Penetration Testing Guidelines 2.0

for the Financial Industry in Singapore

The Association of Banks in Singapore

April 2024

Table of Contents

1. Executive Summary

The security of IT systems is paramount to maintaining trust and confidence in the services provided by Financial Institutions (FIs) in Singapore to their customers.

This document is a set of guidelines for penetration testing to ascertain the effectiveness of the security controls put in place to preserve the confidentiality, integrity and availability of IT systems. This document is not intended to be a compliance document and FIs should check against prevailing regulatory requirements.

Penetration testing may be performed at a cadence determined by respective FIs based on system criticality and exposure to cyber risk. It is a good practice to conduct penetration testing on systems that are directly accessible from the internet at least once every year and when the systems undergo major changes or updates.

2. Definitions

2.1 FIs refers to the Financial Institutions, including members of the Association of Banks in Singapore.

2.2 Penetration testing is security testing in which the penetration testers mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. Penetration testing represents the results of a specific tester or group of testers at a specific point in time using agreed-upon rules of engagement.

2.3 Vulnerability assessment is the process of identifying, assessing and ranking security vulnerabilities in a computer system through broad port scanning. Vulnerability assessment is typically done by running automated tools and is different from a penetration test.

2.4 Production environment refers to the environment providing the service to end users and customers (internal or external).

2.5 Credentialed testing refers to authenticated testing with login credentials provided to the tester.

2.6 OWASP refers to the “Open Worldwide Application Security Project” (owasp.org) that provides best security practice recommendations and maintains a list of Top 10 Risks Web Application findings.[1]

2.7 SANS refers to the “SysAdmin, Audit, Networking, and Security” Institute (sans.org) that provides best security practice recommendations and maintains a list of the Top 25 Most Dangerous Software Errors.[2]

2.8 CVE refers to Common Vulnerability and Exposures. CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE’s common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.[3]

2.9 CVSS refers to Common Vulnerability Scoring System. CVSS provides a universally open and standardised method for rating IT vulnerabilities.[4]

2.10 CWE refers to Common Weakness Enumeration, a formal list or dictionary of common software weaknesses that can occur in a software’s architecture, design, code or implementation that can lead to exploitable security vulnerabilities.[5]

2.11 Software weaknesses refers to flaws, faults, bugs, vulnerabilities and other errors in software implementation, code, design, or architecture that if left unaddressed could cause systems and networks to be vulnerable to attacks. Examples of software weaknesses include:

- buffer overflows;

- format strings;
- structure and validity problems;
- common special element manipulations;
- channel and path errors;
- handler errors;
- user interface errors;
- pathname traversal and equivalence errors;
- authentication errors;
- resource management errors;
- insufficient verification of data;
- code evaluation and injection; and,
- randomness and predictability.

2.12 Common Attack Pattern Enumeration and Classification (CAPEC) refers to the most common methods threat actors use to exploit vulnerabilities resulting from CWEs. Used together, CWE and CAPEC provide understanding and guidance to software development personnel of all levels as to where and how their software is likely to be attacked, thereby equipping them with the necessary information they need to help them build more secure software.

3. Introduction

The Penetration Testing Guidelines reflect the latest industry best practices and provide a baseline penetration testing framework for FIs and members of the Association of Banks in Singapore, as well as their vendors and contractors that perform the same task. There are other industry guidelines on penetration testing that are developed by organisations, such as Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST), PCI Security Standards Council (PCI SSC), and the Institute for Security and Open Methodologies (ISECOM), that FIs may utilise.[6] These frameworks offer extensive coverage, industry-standard best practices, and effective risk mitigation strategies.

Penetration testing is one of the many security activities that FIs can conduct to assess their security posture (refer to Appendix B for a summary of the different types of security assessments FIs may consider). FIs may develop a strategy for the types of security assessments that they will implement to meet their security objectives. This document focuses on penetration testing, covering the phases from planning to discovery, attack, reporting, and retest.

FIs may refer to this document as guidance for penetration testing approach but not for compliance. The Technology Risk Management Guidelines published by the Monetary Authority of Singapore may be taken as a reference for the reader to understand the expectations set out by the regulator for FIs in Singapore.[7]

4. Penetration Testing Styles

There are three types of penetration testing styles – Blackbox, Greybox, and Whitebox. These styles differ according to the amount of information penetration testers have access to, the context of the application, and the desired test outcomes.

