|  |  |  |
| --- | --- | --- |
| **Client:** | **$(client)** | |
| **Period end date:** | **$(start) - $(end)** | |
| **Ref. no.:** |  | |
| **Prepared by:** | $(user) | **Date:** |
| **Approved by Manager:** |  | **Date:** |
| **Approved by Partner:** |  | **Date:** |

**Guidance (click to expand):**

The purpose of this template is to document understanding and evaluation of the computer information system (CIS). Where a more detailed review of the IT environment is required, the documentation template may be modified accordingly. This document assists in evaluating whether general level controls are satisfactory.

There may be management IT specialist in the entity. The auditor shall evaluate his status and role in the entity and evaluate relevance and effectiveness of his work. However, an IT audit specialist might be considered, for example, on new engagements, clients undergoing IT expansion or development, or in case of complex IT environment.

This documentation template consists of generic questions applicable to most of the CIS environments, headed by a control objective. Supporting questions assist the auditor in understanding and evaluating the stated objective. For most of the supporting questions, there is a 'consider', providing the auditor with matters to think about when answering the question.

The auditor’s understanding and evaluation shall be based on inquiries primarily of the client’s IT staff, inspection and/or observation.

Refer to ISA 315 (Revised) for more detailed guidance on the understanding and evaluation of the IT environment.

