**General Control Checklist**

**Security Risk Assessment & Audit Services**

Version: 1.2

July 2022

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of and may not be reproduced in whole or in part without the expressed permission of HKSAR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Amendment History | | | | |
| Change Number | Revision Description | Pages Affected | Version Number | Date |
| 1 | First Draft | N/A | 1.1 | 29 Jul 2022 |
| 2 | Revise name of bureau | N/A | 1.2 | 1 Aug 2022 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc23491091)

[2. Service requirement 5](#_Toc23491092)

[2.1. Tasks 5](#_Toc23491093)

[3. Items to be checked 6](#_Toc23491094)

# Introduction

This document details a checklist to check against the clauses of the Work Assignment Brief.

# Service requirement

Below are used for checklist of the required services.

## Tasks

|  |  |
| --- | --- |
| Items | Status |
| Perform general control review |  |
| Conduct compliance checking against S17 and Departmental Security Policy or policies that are relevant |  |
| Identify and recommend safeguards in Follow Up Action Plan |  |
| Document the findings and results in Security Audit Report |  |

Note:

A set of documentation is requested in advance for IT&C consultants’ general control review after the Project Initiation Meeting adjourns. The documentation is suggested to get prepared before subsequent on-site activities.

Findings, responses, queries, and comments (where applicable) for each security requirement would be documented in the subsequent report accordingly.

# Items to be checked

This section highlights the relevant items which are referenced to the **Practice Guide for Security Risk Assessment & Audit** of OGCIO. The items are categorised into fourteen security domain areas for ease of reference and to be checked in a security audit in compliance and best practice perspective. This checklist is not intended to cover all aspects, but rather acts as a preliminary reference. The EEB(EB)/EPD or its service contractor is recommended to go through the items list with the IT&C consultants.

An interview or group discussion will be performed on or before the on-site audit activities. Separate further interviews or discussions might be conducted with responsible person depending on the responses and past records might be requested and verified at later stage.