Table 1: Blackbox, Greybox, and Whitebox

Types	Blackbox	Greybox	Whitebox
Description	No internal knowledge of the target system is provided to the penetration tester.	Limited information is provided to the penetration tester, e.g., login credentials.	All relevant information is provided to the penetration tester, including architecture documentation and source code.
Purpose	Blackbox testing is used to test if the system is	Greybox testing is typically used to assess the level of privilege a	Whitebox testing aims to identify potential weaknesses in various

	penetrable to real malicious threat actors.	normal user could gain and the potential damage they could cause. It is used to simulate an insider threat or an external attack where the malicious actor has breached the network perimeter.	areas such as logical vulnerabilities, potential security exposures, security misconfigurations, poorly written development code, and lack-of-defensive measures.
Benefits	It is the most realistic option as the test largely depends on the penetration tester's ability to locate and exploit vulnerabilities in the target network or application.	Greybox tests strike a balance between depth and efficiency. The additional information furnished to the penetration testers would enable them to penetrate the system and exploit vulnerabilities more efficiently than blackbox. It also reduces the time spent by the penetration tester to gather information.	With the amount of information available to the tester, whitebox tests enable penetration testers to capture more vulnerabilities as compared to black and greybox tests.
Considerations	If the security perimeter cannot be breached, then any vulnerabilities of internal services or post-authenticated pages for web applications and network may remain undiscovered and unpatched.	Greybox testing is more comprehensive than Blackbox testing. However, it is time-consuming to conduct. It does not simulate a true external attack as additional information is provided to the testers.	It is a time-consuming exercise to run through the large amount of data to identify potential points of weakness and may not give an accurate understanding of the risk associated with the vulnerabilities detected.

5. Types of Penetration Tests

Penetration tests are typically carried out periodically, for example through annual penetration test, and when existing systems undergo changes or new systems are implemented. The former is also broader in scope as compared to the latter. For instance, if an administrative web console is discovered during a network scan, a web application test on the exposed service can be considered as a follow-up action.

Below are the different types of penetration testing that FIs typically carry out. The list is non-exhaustive:

Network Penetration Testing

Network penetration testing is performed to identify vulnerabilities on host systems and network devices that can be exploited by a threat actor. It includes network discovery, which incorporates network mapping, host identification, and service enumeration, and network vulnerability assessment, where unnecessary or unauthorised hosts and services are identified and exploitation where applicable.

Web Application Penetration Testing

Web application penetration testing is performed to identify and assess weaknesses and vulnerabilities on web applications that can be exploited by threat actor. Web application penetration testing can be conducted on services and applications discovered during network testing or those that have undergone major changes.

Mobile Application Penetration Testing

Mobile Application Penetration Testing is performed as native mobile applications may contain weaknesses or vulnerabilities in the communications channel, server-side infrastructure and client software running on the mobile device.

API Penetration Testing
Application Programming Interface (API) penetration testing is performed as APIs are a software intermediary between different applications or systems. Modern web and mobile applications use APIs, and organisations also expose their API gateways to third parties for Business-to-Business (B2B) integration.

Thick Client Penetration Testing
Thick client penetration testing is performed as thick clients in financial organisations are used to provide desktop experience in environments where the end user has a well-defined and regular number of tasks for which the system is used. Thick clients usually communicate with the application server using API frameworks or Transmission Control Protocol (TCP) protocols. The difficulty of testing Thick clients which are communicating using TCP protocols are higher as the penetration tester needs to capture and analyse the TCP traffic first, before attempting to intercept and modify TCP session connections.

Wireless Penetration Testing
Wireless Penetration Testing is performed as wireless networks are commonplace in organisations to provide seamless network connectivity for internal employees and devices. Sometimes, a dedicated wireless network is also created specifically for guests. It is important to acknowledge that these wireless networks can inadvertently present a potential entry point for threat actors to breach the organisation’s network especially in the presence of misconfigurations or vulnerabilities.

Mainframe applications penetration testing
Mainframe applications penetration testing is performed to identify and assess weaknesses and vulnerabilities on Mainframe applications that can be exploited by threat actor. The common approach is to perform an automated Static Application Security Testing (SAST) / Expert Security Code review.

Hardware penetration testing
Hardware penetration testing is performed to identify and assess weaknesses and vulnerabilities on the physical devices and interfaces of a system (e.g Laptops, Thin clients in the office, presentation devices, Surface Pro tablets). The scope of the test should include review of OS image, USB-device related attacks, removing HDD and checking presence of BitLocker, etc.

