### IT INTERNAL CONTROL CHECKLIST

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Auditee:** |  | **Reviewed by:** | **Name** | **Rank** | **Date** |
| **Period end:** |  | **Level 1** |  |  |  |
| **Prepared by:** |  | **Level 2** |  |  |  |
| **Rank:** |  | **Level 3** |  |  |  |
| **Date:** |  | **Date:** |  |  |  |

The following table can be used to document the application systems of the auditee.

| Application name | Description and purpose of the application | Modules / subsystems of application used | Does the system interface with the financial system? Give brief description of the nature and frequency of the interface. |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

For identified application systems, complete the following questions.

| **Focus area** | **Answer**  **Yes / No** | **Examples of evidence to be obtained / verified** | **What could go wrong if control have not been implemented?** | **Reference to evidence obtained** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| ***Information Technology governance*** |  |  |  |  |  |
| 1. Does the organization have an IT strategic committee? |  | Request and obtain ICT strategic committee meeting minutes | The non establishment of an IT strategy committee at the board level could result in IT governance , as part of enterprise governance, not being adequately |  |  |
| 1. Does the organization have an IT strategic plan that supports business requirements and ensures that IT spending remains within the approved IT strategic plan? |  | Approved IT strategic plan | The non establishment of an IT strategic plan could result in IT goals not contributing to the departments strategic objectives and related costs and risks |  |  |
| 1. Does the organization have an active IT steering committee? |  | Minutes of meetings | IT governance which forms part of the organizational governance structure are not adhered to |  |  |
| 1. Are there defined roles and responsibilities for each IT function / role-player |  | Organisational chart , IT business plan. If none, ask the IT director to describe each role player. | Undefined IT roles and responsibilities could result in the IT function that is non-responsive to the department’s needs |  |  |
| 1. Is a training program to build IT capacity in place? |  | Request and obtain a program for training and the transfer of skills. | Lack of defined IT training could result in IT function failing to meet operations as well as creating reliance on key staff members |  |  |
| 1. Does the entity make use of service providers? if so, are there service level agreements in place for all vendors to whom IT services has been outsourced. |  | Obtain a list of outsourced activities and obtain copies of signed service agreements with all service providers, cross check the list with the agreements | The non-establishment of service level agreements could result in poor understanding of IT cost, benefits, strategy, policies, service levels and not ensuring satisfaction of end users with service. |  |  |
| ***Security management*** |  |  |  |  |  |
| 1. Is there a formally approved IT security policy to ensure data confidentiality, integrity and availability? |  | Approved IT security policy | If an organisation does not have an security policy there is no clear direction to maintain information security across the organisation and to properly safeguard the organisations’ assets. |  |  |
| 1. Does the organization have installed anti-virus programs on all computers which is updated regularly? |  | Discussion, observation and screen dump of the antivirus program | IT services could be interrupted, data corruption could occur. |  |  |
| 1. Is there a process in place to ensure up-to-date security on all systems software (patch management process) |  | Patch management procedures and process (patches and updates regarding e.g. operating system, anti-virus, firewall, etc., frequency) | The system software could not function properly. |  |  |
| ***Program change management*** |  |  |  |  |  |
| 1. Are there formally documented and approved processes to manage upgrades made to all financial / performance information systems? |  | Approved procedures / guidelines on how changes and upgrades to packages systems are to be handled? | Unauthorised changes are made to the systems, changes are made without being properly tested first, there is a lack of supporting change request documentation for changes made, changes made do not address user requirements. |  |  |
| 1. When an upgrade is made to the systems, is formal change request documentation completed indicating the change to be made and the reasons for all changes to the financial systems? |  | Examples of change request documentation completed. | Unauthorised changes are made to the systems, changes are made without being properly tested first, there is a lack of supporting change request documentation for changes made, changes made do not address user requirements. |  |  |
| 1. Do programmers have access to the test and live environments? If packaged systems, does the vendor have access to the production environment? |  | Discussion with the system administrator, programmers, / vendor, printout from system including vendor / programmer access | Unauthorised changes can be made to the system, changes are not properly tested, lack of supporting documentation for changes made, changes made do not address user requirements. |  |  |
| ***Physical access controls*** |  |  |  |  |  |
| 1. Are there policies in place which cover physical access to IT environments? |  | Discussions with management and observation | Unauthorised access to IT environments could result in damages to hardware, theft, etc. |  |  |
| 1. Is physical access to sensitive areas (such as computer room, operations, storage rooms, network rooms etc.) controlled? |  | Discussions with management and observation | Unauthorised access to IT environments could result in damages to hardware, theft, etc. |  |  |
| 1. Is physical access properly controlled after hours? |  | Signed off logs to these areas. | Unauthorised access to IT environments could result in damages to hardware, theft, etc. |  |  |
| ***Environmental controls*** |  |  |  |  |  |
| 1. Are there policies and procedures in place to cover environmental controls? |  | Discussions with management and observation | If environmental controls are not properly addressed, the organisation might not recover from an interruption at all or quickly enough. |  |  |
| 1. Are the following environmental controls in place:  * Fire suppression systems * Fire extinguishers * UPS, generators, * Air conditioning systems (especially in computer room) * Humidity, temperature control systems |  | Observation | If a organisation does not have proper controls in place, the organisation might not recover from an interruption at all or quickly enough. |  |  |
| 1. Is there a formal, documented and tested emergency procedure in place? |  | Register of emergency procedures carried out. | In case of an emergency, the personnel involved might not be aware of what is expected from them and lead to business interference. |  |  |
| ***IT service continuity*** |  |  |  |  |  |
| 1. Does the entity have a disaster recovery plan? |  | Approved disaster recovery plan | The auditee might not be able to recover from such disaster. |  |  |
| 1. Are copies of the IT continuity plan and disaster recovery plan kept off-site |  | Agreement with entity where plans are kept | Should a disaster occur, the auditee might not be able to access the disaster recovery plan. |  |  |
| 1. Has a backup and retention strategy been implemented? |  | Approved backup and retention strategy | If no backups exist and a disaster occurs, the organisation may not be able to continue services. |  |  |
| 1. Are backups performed, verified and checked for successful completion? |  | Review of, for example, backup register / log that is signed off | If no backups exist and a disaster occurs, the organisation may not be able to continue services |  |  |
| 1. Are backups stored in a secure offsite storage facility? |  | Inspect offsite location /agreement with external party | If backups are not stored at an offsite location the organisation might not recover from a disaster |  |  |
| ***Logical Access control*** |  |  |  |  |  |
| 1. Is there a formally documented and approved user management standards and procedures in the organization? |  | Formal approved user account management policy | Without a sound and approved framework users do not have any rules and procedures to follow in order to minimize risk of errors, fraud and the loss of data confidentiality, integrity and availability. |  |  |
| 1. Are processes in place to review user access rights on the system and if the rights are in line with their responsibilities |  | Evidence of reviews | Unauthorised user access to systems. |  |  |
| 1. Does every user have a unique user name |  | Lists of active users on the system. | User IDs which are not linked to specific persons could result in a lack of accountability |  |  |

**Conclusion**

**The following risks have been identified:**

***[All risks identified will be taken to the of Risk of material misstatement on financial statement level working paper]***