| **Security Domain** | **Items to be Checked** | **Remarks/ Reasons for Non-conformance** |
| --- | --- | --- |
| ***Management Responsibilities*** | * Departmental IT security organisational framework and the associated roles and responsibilities are defined. |  |
| * Sufficient segregation of duties to avoid execution of all security functions of an information system by a single individual is applied. |  |
| * Departmental budget covers the provision for necessary security safeguards and resources. |  |
|  | | |
| ***IT Security Policies*** | * Security policy is well documented and easy to understand. |  |
| * Security policy is easily accessible by all involved parties. |  |
| * Security policy is periodically reviewed and updated to reflect current environment. |  |
| * Users are informed and committed to the security policy. |  |
| * All rules stated in the security policy are implemented. |  |
| * Security policy is approved, promulgated and enforced by the Head of B/D and the management. |  |
|  | | |
| ***Human Resource Security*** | * All staff are advised with acknowledgement of their IT security responsibilities upon being assigned a new post, and periodically throughout their term of employment. |  |
| * All roles & responsibilities are clearly defined. |  |
| * Adequate training on security is given to relevant parties. |  |
| * Access to classified information higher than RESTRICTED is restricted to officers who have undergone appropriate integrity checking as stipulated by the Secretary for the Civil Service. |  |
| * Information security responsibilities and duties that remain valid after termination or change of employment has been defined and communicated to the staff. |  |
|  | | |
| ***Asset Management*** | * An inventory of information systems, hardware assets, software assets, valid warranties and service agreements are properly owned, kept and maintained. |  |
| * Computer resources and information are returned to the Government when a staff is transferred or ceases to provide services to the Government. |  |
| * Information is properly classified and its storage media is labelled and handled according to government security requirements. |  |
| * Proper security measures are in place to protect storage media with classified information against unauthorised access, misuse or physical damage. |  |
| * All classified information is completely cleared or destroyed from storage media before disposal or re-use. |  |
|  | | |
| ***Access Control*** | * Personal Data (Privacy) Ordinance (Cap. 486) is observed when handling personal data. |  |
| * User right assignment for various type of users on the system is documented and reviewed with appropriate segregation of duties. |  |
| * There is well-defined process to re-validate the user access right at the system and application level periodically. |  |
| * User privileges and data access rights are clearly defined and reviewed periodically. |  |
| * Records for access rights approval and review are maintained. |  |
| * Each user is given with unique user identity. |  |
| * All users are granted with minimum privileges that are sufficient for carrying out their duties. |  |
| * Users are informed about their privileges and access rights. |  |
| * For distribution of user accounts and passwords, there are proper and secure procedures commensurate with the classification of information to be accessed. |  |
| * Logs are properly kept for users’ activities such as log in/out time, connection period, connection point, functions performed etc. |  |
| * No unused accounts are found in the system/network. |  |
| * Administrators are also provided with user accounts. |  |
| * Administrator accounts are solely used for administration work. |  |
| * Users are classified into different categories with well-defined privileges for each category. |  |
| * There is a well-documented password policy for the system/network. |  |
| * Mission critical system follows the strong password policy. |  |
| * Last eight password selection(s) cannot be reused for renewal. |  |
| * There is expiry period (3 – 6 months) on the password. |  |
| * Maximum 5 trials are allowed for password attempts. |  |
| * No dictionary words, user names or obvious phases are found in the password contents. |  |
| * Users change the password regularly or immediately when their accounts are newly created. |  |
| * No users write their passwords in labels or obvious place. |  |
| * There are appropriate policies and procedures specifying the security requirement of using mobile computing and remote access. |  |
| * There are control measures for remote access to the computer, application systems and data. |  |
| * Two-factor authentication is adopted for high risk access. |  |
| * For remote access to the B/D's internal network via Virtual Private Network (VPN) connections or B/D’s internal email systems via the Internet, two-factor authentication is implemented. |  |
| * Strong encryption and/or two-factor authentication (for CONFIDENTAL data only) as well as inactive session timeout are in place over VPNs. |  |
|  | * A formal usage policy and procedures is in place, and appropriate security measures shall be adopted to protect against the risks to IoT devices. |  |
|  | | |
| ***Cryptography*** | * Cryptographic keys through their whole life cycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys are properly managed. |  |
|  | | |
| ***Physical and Environmental Security*** | * There are evidence or supporting documents indicating that the physical security requirements of the computer rooms/server rooms/computer areas meets the requirements specified in the departmental IT security policy, government security requirements and other related standards. Examples include previous SRAA reports or certification/notification issued by Architectural Service Department. |  |