IoT Penetration testing
IoT Penetration testing is performed as there is widespread adoption of IoT devices to enhance efficiency and connectivity inside an organisation, and this introduces new entry points for cyber threats. It is crucial to recognise that these interconnected devices can unintentionally presents potential loopholes for threat actors to compromise the organisation's overall security posture. By thoroughly evaluating the functionality and security protocols of IoT devices, organisations can ensure that sensitive data remains protected and that the devices themselves do not become inadvertent gateways for cyberattacks.[8]

6. Test Environments

There are two main types of environments that can be used to conduct penetration testing, (i) production, and (ii) non-production environments. The environment in which the penetration test is performed should be clearly specified in the final report.

FIs may determine the environment to be used based on FIs’ risk assessment. Penetration testing may be performed against a production environment, where possible. This would help surface weaknesses in the actual production systems and networks that could pose immediate risk. However, FIs should assess the associated operational risks based on the principles listed below. If the risks in the assessment are significant, the test could be performed in a production-like environment.

There are several principles to consider, such as:

1. *Data Integrity.* For example, credentialed testing may impact the integrity of information and, if done in the production environment, the test production credentials could potentially be utilised for illegal activities, such as fraud/money laundering.

2. *Data Confidentiality.* Penetration testing performed against a production environment may lead to potential access to confidential data (e.g. CID). For non-production environment penetration testing, only test data should be used.
3. *Service Impact.* FIs may consider whether there is a high risk that the penetration testing may result in service outage, causing clients or customers to lose access to, or result in destructive outcomes where the entire system becomes unusable.
4. *Feasibility.* For example, pre-live testing for newly built services/applications may be done in non-production environment since the production environment is not yet launched.
5. *Penetration Testing Style*. Greybox and whitebox testing may be more intrusive and riskier than blackbox testing.

Penetration tests done in production environment should include proper safeguards, such as those listed below, and these may be established in the rules of engagement:

- Notify monitoring teams and system custodians/owners about ongoing tests.
- Clean up and ensure test artifacts and hacking tools are removed after the test, if any.
- Promptly remove all test production credentials or any temporary access rights granted for the test upon completion of assessment.
- Leverage a controlled penetration testing to ensure no service outage. This may include restricting the testing hours or limiting reach in exploiting certain security vulnerabilities, such as remote code execution, SQL injection, etc.
- Ensure there is adequate backup for the production environment and ability to recover from a backup should the penetration test takes down a system.
- Adequately segment the production environment so that penetration testing traffic is restricted from reaching unintended systems that are not within the testing scope.
  Ensure data protection measures are taken. For example, mock data should be used in place of production data in test cases where data is expected to be transmitted out of company network to prevent potential production data leakage.
- Production data should not be stored and proper clean up procedures should be in place.
- Tests which can modify production data and disrupt business operations or cause error in transactions should not be allowed. These may include resetting of existing passwords or injection attacks that will create persistent data in the production environment. Consideration should be given to the option to conduct these tests in an environment that mirrors the production environment.
- The penetration testing should be done under the FI's monitoring. This ensures the activities carried out by the service providers are within the intended scope of the test and do not disrupt operations.

A non-production environment refers to an environment that hosts similarly configured non-production systems. These are environments which host systems whose configurations and software versions mirror the production environment, including, but not limited to, staging and user acceptance test environments. When a non-production environment is used for testing, the differences in the setup between the non-production and production environments, as well as the applicability of the test findings to the production environment should be assessed and documented in the penetration test report.

7. Phases in Penetration Testing

Penetration testing phases may be grouped into five main phases: (i) planning, (ii) discovery, (iii) attack, (iv) reporting, (v) retest. While these are the basic grouping, they only serve as guiding principles as different FIs may have varying phases depending on their preferred approaches.

7.1 Phase 1: Planning

Penetration testing is a resource-intensive exercise that also poses risks to the FI. To ensure that the testing is well-resourced and risks are minimised during the execution, planning is an integral part of penetration testing. It includes determining the rules of engagement and seeking the appropriate management approval, where necessary.

The testing scope is determined at the planning stage and covers online services and infrastructure that are internet-facing and within the FI direct control. For outsourced environment, outsourcing vendor should also conduct annual penetration testing for their public internet facing network infrastructures. Outsource vendors are expected to follow the methodology as laid out in this document

7.2 Phase 2: Discovery

The Discovery Phase is for penetration testers to gather information and understand the target systems, as well as plan an attack strategy. Different FIs may rely on various sources of information through either active or passive methods. Passive reconnaissance pulls information from publicly available resources, whereas active reconnaissance involves direct interaction with the target system to gain information, including web reconnaissance and network mapping.

