CITY UNIVERSITY OF HONG KONG
Information Security
Internal Assessment Standard

(Approved by the Information Strategy and Governance Committee in January 2023)

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2023-01-28

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2023-01-28	Revised the link in this document.

Distribution

Copy	Issued to	Location
Master	Public	https://www.cityu.edu.hk/cio/information-security/information-security-policies-and-standards

Contents

1 Policy Statement

The City University of Hong Kong or hereinafter referred as the "University" shall carry out continuous information security internal assessment regularly to detect and remedy any findings of its information security controls.

This Information Security Internal Assessment is totally independent with Internal Audits conducted by the Internal Audit Office of the University. The roles and responsibilities of Internal Audit Office are defined by the Audit Charter of the University.

2 Objective

The purpose of this document is to establish an information security internal assessment standard in which authority, responsibilities, assessment process, and documentation standards are set out and provided as guidance during the assessment process.

3 Information Security Internal Assessment

To ensure that security measures comply with the University's security policies, standards and requirements, continuous information security internal assessment shall be established.

Internal assessment is an effort initiated internally from the University, though the assessment may be conducted by third party service providers.

External assessments or external audits are initiated, required and conducted by independent third parties, such as Hong Kong SAR Government, University Grants Committee, regulatory bodies, and accredited certification bodies.

The main objectives of an information security assessment are to:

- Check for conformance to existing security policies, standards, guidelines and procedures
- Identify the inadequacies and examine the effectiveness of the existing policies, standards, guidelines and procedures
- Identify and understand the existing vulnerabilities
- Review existing security controls on operational, administrative and managerial issues, and ensure compliance to minimum security standards
- Provide recommendations and corrective actions for improvement

4 Authority

As part of the Information Security Governance of the University, Central IT is authorized by the University to:

- conduct information security assessment of all information systems in the University or require the owners of information systems to conduct information security assessment and submit the reports to the Central IT
- test the compliance of security management measures by recovery drill

- carry out supportive and random checks by surprise checks
- contain and isolate any information system in the University if necessary

5 Scope of Assessment

For each assessment, Central IT shall define the scope, examples of scope are:

- Information security policies, standards, and guidelines review
- Web application security assessment
    - Common web applications vulnerabilities
    - Logical access control to data and functions
- Platform security assessment
    - Network infrastructure security assessment
    - Host security assessment

6 Responsibilities

6.1 Senior Management of Central IT

- Authorize and approve information security internal assessment conducted by Central IT
- Require departmental Information System Owners to arrange security assessment which could be conducted by qualified staff of owner departments or external service providers
- Oversee the performance of information security internal assessment
- Review of assessment findings and provide guidance on the corrective actions
- Sign off or accept the assessment report

6.2 Central IT

- Maintain a register of information systems in the University, owned by Central IT and/or other University Units

6.3 Information Security Unit of OCIO

- Coordinate information security internal assessment efforts with Central IT and Information system owners
- Support the Information System Owners to coordinate and liaise with external information security assessment service providers to carry out security assessments
- Provide advice for determining corrective actions in relation to assessment findings
- Monitor the implementation of corrective actions

6.4 Information Security Assessor

Information Security Assessor can be qualified member from the University or qualified personnel from third party services providers. An Information Security Assessor shall:

- Possess the necessary skills, expertise and qualifications
- Prepare and conduct information system internal audits
- Conclude audit findings and report to the owner of information system

- Exercise good judgment in reporting immediately for any significant security risk findings to Information System Owner
- Discuss and agree corrective actions and the timeline in relation to the audit findings with Information System Owner
- Follow up with Information System Owner regarding the status of corrective and/or preventive actions

6.5 Information System Owners

- Inform Central IT of their Information Systems
- Conduct background checks and qualification checks on Information Security Assessors, to see if they possess necessary experience, expertise and qualifications
- Allow physical and logical access only to the systems, networks or computer equipment, which are necessary to perform the evaluations, and protect all assets that may be affected
- Be cooperative and open-minded. Acknowledge the results and develop plans for improvement if there are security needs
- Provide response to Information Security Assessors' enquiries within a reasonable time span
- Provide sufficient office space and office equipment for the Information Security Assessors to perform their service; a restricted area is preferred
- Provide all necessary documentation about the specific area under assessment
- Hold regular meeting with Information Security Assessors for project control and review
- Apply changes or enhancements at the earliest opportunity, especially those that are at high risks
- Submit Information Security Internal Assessment report, and action plans to Central IT and Head of Department of the assessed information system