| * All cables are tidy and properly labelled to assist maintenance and fault detection. |  |
| * All under floor spaces, if any, are properly cleaned up. |  |
| * The ceiling is regularly cleaned to avoid dust and dirt. |  |
| * Water detectors, if any, are fitted in the under floor space to detect flooding automatically. |  |
| * Cables in ceiling voids are properly installed. |  |
| * UPS are installed for necessary equipment. |  |
| * UPS are capable to provide sufficient power supply for an expected period of time. |  |
| * UPS are regularly tested. |  |
| * UPS are located in a safe place. |  |
| * Operators in computer room are properly educated for the power supply control and power failure scenarios. |  |
| * No inflammable equipment or materials are left in the computer room. |  |
| * All automatic fire detection systems are operated in proper conditions with regular testing and inspection. |  |
| * All automatic fire extinguishing system installed is regularly tested and is in good conditions. |  |
| * All water pipes passing through the room or under the floor, if any, are in good conditions. |  |
| * The room temperature and humidity is monitored and set in a way that fits for the computer equipment to be operated in good conditions. |  |
| * All keys of the doors in the computer room are properly issued, kept and recorded. |  |
| * There are well-defined procedures for handling and distributing keys of the locks. |  |
| * All personnel are trained and informed about the use of the fire extinguishers and other physical protection mechanism. |  |
| * Smoking, food and drinks are not allowed inside the computer room. |  |
| * Portable computers, mobile device and other computer equipment, which are brought into the computer room, are controlled. |  |
| * There are specially assigned staff responsible for arranging cleaning of the computer room. |  |
| * There is regular inspection of equipment and facilities. |  |
| * All visitors are authorised and identified before entering into the computer room. |  |
| * All visitors are accompanied with authorised staff at all times. |  |
| * All visitors are provided with visitor labels when entering into the room. |  |
| * All visits are recorded. |  |
| * There is proper access control to enter the computer room. |  |
| * All entrances to computer room are controlled by locked doors. |  |
| * Only authorised staff are allowed to enter the computer room with sign-in and sign-out processes. |  |
| * All manuals and documents are not freely put aside and bookshelves are provided with filing and access controls. |  |
| * Computer stationery held in a computer room is just sufficient for operation. No extra stock is held to avoid fire. |  |
| * All computer stationery are properly kept and controlled. |  |
| * There is procedure for issuing, authorising and recording computer stationery. |  |
| * A proper inventory is kept for all computer equipment. |  |
| * Sample physically checking on the computer equipment against the inventory record is correct. |  |
| * Mobile devices or removable media are secured when user have to leave his/her device/media unattended. |  |
| * IT equipment being taken away from sites is properly controlled. |  |
| * Automatic re-authentication feature is used and enabled on all computers. |  |
|  | * For IoT devices, security controls is enforced to protect the device against loss, theft and damage according to the classification of information being stored, processed and transmitted by the IoT devices. |  |
|  | | |
| ***Operations Security*** | * All software and files downloaded from the Internet are screened and verified with anti-malware solution. |  |
| * There are procedures established and documented for backup and recovery. |  |
| * Logs are kept for all backups and recovery taken including date/time, backup media used, taken by who etc. |  |
| * At least two-backup are kept with one is placed off-site. |  |
| * There are well-defined retention periods and disposal procedures for backup media. |  |
| * All backup media are properly labelled and locked in a safe place/area. |  |
| * The place or cabinet where backup media is kept is always in lock. |  |
| * There is proper transportation control for off-site storage. |  |
| * Access to media is properly controlled and recorded. |  |
| * An inventory is kept for all storage media. |  |
| * Daily logs e.g. system logs, error logs or user activity logs are properly kept, reviewed and analysed. |  |
| * Logs of Approved Email System and Internet access service centrally provided by OGCIO or B/Ds are recorded. |  |
| * Access to operating system utilities is restricted to authorised persons only. |  |
| * No unused/suspicious services are running under the operating system account. |  |
| * No unused user accounts are remained in the operating systems. |  |
| * System logs are properly generated and reviewed on daily or regular basis. |  |
| * The clocks of information systems are synchronised to a trusted time source. |  |
| * Controls on changes to information systems are in place. Change records are maintained. |  |
| * Patches are regularly applied to the operating systems to fix their known vulnerabilities. |  |
| * An inventory record of hardware equipment and software packages (including the patch management system itself) and version numbers of those packages mostly used within the B/Ds is created and maintained. |  |
| * Security risks of using end-of-support software are assessed and appropriate security measures to protect the information systems and related data are implemented by B/Ds. |  |
|  | | |
| ***Communications Security*** | * Network connected to Internet is protected by Firewall. |  |