7.3 Phase 3: Attack

The Attack Phase is the stage where the penetration testers start to scan for vulnerabilities. They could attempt to exploit the vulnerabilities or perform proof of concepts to validate the vulnerability identified and, in certain cases, gain access to sensitive information and resources. As exploitation might have an adverse impact on the systems, this phase needs to be carefully controlled and monitored. After the attack has been completed, the penetration testers should remove or clean up any exploitation artifact in the environment.

7.4 Phase 4: Reporting

The penetration test report provides clear and concise information to stakeholders (technical teams, senior management, and business owners) enabling them to understand the security risks and take appropriate actions to address them.

Vulnerability Severity Assessment

After the attack phase and vulnerabilities are identified, FIs may assess the vulnerabilities based on their preferred methodology (see sample of a report format below). There are several industry recognised standards that can be used to rate an issue's severity and one of them is Common Vulnerability Scoring System (CVSS). The CVSS provides an approach to capture characteristics of a vulnerability and produce a score reflecting its severity. The score would then be translated into a qualitative representation (such as low, medium, high, and critical) to help organisations properly assess and prioritise their vulnerability remediation process. CVSS is commonly used for classifying the severity of vulnerabilities discovered on a system which in turn is a factor to be considered when prioritising vulnerability remediation activities.

Table 2: Example of CVSS[9] qualitative severity rating scale:

Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Table 3: Sample of a penetration test report format

Executive Summary Penetration Tester Name Application Owner/Custodian Project Scope Timelines Reviewers' Names

Methodology

1. Environment tested (i.e., production-like*, production, end user protection application (Anti-virus software, RASP)*

2. Scope of System tested (i.e. Specific Version Build Provided for Mobile Testing, Host IP address, web application URL, test user accounts/roles, APIs details, Mobile OS version)

3. Findings

Overview [covers description of vulnerabilities, severity level (Critical, High, Medium, Low) and affected systems]

Register (Reference, Severity, Title, Impact summary, Status – Open/Closed)

Individual findings

a. Reference number

b. Severity

c. Title

d. CWE ID (optional, where applicable)

e. Documentation showing the proof of exploit

f. Fixes: Documentation on retest of findings raised for closure

g. CVSS Vector and Score (where applicable, if the risk rating is adjusted from the original CVSS score or FI approved scoring system, a justification should be documented.)

h. Scope (URL + Parameter or IP + Port)

i. Recommendation (The recommendation should be specific, feasible, and tailored to the FI's needs and resources. It may include suggestions for technical controls, process improvements, timelines, or staff training. Add literature references when applicable)

Details of the finding with sufficient elements to reproduce the findings, supported by screenshots, if applicable.

Notes:

- It is common to include screenshots, code snippets, or other evidence to support the findings.

- Penetration testing report contains confidential information of vulnerabilities and circulation should be limited on a need-to-know basis.-

7.5 Phase 5: Retest

Upon completion of the penetration testing and submission of the penetration test report, the FI will formalise a timeline to remediate the issues found during the assessment, based on risk appetite, threat vectors and compensating controls. Once security fixes or compensating controls are deployed, it needs to be validated through a retest to ensure that security vulnerabilities are successfully mitigated or remediated.

8. Penetration Tester Selection Criteria

When assessing a penetration tester, various aspects of their skills, experience, and approach should be considered to ensure a comprehensive evaluation. Here are some key areas to assess:

Technical Expertise and Experience

Evaluate the penetration tester's technical knowledge and skills. Inquire about the candidate's previous experience and specific projects he/she has worked on. For example:

(i) Number of years of relevant experience in penetration testing;
(ii) Where possible, public and endorsed vulnerability advisories published; and,
(iii) Where possible, experience in speaking in public during technical security conferences.

Continuous Learning

Technology used in FIs, and the cyber threats that they are subject to, are constantly evolving. Hence, penetration testers need to keep up with these trends to stay relevant and effective through continuous learning. It is recommended to identify evidence of the tester's commitment to continuous learning, including through presenting in security conferences, research projects, or other related professional contributions to the security community.

When engaging penetration testing service providers, FIs should obtain assurance of their policies and procedures on penetration testing engagement methodologies, reporting, and data handling, as well as employee background checks on security testers to protect the interest of FIs. The assurance could be provided for through avenues such as reviews conducted by FIs or accreditations by qualified parties.

