香港賽馬會
The Hong Kong Jockey Club

Security Test Standard

Version 1.1

September 2021

Document Type:	-
Topic:	Security Test Standard
Policy Reference:	-
Version:	1.1
Classification:	Internal
Supersedes:	HKJC Security Test Standard, version 1.0, dated March 2021
Owner:	Head, Information Security
Approved By:	Executive Director, Information Technology & Sustainability
Maintained By:	Information Security Department
Review Date:	September 2021
References:	-

Table of Contents

1 Introduction

1.1 Objectives

This standard is to define the objectives, types, frequencies and the minimum requirements of security testing on applications and systems within the Hong Kong Jockey Club (HKJC).

1.2 Scope

This Standard applies to all business applications and infrastructures used or hosted by HKJC and all HKJC employees, contractors, third parties, and agents using those applications and infrastructures.

1.3 Key Terminology

Term	Description
DAST	Dynamic Application Security Testing
IAST	Interactive Application Security Testing
SAST	Static Application Security Testing
SME	Subject Matter Expertise
CI/CD	Continuous Integration and Continuous Delivery

1.4 Roles and Responsibilities

Roles	Responsibilities
HKJC Application Owners	• Document security requirements of their applications for security tests. • Review the automatic vulnerability scan result to ensure vulnerabilities are remediated.
Information Security Team	• Review and/or recommend any specific testing method to be adopted by HKJC. • Perform application security review on new projects or systems with significant changes.
Assessors from HKJC internal or third party	• Have access and use appropriate industry standard testing tools, valid license for testing tools. • Conduct security tests.
Developers	• Align with industry best security practices to develop an application.

	• Perform automated vulnerability scanning and static code analysis to identify vulnerabilities during application development. • Take HKJC IT security policies and standards requirements into consideration during design phase and implement security coding practices during application development lifecycle.

2 Security Test Objectives

The objectives of performing security tests are to ensure:

- All specific security controls are functioning as designed;
- Critical, high and medium issues identified must be remediated for all new and existing applications or systems (including production environment and testing environment);
- Testing scope is defined;
- Testing scope is approved;
- Documenting activities are performed during the testing lifecycle;
- Validation checks to detect any corruption of information through processing errors or deliberate acts;
- Documenting findings, taking action for remediation and retesting to confirm the closure of findings.

All security testing engagements must be formally reviewed and approved by Information Security and the System owner before testing commences.

Security Testing should not only be done before going production. HKJC should also consider annual testing, regular requirement for existing systems and business as usual environment to decide the time to carry out the testing.

IT Operations and Security Operations (e.g. SOC) and relevant stakeholders must be notified for the testing period.

3 Assessor Selection (Internal and Third Party)

An individual or group, whether internal to HKJC or a third party, may conduct network and application penetration testing if the tester meets all the following criteria:

- **Independence:** The tester must be independent of the development organization, the business application or network owner and the operations support team.

- **Subject matter expertise:** The tester must have industry recognized network and application penetration testing certifications or experience conducting end-to-end network and application penetration testing at HKJC or at a company of a comparable size.

- **Tools:** The tester must have access to appropriate industry standard testing tools, valid license for testing tools, and be skilled (i.e. certifications, past experience) in the use of such tools. If external SME is needed, the external tester should prepare the list of tools to be used during the test for IS team to review and approve before the engagement starts.

4 Requirements prior to Security Testing

All security testing engagements must be formally reviewed and approved by Information Security and the Application Owner before testing commences.

For new project/product, Application Owners must document the following security requirements before the security test:

- Threat Assessment
- Network Architecture
- Access Control
- Protection of Data
- System Configuration
- Source Code Repository (or outsourced / source code escrow)

For existing applications/systems (in production environment), Application Owners must document the followings:

- Resourcing requirements
- Testing windows
- Test type
- Agreed entry points
- Recovery Plans
- Reporting and Remediation Plan

5 Testing Criteria

Determining the requirements and frequencies for security control assessments are critical functions for HKJC. System owners should review the minimum testing frequencies established and determine if the minimum frequencies are adequate for a given information system. HKJC must follow the criteria below when determining the testing requirements and frequencies for the systems and applications:

5.1 System Classification Levels

HKJC must define the testing frequencies based on their system categorizations and impact (classification) level for each application and system. Security controls implemented on systems that are categorized as the highest-rated classification should be tested and scanned on a regular periodic-basis (e.g. annual testing) and more frequently than the lower-rated systems.