7 Information Security Internal Assessment Process

7.1 Initiation

The Central IT Senior Management is responsible for initiating and defining the scope of the Information Security Internal Assessment. If the internal assessment will be conducted by Central IT, the Information Security Unit of the OCIO will be leading the assessment. If the Information System Owner is required to submit an assessment report to Central IT, the Information Security Unit will advise the owner about the necessary skills, expertise and qualifications.

7.2 Planning

The Information Security Assessor needs to prepare adequately for each Information Security Internal Assessment, to obtain a thorough understanding of the scope and objectives of the assessment, and the information system being assessed.

If the Information Security Assessor is in any doubt, or requires clarification, they should refer back to the Senior Management of Central IT timely before conducting of an assessment.

7.3 Execution

7.3.1 Assessment Schedule

The schedule of Information Security Internal Assessment shall be agreed between the Information Security Assessor and the management of assessed units. The assessment schedule shall be distributed to the units so that adequate resources can be allocated.

The Information Security Assessor shall inform the Senior Management of Central IT and the owner of information system about any delay encountered during the planning of an assessment and make corresponding adjustment to the assessment schedule.

7.3.2 Supervision

The fieldwork staff of the Information Security Internal Assessment shall be properly supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional standards are met.

7.3.3 Assessment Documentation

The assessment work performed during each internal assessment engagement shall be documented following pre-defined documentation requirements. At minimum, assessment documentation should include:

- Assessment Scope and Objectives
- Assessment Program
- Assumptions & Limitations
- Methodology & assessment tools used
- Descriptions of current environment
- Summary of findings
- Details of findings or vulnerabilities with rankings and recommendations

7.3.4 Concluding the Assessment

Prior to concluding the assessment, the Information Security Assessor should review the findings, and agree on the conclusion with personnel responsible for the functions or processes which have been reviewed.

At the closing meeting of the assessment, the Information Security Assessor shall present and agree the assessment findings and conclusions with the assessed parties, in a way that they are understood and acknowledged. Participants in the closing meeting should include the owner and management of the assessed information system and where appropriate, those responsible for the functions or processes which have been reviewed.

The Information Security Assessor and the management shall discuss and agree corrective actions for any findings identified. The assessment findings and corresponding corrective actions agreed must be properly documented by the Information Security Assessor.

7.3.5 Reporting

The Information Security Assessor is responsible for compiling an assessment report, in an appropriate form, upon the completion of the assessment. The report should identify the reviewed information system, the owners of the system, the intended recipients and any restrictions on circulation.

The assessment report should state the following:

- Scope, objectives, period of coverage and the nature, timing and extent of the assessment work performed
- Assessment findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the assessor has with respect to the assessment

The Information Security Assessor shall have sufficient and appropriate evidence to support the results reported. When issued, the assessment report should be signed and dated by the Information Security Assessor.

The assessment report shall be distributed to the following parties or according to the terms of the engagement letter.

- Senior management of Central IT
- Information Security Unit of the OCIO
- Owners of the assessed information system
- Head of Department of the assessed information system

Information System Owner is required to make a formal written response to the assessment report.

7.4 Follow-up Activities

After the reporting of findings and recommendations, the Information System Owners shall be responsible for coordinating the effort from relevant parties in implementing the corrective actions applicable to the audit findings.

The Information Security Unit shall monitor the overall progress of the corrective actions to ensure control deficiencies or performance improvement observations are timely mitigated or addressed.

The Information Security Unit should request and evaluate relevant information to conclude whether appropriate action has been taken to mitigate the control deficiencies or address the performance improvement observations. The follow up activities shall be documented by the responsible assessor on the assessment report assigned by the senior management of Central IT or owner of information system.