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 programme 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 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;

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:

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

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 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):

a)   client presentations;

b)   effective communication (oral & written); and

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 Outline of Security Posture Assessment (SPA) reports

The reports provided for each SPA exercises shall meet the following minimum requirements as stated in Table 4.

Table 4. Reports requirement

Items	Minimum requirements
Executive summary	Brief 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: a) clarification systems or segments that are considered during the test; and b) ID 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, 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/how the systems/host/application may be exploited using each vulnerability.
	
	b) POC/evidences.
	
	c) risk ranking/severity of each vulnerability.
	
	d) targets affected.
	
	e) references (if available):
	
	   i) Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), Bugtraq ID (BID), Open Source Vulnerability Database (OSVDB), etc.; and/or
	
	   ii) vendor and/or researcher.
	
	f) description of finding.

Tools used	In additional to manual scripting techniques, the assessment tools utilised that comprises freeware (open source), commercial and proprietary tools, shall be listed.
Appendix	(if necessary)

11.2 Outline of post assessment report

The SPA findings shall require remediation and retesting, a post remediation report shall also be provided.

All remediation efforts shall be completed and retested within a reasonable period of time after the original SPA 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 retest;

d)   original findings; and

e)   results of retest.

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; and

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 (ID) 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 legislatory, regulatory, contractual and business requirements.

13.4   Privacy and personal protection

Privacy and protection of personally identifiable information such as Personal Data Protection Act (PDPA) 2010.

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 risk level that are associated with the common vulnerabilities identified in a SPA programme should refer to Table 5.

Table 5. Vulnerability category and risk rating

Reference	Risk Rating	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.
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 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
(informative)

Abbreviations

4G	4th Generation
API	Application Program Interface
BID	Bugtraq ID
BRUF	Susceptible to Brute Force
CCT-APP	CREST Certified Tester Application
CCT-INF	CREST Certified Tester Infrastructure
CEH	Certified Ethical Hacker
CIS	Centre of Internet Security
CISSP	Certified Information Systems Security Professional
CONF	Configuration
CPE	Customer Premise Equipment
CPU	Central Processing Unit
CRISC	Certified in Risk and Information Systems Control
CSRF	Cross Site Request Forgery
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DAST	Dynamic Application Security Test
DBA	Database Configuration and Vulnerability Assessment
DBI	Database Information
DNS	Domain Name Server
DNSBL	DNS Blacklist/Blocklist
DOS	Denial of Service
ENUM	Enumeration
EPT	External Penetration Test
GIAC	Global Information Assurance Certification
GPEN	GIAC Certified Security Assessor
GWAPT	GIAC Web Application Security Assessor
GXPN	GIAC Exploit Researcher and Advanced Security Assessor
HA	Host Operating System Configuration and Vulnerability Assessment
HTTP	Hyper Text Transfer Protocol
ICT	Information Communications Technology
ID	Identification
IDS	Intrusion Detection Systems

IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPT	Internal Penetration Test
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITIL	Information Technology Infrastructure Library
LDAP	Lightweight Directory Access Protocol
MITM	Man-in-the-Middle
NDA	Non-Disclosure Agreement
OSVDB	Open Source Vulnerability Database
OSCP	Offensive Security Certified Professional
PDA	Perimeter Security Device Configuration and Vulnerability Assessment
PDPA	Personal Data Protection Act
PMP	Project Management Professional
POC	Proof of Concept
PRINCE2	PRojects IN Controlled Environments
PUA	Privileged User Access
PWD	Password
RBL	Realtime Blackhole Lists
RECONS	Reconnaissance
SAST	Static Application Security Test
SBA	Security Baseline Assessment
SIM	Subscriber Identification Card
SPA	Security Posture Assessment
SPR	Security Policy Review
SQL	Structured Query Language
SS7	Signaling System 7
SSL	Secure Sockets Layer
URIBL	Uniform Resource Identifier Blacklist
UI	User Interface
URL	Uniform Resource Locator
VAPT	Vulnerability Assessment and Penetration Test
XSS	Cross Site Scripting

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]   *Open Web Application Security Project (OWASP)*, the OWASP foundation

Acknowledgements

Members of the Trust and Privacy Sub Working Group