The table below lists the System Criticality Definitions:

Criticality	Definition	Criteria	Example
Lifeblood	Business units would fall quickly without this system.	Impacting betting or critical business. • Immediately affecting revenue generation	• Online Transaction Processor – Cashbet • Interactive Phone Betting System • Cashbet Network System • Soccer Betting Control System • Common Architecture Platform • Racing Information System
Critical	Absolutely necessary to the functioning of	Impacting betting or critical business. • Not immediately affecting revenue generation	• OCB Information Display System • Electronic Fund Transfer Gateway • WEBI Common Administration Systems

	all business units or corporate units.	Impacting critical corporate IT infrastructure services.	• Corporate Email Services • Internet Service System
Important	Important requiring IT high availability.	Impacting non-betting business. • Affecting visibility to public	• Customer Management System • Catering Point-of-Sales • Stables system
		Impacting corporate IT infrastructure (including security & system management) services requiring IT high availability.	• Corporate EMC • IP-based Private Automatic Branch Exchange
Moderate	Somewhat important but without IT high availability.	Impacting non-betting business. • Not affecting visibility to public • Affecting production operations	• Car Park Automation System • IT Library System
		Impacting corporate IT Infrastructure (including security & system management) services not requiring IT high availability.	• Access Control System • Corporate Antivirus System • Corporate Short Message Services
Peripheral	Supporting systems.	Impacting non-betting business. • Not affecting visibility to public • Not affecting production operations	• End User Services e-Form • Project & Profolio Management • Office Communication Services

For Penetration Testing and Vulnerability Scanning see the following table:

Criticality	Penetration Testing	Vulnerability Scanning
Lifeblood	Annually	Monthly
Critical	Annually	Monthly
Important	Every 2 years	Monthly
Moderate	Every 3 years	Quarterly
Peripheral	Prior to major change	Quarterly

- Systems that are **externally-facing** (e.g. Internet-facing) will require the most frequent testing and scanning as they may lead to the highest-rated risk. For these systems, vulnerability scanning should be conducted **MONTHLY** and penetration tests conducted **ANNUALLY** and prior to any major changes or updates are made.

5.2 Security Controls or Specific Assessment Tools Providing Critical Functions

For systems and tools that provide critical security functions (e.g. firewalls, domain controllers, Log management systems, SIEM system), HKJC must conduct the **vulnerability scanning half-yearly** and **penetration tests annually** to ensure the critical functions are provided in a secure environment.

5.3 New Applications or Applications with Major Change(s) Deployment

Vulnerability scanning and penetration tests should be performed for new applications or **IMPORTANT, CRITICAL**, or **LIFEBLOOD** applications with major change(s) before the production deployment.

Major Change(s) is defined by Information Security as any one of the following, but not limited to:

- An architectural change such as a move to a new data center or cloud provider, or deployment of a new database
- Deployment shift from internal-facing to external-facing
- Significant change to the functional requirements, or application configuration including security control features
- Business, System and Platform Owners must define significant functional or application configuration changes for their systems or applications
- Any major release on the application libraries

- New network services, web services, API, and new functionality added to the application
- New user interface (UI) or significant change to the UI, to include all updates except cosmetic changes
- Update of an authentication or authorization mechanism
- Increase in the classification of data processed by an application

Minor Change(s) is defined by Information Security as implementation of low-risk, well-understood changes which do not have a major impact and do not require the involvement of release management. All other changes are defined as Major Change(s).

6 Testing Environment Selection

Testing should be conducted in the production platform when possible. If a non-production platform is selected, it should be a representative of the production environment.