| * Intrusion detection strategy is implemented to detect abnormal activities on the network by installing a network intrusion detection system (NIDS) or network intrusion prevention system (NIPS) at critical nodes of the network. |  |
| * Network segmentation/isolation is adopted and is a standard abided by all newly implemented systems or major enhancements and changes associated with the systems. |  |
| * All remote access into the internal network is properly controlled with authentication and logs. |  |
| * Administration to network components is done by authorised staff only. |  |
| * Controls are put on the use of network resources such as file sharing, printing etc. to allow only authorised and authenticated users to use. |  |
| * Upgrading on software located in the network is done by authorised persons only. |  |
| * Policy is set up to control the proper use of the network and its resources. |  |
| * Security protection, e.g. encryption, is used for information that is allowed to be transmitted and sent through the network. |  |
| * Dedicated person is assigned to monitor the network performance and the daily operation. |  |
| * All network user profiles are properly protected from unauthorised access. |  |
| * Network configuration is documented and put in a secured place. |  |
| * All network components are located in a secure area. |  |
| * Proper security measures have been defined and implemented to ensure the security level of the departmental information system being connected with another information system under the control of another B/D or external party is not downgraded. |  |
| * Agreement on the secure transfer of classified information between B/Ds and external parties are established and documented. |  |
|  | * Wi-Fi infrastructure is reviewed to assess the impact of the vulnerability found in Wi-Fi communication standards and protocols periodically. |  |
|  | * Resources records of Government's Internet domains is protected by prevailing security controls i.e. Domain Name System Security Extensions (DNSSEC). |  |
|  | * HyperText Transfer Protocol Secure (HTTPS) is implemented for all Internet services, including informational websites. |  |
|  | | |
| ***System Acquisition, Development and Maintenance*** | * There are well-documented change control procedures. |  |
| * Evaluation or estimation has been made on the effects of such change requests. |  |
| * All changes are properly approved, recorded and tested before implementation. |  |
| * Adequate backups (before and after) are performed before and after the change. |  |
| * Recovery procedures are defined before each change. |  |
| * There are controls to ensure that no testing data/programs are resided in the production environment. |  |
| * After applying to production environment, verification (e.g. manual review) has been made to assure that all changes were implemented as desired and planned. |  |
| * There are proper access rights granted to allow only dedicated staff or administrator to amend the system/network’s configuration. |  |
| * The backup and recovery procedures have been revised to reflect the change if necessary. |  |
| * Secure development environments for system development and integration efforts that cover the entire system development life cycle are established. |  |
|  | * Version control mechanism is established to record changes to program source code over time during application development. |  |
|  | | |
| ***Outsourcing Security*** | * Risks of utilising external services or facilities are identified and assessed. |  |
| * Copy of signed confidentiality and non-disclosure agreement is properly managed. |  |
| * All the government data in external services or facilities are cleared or destroyed according to the government security requirements at the expiry or termination of the service, or upon request of the government |  |
|  | | |
| ***Security Incident Management*** | * There is established incident monitoring and response mechanism, which has been tailored to specific operational needs, for each system. |  |
| * There is predefined retention period of logs for tracing security incident when necessary. |  |
| * Security incident response/handling procedure is periodically reviewed and drilled. |  |
| * Should there be any security incidents, they are handled and escalated properly by staff, based on the established reporting channels. |  |
| * The latest version of the incident monitoring/response procedure is made available to the end users. |  |
|  | | |
| ***IT Security Aspects of Business Continuity Management*** | * Disaster recovery and emergency response plans are reviewed, drilled and updated according to documented frequency. |  |
| * Plans for emergency response and disaster recovery of mission critical information systems are fully documented, regularly tested and tied in with the Business Continuity Plan. |  |
| * There is adequate resilience to meet the availability requirements of IT services and facilities. |  |
|  | | |
| ***Compliance*** | * Security policy should require that periodic security risk assessment and audit is performed. |  |
| * The recommendations from last security risk assessment and audit are followed up. |  |
| * All relevant statutory, regulatory and contractual requirements to the system operation are identified and documented. |  |
| * Records to evidence compliance with security requirements and support audits of effective implementation of corresponding security measures are kept. |  |
| * Selection of auditors and conduct of audits are objective and impartial. |  |
| * Use of software and program for security risk assessment or audit is restricted and controlled. |  |
|  | * Appropriate security measures are implemented throughout the whole data lifecycle for information system that involves personal data. |  |

*<< END >>*