Professional Certifications and Training

The security assessor may possess relevant certifications and training issued by internationally-recognised accreditation organisations/bodies, such as CREST, Global Information Assurance Certification (GIAC), OffSec (Offensive Security), (ISC)², INE, and other reputable certifications. Please refer to "**References**" section for more details. These certifications demonstrate a level of knowledge and commitment to the field. Additionally, verify if the tester attends regular training and keeps up with the latest security trends.[10]

Organisations may consider approaches to avoid complacency and blind spots, such as rotating penetration testers for the different applications of the Annual Penetration test or running a separate bug bounty program.

Appendix A: Penetration Testing-Related Professional Certifications

1. General Penetration Testing Certifications:
   a. CREST Registered Penetration Tester (CRT), source: https://crestapproved.wpengine.com/certification-careers/crest-certifications/crest-registered-penetration-tester
   b. OffSec Certified Professional (OSCP), source: https://www.offsec.com/courses/pen-200
   c. Global Information Assurance Certification (GIAC) Penetration Tester (GPEN), source: https://www.giac.org/certifications/penetration-tester-gpen
   d. eLearn Security Junior Penetration Tester (eJPT), source: https://security.ine.com/certifications/ejpt-certification/
   e. eLearn Security Certified Professional Penetration Tester (eCPPT), source: https://security.ine.com/certifications/ecppt-certification/

2. Web and Mobile Application Security Certifications:
   a. CREST Certified Web Application Tester (CCT APP), source: https://www.crest-approved.org/certification-careers/crest-certifications/crest-certified-web-application-tester
   b. OffSec Web Expert (OSWE), source: https://www.offsec.com/courses/web-300
   c. OffSec Web Assessor (OSWA), source: https://www.offsec.com/courses/web-200/
   d. GIAC Web Application Penetration Tester (GWAPT), source: https://www.giac.org/certifications/web-application-penetration-tester-gwapt
   e. GIAC Mobile Device Security Analyst (GMOB), source: https://www.giac.org/certifications/mobile-device-security-analyst-gmob
   f. eLearnSecurity Web Application Penetration Tester (eWPT), source: https://security.ine.com/certifications/ewpt-certification/
   g. eLearnSecurity Mobile Application Penetration Tester (eMAPT), source: https://security.ine.com/certifications/emapt-certification/
   h. Burp Suite Certified Professional (BSCP), source: https://portswigger.net/web-security/certification

3. Wireless and Network Security Certifications:
   a. CREST Certified Infrastructure Tester (CCT INF), source: https://www.crest-approved.org/certification-careers/crest-certifications/crest-certified-infrastructure-tester
   b. OffSec Wireless Professional (OSWP), source: https://www.offsec.com/courses/pen-210
   c. OffSec Exploit Developer (OSED), source: https://www.offsec.com/courses/exp-301/
   d. GIAC Assessing and Auditing Wireless Networks (GAWN), source: https://www.giac.org/certifications/assessing-auditing-wireless-networks-gawn
   e. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), source: https://www.giac.org/certifications/exploit-researcher-advanced-penetration-tester-gxpn
   f. OffSec Experienced Pentester (OSEP), source: https://www.offsec.com/courses/pen-300/

4. Cloud Security Certification:
   a. GIAC Cloud Penetration Tester (GCPN), source: https://www.giac.org/certifications/cloud-penetration-tester-gcpn

5. Information Security Management Certifications:
   a. Certified Information Systems Security Professional (CISSP), source: https://www.isc2.org/Certifications/CISSP#
   b. Certified Information Security Manager (CISM), source: https://www.isaca.org/credentialing/cism

6. OT Security Certification:
   a. GIAC Global Industrial Cyber Security Professional (GICSP), source: https://www.giac.org/certifications/global-industrial-cyber-security-professional-gicsp/

Appendix B: Other Security Activities

Penetration testing is one of the many types of security activities that FIs may embark on to test its security posture. These are some of the other types of security activities that firms may leverage to as part of their security assessment regime. This list is non-exhaustive.

1. Adversarial Attack Simulation Exercise

Adversarial Attack Simulation Exercise[11] (AASE) or sometimes referred to as Red Team Exercise provides a realistic picture of the FI's capability to prevent, detect and respond to real adversaries by simulating the Techniques, Tactics and Procedures (TTP) of threat actors to target the people, processes and products, technology underpinning the Critical Functions in a FI.

2. Bug Bounty Program

Organisations may also employ the use of financial incentives (also known as "bug bounties") to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organisation's needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organisations may run public and private bounties simultaneously.