- When testing a production application, the following criteria must be met:
    - Proper project and risk management coordination with the Application Owner, to limit the potential negative interactions with the production platform during the penetration test
    - Availability of complete system backup and a documented and available restoration plan prior to the start of testing
    - Application and data support teams must be notified of the application testing timeframes to create awareness and establish availability requirements in the event restoring the application or data is necessary.
    - Testing scope includes end-to-end data flow (e.g. web server -> application server -> database server)
    - Expected application operation is verified after test completion.
    - Any findings discovered in the non-production environment are remediated in both the non-production and production environments within timelines defined based on criticality
- When testing a non-production platform, the following criteria must be met:
    - The non-production environment is a representative of the production environment (e.g. software versions, configurations, traffic flows and security controls)
    - Any findings discovered in the non-production environment are remediated in both the non-production and production environments within timelines defined based on criticality

7 Security Testing Types

The following are the security testing types for HKJC's systems and applications:

Testing Type	Description	Target System Types
Compliance Scans / Checks	A compliance check scans the target and returns results if the target is compliant based on the standards selected for the scan. This allows an administrator to see how their systems are configured and if they are compliant with HKJC's standards.	Network, System or Application
Vulnerability Scans	Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.	Network, System or Application
Network Penetration Testing	A network penetration test is the process of identifying security vulnerabilities in applications and systems by intentionally using various malicious techniques to evaluate the network's security, or lack of responses.	Network, System or Application
Application Penetration Testing	Differently from network penetration test, the application penetration test is mostly focused on the Application Layer of TCP/IP model.	Application
Objective-based Testing	Objective-based Testing is a multi-layered cybersecurity assessment technique agreed upon objectives that include networks, technical and physical assets, storage devices etc. (e.g. Red team exercise acts as an adversary, attempting to identify and exploit potential weaknesses using sophisticated attack techniques.)	Network, System or Application
CI/CD Security Testing	Automated testing including SAST and DAST should be integrated in the CI/CD process.	Application under CI/CD process
Cloud Security Testing	Cloud-based application security testing is a relatively new type of testing in which the applications are tested by a solution / tool	Cloud-based application

	/ scanner hosted in cloud. It differs from traditional application security testing in a few ways.	
Physical Security Testing	Physical Security Testing is a regular testing to ensure the effectiveness of the physical security controls that are in place. (e.g. checking the "Clean Desk Policy" Effectiveness with assigned staff to check every staff's desk at a designated timely basis.)	Physical assets

7.1 Vulnerability Scans

- Vulnerability testing should be an authenticated testing wherever possible to ensure test completeness and minimize false negatives.
- Vulnerability testing tools must be approved before use.
- Vulnerability signatures or databases must be updated to the latest version before scans.
- Security Operations (e.g. SOC) must be notified whenever there are any significant changes in the wired or wireless network to ensure vulnerability testing is comprehensive.
- The system owners must be notified if the scans may lead to potential harms to the system. Note: Brute-force password cracking shall be avoided.

If it is required to perform an on-demand manual scanning, a request must be submitted to the Information Security.

7.2 Network Penetration Testing

Network penetration testing must focus on finding security weaknesses, exploitable vulnerabilities at specific levels of an environment, and include testing at the network, system, service and application levels.
Network penetration testing must include the following components:

1. **External testing**
   - Posture checking of any external system to identify vulnerabilities that may exist in exposed systems, services or applications
   - Network discovery, network mapping, host identification and service enumeration
   - Identification and validation of misconfigured systems, services and applications
   - Physical location network penetration testing

2. **Internal testing**
   - Posture checking to identify specific exploitable vulnerabilities like escalating privileges, installing custom-crafted malware and exfiltration of sensitive data
   - Network discovery, network mapping, host identification and service enumeration
   - Identification and validation of misconfigured systems, services and applications

3. **Wireless testing**
   - Review of the wireless environment to determine if someone in physical proximity to a campus or wireless equipment could breach the internal network or move from the 'Guest' wireless network to the internal network
   - Identification of rogue access points
   - Identification of unauthorized Access Points
   - Identification of site survey for excessive wireless signals

Internal network penetration testing must be conducted from inside HKJC's networks and from DMZs.

External network penetration testing must be conducted from outside HKJC's networks to identify the vulnerabilities and weaknesses of external facing systems.

Network penetration testing must be conducted according to the standard penetration lifecycle which includes Planning, Discovery, Exploitation, Vulnerability Identification, Result Analysis and Reporting, Remediation, Validation, Re-test for Confirmation, Documentation.

- During **Planning,** the test plan, test use cases, network segments, location, and scanning tool must be defined.