**General Purpose CIS Template**

|  |  |  |
| --- | --- | --- |
| **Control objective** | **Objective satisfied?**  **Yes/No** | **Summary of findings** |
| **Organization and Management Policies**  **To ensure that organizational policies and management procedures are in place to enable the IT function to be properly controlled.** |  |  |
| **Supporting questions** | **Yes/No** | **Comments** |
| **IT strategy** | | |
| Is there a formal documented plan for IT covering systems to be developed or enhanced over the next 1 - 3 years? |  |  |
| Is there an IT Steering Committee?  Consider:   * Other, less formal, means of establishing and communicating IT strategy * User management representation |  |  |
| **IT policies and procedures** | | |
| Are there formal and comprehensive IT policies and procedures relating to Information Security, User Access Management, Program Change Management, Backup Management, Password Management etc.?  Consider:   * Approval at board level * Objectives * Scope * Responsibility for monitoring or update * Distribution to staff |  |  |
| **Role of internal audit** | | |
| Is the internal audit department involved in review of IT controls?  Consider:   * Competence of internal audit personnel * Frequency of review * Matters raised in such reviews and its implication on audit |  |  |
| **IT security function** | | |
| Is there a formal IT Security function in the organization?  Consider:   * Roles and responsibilities of IT security function * Reporting lines (independent of IT) * Security awareness trainings |  |  |
| **Control consciousness** |  |  |
| Is the attitude of management and the structure of the organization conducive to control consciousness? |  |  |
| **Control objective** | **Objective satisfied?**  **Yes/No** | **Summary of findings** |
| **Segregation of Duties**  **To ensure there is reasonable segregation of duties for staff, both within the IT department and between the IT and user functions, to prevent and/or detect errors or irregularities.** |  |  |
| **Supporting questions** | **Yes/No** | **Comments** |
| Is there an organizational chart for the IT department?  (Attach copy) |  |  |
| Is segregation of duties within the IT department appropriate for the size of the organization?  Consider:   * Number of IT staff * Segregation of functions e.g. * Systems programmers * Application programmers * Database administrator * IT operations * Data input * Network security * Reliance on key personnel * Reliance on contract staff |  |  |
| Do IT staff only have responsibilities for functions within the IT department?  Consider:   * Responsibility for initiating or authorizing transactions * Amendments to master files * Correction of input errors |  |  |
| **Control objective** | **Objective satisfied?**  **Yes/No** | **Summary of findings** |
| **Logical Access Controls**  **To ensure that unauthorized access cannot be gained to sensitive data or programs.** |  |  |
| **Supporting questions** | **Yes/No** | **Comments** |
| Have sensitive data or applications been identified? |  |  |
| Have appropriate security measures been  implemented to restrict users' access to  data and programs?  Consider:   * User-id and passwords * Menu facilities * Management approval of menu options * Periodic review of appropriateness of access rights * Review of security logs |  |  |
| Check from the system controls relating to  passwords:   * Password length (e.g. 6 characters). * Password composition (e.g. alphanumeric) * Password change interval (e.g. 90 days) * Account lockout (e.g. 3 invalid attempts) * Password history (e.g. 5 password remembered) * Force password change on first login * Session time out (e.g. 10 min of inactivity) * Concurrent sessions allowed |  |  |
| Are system development staff prevented from accessing data and software in the live environment?  Consider:   * Segregation of live and test environments * Procedures for emergency changes e.g. documentation or review |  |  |
| Is the allocation, authorization and use of powerful user-ids (e.g. system administrator, database administrator etc.) or passwords controlled and monitored?  (Note to whom these user ids are  assigned) |  |  |
| **Control objective** | **Objective satisfied?**  **Yes/No** | **Summary of findings** |
| **Physical Access Controls**  **To ensure that the risk of accidental or malicious damage to, or theft of, computer equipment or media is minimized.** |  |  |
| **Supporting questions** | **Yes/No** | **Comments** |
| Is there adequate physical security over computer equipment, data, media and documentation?  Consider:   * Buildings (including the protection of * terminals) * Server room * Communications equipment * Fire proof storage for magnetic media * Fire prevention or detection * Off-site storage |  |  |
| **Control objective** | **Objective satisfied?**  **Yes/No** | **Summary of findings** |
| **Systems Development and Program**  **Change Controls**  **To ensure that systems development**  **and program changes are authorized, tested, documented and operate as designed.** |  |  |
| **Supporting questions** | **Yes/No** | **Comments** |
| **In-house developments** | | |
| For in-house developed systems, is there a formal methodology?  Consider:   * Formal software development methodology adopted * Internal procedures developed by the systems development team * Prototype software * Programming standards followed |  |  |
| **Packages** | | |
| Is the business dependent on externally  supplied and maintained application  systems?  Consider:   * Maintenance agreement with the supplier * Changes and upgrades checked and tested before installation * Source code provided * Measures to prevent unauthorized access to the software * If the software is owned by the supplier, is there an escrow agreement? |  |  |
| **Other** | | |
| Are users appropriately involved in the systems development process?  Consider:   * Specification of requirements * Contribution to priority setting * User sign offs * User acceptance testing * Training * Formal approval before implementation * Development of user manuals etc. |  |  |
| Are development staff restricted from implementing new program versions into the production environment? |  |  |
| Is comprehensive systems and program documentation produced?  Consider:   * Compliance with standards * System documentation * Operating instructions * User documentation |  |  |
| Are there program change control procedures?  Consider:   * Program change documentation * Management authorization * Test procedures * User involvement in authorizing and testing |  |  |
| **Control objective** | **Objective satisfied?**  **Yes/No** | **Summary of findings** |
| **Business Continuity and Computer**  **Operations**  **To ensure that the business will be able to resume effective operations (within a reasonable period of time) in the event that the existing processing facilities are no longer available.** |  |  |
| **Supporting questions** | **Yes/No** | **Comments** |
| **Backup procedures** | | |
| Are backup copies of data files and programs taken regularly?  (Note the backup cycle)  Consider:   * Data at end of day, week, month, year * Whether back up taken after changes in the application |  |  |
| Are backup copies held in a secure location remote from the computer site?  Consider:   * Data files * Programs * Systems software * Systems documentation * Operating procedures * User procedures * Disaster recovery plan |  |  |
| Are backup versions taken offsite regularly? |  |  |
| Have the backup and restoration procedures been tested?  Consider:   * Time taken to restore * Completeness and accuracy of data restored |  |  |
| **Disaster Recovery Planning** | | |
| Have the business's critical systems without which the entity’s operations and business could be affected have been identified?  Consider:   * How long could the business operate effectively without their critical computer systems e.g. hours, less than seven days, etc.? |  |  |
| Has a disaster recovery plan been developed, documented and tested?  Consider:   * Regular review and update of the plan (Note when it was last updated) * Periodic testing (Note when last tested) |  |  |
| **Insurance** | | |
| Does the organization have adequate insurance cover relating to its IT risks?  Consider:   * Loss of computer equipment and data * Consequential loss * Additional cost of working * Denial of access * Exclusion clauses |  |  |
| **Control objective** | **Objective satisfied?**  **Yes/No** | **Summary of findings** |
| **User Management e.g. Finance Director/ Financial Controller/ Chief**  **Accountant**  **To ensure that IT systems satisfy the business needs.** |  |  |
| **Supporting questions** | **Yes/No** | **Comments** |
| Are users satisfied with the critical accounting systems?  Consider:   * Management information * Timeliness of reporting * User friendliness * Response times |  |  |
| Are the systems stable?  Consider:   * Few modifications since, say, six months before the start of the accounting period * New systems planned |  |  |
| **Conclusion**  **Summarize the internal control weaknesses identified which have an impact on the control objectives, for consideration when planning reliance on CIS controls.** | | |
|  | | |