3. Attack Surface Management

Attack surface management (ASM) is the continuous discovery, analysis, remediation and monitoring of the cybersecurity vulnerabilities and potential attack vectors that make up an organisation's attack surface.

4. Breach and Attack Simulation

Breach and attack simulation (BAS) is a tool/service to mimic the tactics, techniques and procedures (TTPs) used by threat actors to identify gaps in the organisation's defenses and assess the effectiveness of their security controls.

5. Threat Modelling

Threat Modelling is the process where the outputs of the Threat Intelligence process are used to generate likely attack scenarios that can accurately simulate real-world cyber security threats under operational conditions. The threat model report defines profiles of the likely threat actors expected to target the critical functions and the underpinning systems of the FI. It also provides detailed scenarios, and methods that the threat actors are likely to employ when targeting these systems. Some FIs leverage threat modelling before conducting a penetration test while others may conduct risk assessment or adopt alternative methodologies during the "discovery" phase of a penetration test.

6. DevSecOps

DevSecOps (Development, Security, and Operations) integrates security initiatives at every stage of the software development lifecycle to deliver secure applications. DevSecOps infuses security into the continuous integration and continuous delivery (CI/CD) pipeline, to address security challenges at DevOps speed. Static Application Security Testing (SAST) , Dynamic Application Security Testing (DAST), Software Composition Analysis (SCA), Interactive Application Security Testing (IAST) tools are typically used.

ENDNOTES

[1] OWASP Top Ten. Source: https://owasp.org/Top10/

[2] Top 25 Most Dangerous Software Errors. Source: http://www.sans.org/top25-software-errors/

[3] MITRE – Making Security Measurable. Source: http://measurablesecurity.mitre.org/

- Common Vulnerabilities Exposure (CVE)
- Common Attack Patterns Enumeration and Classification (CAPEC)
- Common Weakness Enumeration (CWE)
- Common Weakness Scoring System (CWSS)
- Including the CWE-Top25 (http://cwe.mitre.org/top25/)
- Common Vulnerability Scoring System (CVSS)
- Open Vulnerability and Assessment Language (OVAL) Security
- Security Content Automation Protocol (SCAP)
- Common Platform Enumeration (CPE)
- Common Configuration Enumeration (CCE)

[4] CVSS. Source: https://www.first.org/cvss/

[5] CWE Common Weakness Enumeration (CWE)

- http://cwe.mitre.org/top25
- https://cwe.mitre.org/cwss/cwss_v1.0.1.html
- http://cwe.mitre.org/top25/

[6] Industry guidelines on penetration testing include:

- Technical Guide to Information Security Testing and Assessment. NIST. Source: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- Assessing Security and Privacy Controls in Information Systems and Organizations. NIST. Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf
- Security and Privacy Controls for Information Systems and Organizations. NIST. Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- PTES (Penetration Testing Execution Standard) Technical Guidelines. Source: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- PCI Security Standards Council - Penetration Test Guidance. Source: https://docs-prv.pcisecuritystandards.org/Guidance Document/Penetration Testing/Penetration-Testing-Guidance-v1_1.pdf
- Open Web Application Security Project (OWASP) Penetration Testing Methodologies. Source: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
- The Institute for Security and Open Methodologies (ISECOM). Source: https://www.isecom.org/OSSTMM.3.pdf

[7] MAS Technology Risk Management Guidelines. Source: https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines. Critical Information Infrastructures may also refer to the Cyber Security Agency of Singapore (CSA) Code of Practice for Critical Information Infrastructure. Source: https://www.csa.gov.sg/docs/default-source/legislation/ccop---second-edition_revision-one.pdf?sfvrsn=421a71ab_1

[8] Under the CSA’s Cybersecurity Labelling Scheme Assessment, products that are certified as “level 4” means that the product has undergone structured penetration tests by approved third-party test labs： https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme

[9] CVSS severity scale. Source: https://nvd.nist.gov/vuln-metrics/cvss#:~:text=The%20Common%20Vulnerability%20Scoring%20System%20%28CVSS%29%20is%20a,of%20three%20metric%20groups%3A%20Base%2C%20Temporal%2C%20and%20Environmental

[10] In Singapore, the CSA's Cybersecurity Services Regulation Office (CSRO) administers the licensing framework for the cybersecurity service provider under the Cybersecurity Act. The CSRO website provides a list of licensed PT service provider: https://www.csro.gov.sg/resources/licensed-service-providers/

[11] Red Team: Adversarial Attack Simulation Exercises Guidelines. The Association of Banks Singapore. Source: https://abs.org.sg/industry-guidelines/cyber-security