- **Discovery** must assess:

  - Open ports and access points

- Unsupported operating systems, services and applications
- Unsupported protocols and weak cryptography
- Exploitable systems and applications
- Authentication issues such as authentication bypass, enabled default accounts, weak passwords and plain text passwords
- Vulnerabilities specific to operating system, software or network devices
- Unintended internet access, both inbound and outbound

- **Exploitation** must assess:
  - Remote connectivity
  - Accessing the target system
  - Capturing user credentials
  - Obtaining privileged access
- **Vulnerability Identification** must include:
  - Assessment of the vulnerability
  - Validation of the exploitation steps
  - Categorization of the vulnerability based on the industry standard risk matrix
- **Result Analysis and Reporting** must include:
  - Scope of work and timeline
  - Summary of the findings
  - Evidence of the findings, to the extent it can be produced
  - Source, root cause and impact of each vulnerability
  - Detailed recommendation of remediation steps
- **Remediation** must be prioritized based on the severity of finding(s).
- **Re-test** must be performed to confirm the vulnerability has been remediated successfully

- **Documentation** must include evidencing the steps performed in each phase of the testing lifecycle. Specific documentation must include evidence of:
    - All vulnerabilities discovered
    - Specific tasks performed to reproduce the issue
    - Remediation applied
    - Specific tasks performed during retesting

7.3 Application Penetration Testing

Application penetration must be performed to business applications built, purchased, or contracted by HKJC whether deployed internally, externally, or hosted by third parties for:

- External-facing applications such as web, web service (i.e. application programming interface (API)), and mobile applications
- External-facing or internal-facing applications containing confidential information
- External-facing or internal-facing applications undergoing major architectural or security configuration changes
- The scope of the application testing must be appropriately documented. The following must be defined:
    - The application in scope for the test
    - The network location or address of the application, including domain name and associated protocols and network ports
    - Out-of-scope services or protocols
    - The tester's system network address, to identify testing traffic apart from "real" attack traffic
    - The testing approach, such as the nature of the test, (i.e., automated scanning, manual testing, and testing depth (i.e., sophistication or invasiveness))
    - Level of access to internal, confidential and highly confidential data
    - Controls to protect internal, confidential and highly confidential data during testing
    - Processes for delivery, handling, return, and destruction of authentication credentials
    - Tokens, certificates, passwords and keys obtained by the tester must be defined prior to providing access to data
    - Contact information for each stakeholder, to allow for expedited notification in case system problems or security events occur during testing
    - Tester's scanning machine internet protocols (IPs), to allow those IP addresses to be whitelisted
    - Reassessment parameters for any issues identified during testing

- If testing involves the production environment, a documented, tested and available recovery plan
- Testing start and end dates and approved test windows
- For mobile applications, both the client-side binaries and the server-side API.

Black Box Testing

In Black box testing, penetration testers are not provided with any internal knowledge of the target systems. Black box techniques should be used primarily to assess the security of individual high-risk compiled components; interactions between components; and interactions between the entire application or application system with its users, other systems, and the external environment. Black box techniques should also be used to determine how effectively an application or application system can handle threats.

Gray Box Testing

The penetration tester has the access and knowledge levels of a user, potentially with elevated privileges on a system. Gray box pentesters typically have some knowledge of a network's internals, potentially including design and architecture documentation and an account internal to the network. An internal account on the system also allows testing of security inside the hardened perimeter and simulates an attacker with longer-term access to the network.

White Box Testing

White box testing provides full access to source code, architecture documentation and all other information to the penetration testers. The close relationship between white-box pentesters and developers provides a high level of system knowledge

7.4 Objective-based Testing

Objective-based Testing targets the HKJC's key functions and systems. The testing components must include:

- **Preparation & Scoping**
  - The Club's key functions and systems will be confirmed to determine threat categories.
  - A Control Group responsible for planning and execution of testing is formed.
  - The objective of the testing will be defined and assessment related will be chosen.
- **Threat Intelligence**
  - Information is gathered on the Club to establish credible threat actors who would target you and identify their most likely targets

- **Development of Test Scenarios and Staging**
    - Threat scenarios, attack plans and defensive measures based on intelligence will be developed covering: test goals, initiation, chain of tasks, milestones and timeline
    - Staging of attack platforms is performed to emulate agreed threat actors.
- **Test Execution**
    - Tactics, techniques and procedures of agreed threat actors is used to gain access to the systems and escalation of privilege.
    - Targeted systems are compromised to demonstrate impact.
- **Reporting & Closure**
    - Key observations and improvement areas will be discussed with the Club relevant stakeholders in a post-test debrief workshop
    - A Simulation Testing Report will be published summarizing key findings and recommendations

7.5 CI/CD Security Testing

For DevOps with Security, HKJC should implement a secured delivery pipeline to ensure better security control, less risk and better compliance. The pipeline should have the Code, Build, Deployment and Test Execution, and Release processes. The testing in each process should be automated, streamlined, repeatable and routinized as much as possible which can help to:

- Reduce delivery time
- Improve quality and security
- Eliminate human error

7.6 Code

The codes including infrastructure, application and test must be stored in a version control system. Access and every change to the code base should be audited. During code design and peer-review special attention should be given to detect handing of unencrypted/untokenized sensitive data within the code. Application interfaces should be tested to ensure secured access to the interfaces. HKJC should also scan the codes before implementing changes. Please refer to the section Static Analysis Security Testing (SAST) for details.

7.7 Build

During build process, infrastructure code and application code can be scanned and analyzed thoroughly. Application code should be scanned for security vulnerabilities and other

software defects. Third-party libraries (including open source libraries) should be scanned for security and legal/licensing vulnerabilities. It is required to keep third-party libraries up to date. Please refer to the section Static Analysis Security Testing (SAST) for details.

7.8 Deployment and Test Execution

Deployment process should be automated and/or scripted for reproducibility. It should keep track of software versions and their flow across the environments. Each deployment should be followed by automated test execution. Security testing should be a part of test automation. Test results should be stored to ensure traceability and help troubleshoot. Please refer to the section Dynamic Analysis Security Testing (DAST) for details.

7.9 Static Analysis Security Testing (SAST)

Static Analysis Security Testing (SAST) analyzes application source, byte and binary codes. If the source, byte or binary codes are not available for scanning, proof of a security code review must be maintained.

- Critical, high and medium severity issues discovered during the code review must be remediated before moving the application to production.
- If the application is being developed by a third party, evidence must be maintained to demonstrate that the SAST was completed and vulnerabilities corrected.
- Systems or projects which adopted SAST will auto trigger code scan in each build. SAST must be conducted in both minor release or major release.
- Security vulnerabilities must be documented, assessed and remediated for open source applications. Developers must confirm that there exists no violation of licenses or source code non-compliance during the code review.
- If an automated SAST is not possible due to technology limitations of the SAST tool, a manual code review process must be completed and documented.
- At a minimum, the secure code review process must comply with the latest version of OWASP Top 10 standard.

7.10 Dynamic Analysis Security Testing (DAST)

The Dynamic Analysis Security Testing (DAST) must include the following components:

- Authentication Testing
- Authorization Testing
- Identity Management Testing
- Session Management Testing
- Input Validation Testing

- Cryptography Testing
- Error Handling Testing
- Information Leakage Testing
- Configuring Testing
- Business Logic Abuse Testing
- Testing to identify other vulnerabilities listed in OWASP Top Ten Application Security Risks, OWASP Top Ten Web Application Security Risks, OWASP Top Ten Mobile App Security Risks

7.11 Cloud Security Testing

HKJC should request the Software as a Service cloud service providers to provide their security assurance results such as SOC reports for review. Security testing should also be conducted based on the criteria defined in the section Testing Criteria. The cloud service providers should be informed of the risks involved when performing the testing, and they should be included in the governance model in order to clear mark their responsibilities.

8 Vulnerability Information Handling

Vulnerability information contains sensitive information of HKJC applications, systems and networks. The raw data must be deleted as soon as the closure of a testing exercise. Documents that contain vulnerability results must be classified and protected.

Document Changelog

Date Modified	Version Number	Description of Modification	Modified By
March 2021	1.0	First Release	James Wiles
September 2021	1.1	Align and optimize overall document structure	Technology and Cyber Risk & Compliance