Template 23 : Assessing general IT controls and application controls

This template is to be completed together with the Understanding the IT environment template. The purpose of the template is to assess the IT general and application controls for non-complex IT environment. The form can be completed by the general auditor. However, for IT complex environment, IT Audit specialist services should be utilized.

SECTION A . IT SECURITY

Control objectives:

1. To prevent unauthorized access and interference to IT services and to protect IT facilities from environmental damage
2. To restrict access to IT resources to authorized personnel in accordance with their job requirements
3. To prevent and detect unauthorized disclosure, unauthorized amendment and breach of system integrity

For this section supply brief details of the controls identified in relation to the following questions

Key control questions	***Yes/No***	***Remarks***	***WP ref***
A. 1 IT Security Policy			
Has the management formulated an IT Security Policy which has been distributed throughout the entity? (use of email, malicious or unauthorized software, program change controls, IT security responsibilities, interaction with third parties and contractors, password management, use of internet.)	☐ Yes ☐ No		
Have effective measures been taken to create awareness regarding IT security amongst staff?	☐ Yes ☐ No		
A. 2 Physical and environmental controls			
Has the management carried risk assessment for identifying the threats to the systems, the vulnerability of system components and likely impact of an incident occurring and have counter-measures been identified to reduce the level exposure to an acceptable level?	☐ Yes ☐ No		

Key control questions	***Yes/No***	***Remarks***	***WP ref***
Are Physical access controls for ensuring physical access to IT systems to only those who have been authorized by management, adequate?	☐ Yes ☐ No		
Are environmental controls for minimizing the damage to IT equipment and threat to IT personnel from accidental happenings such as fire, flooding, and power surges, etc., adequate?	☐ Yes ☐ No		
A. 3 Logical Access Controls			
Are the Logical access controls aimed at protecting computer resources (data, programs and terminals) against unauthorized access attempts, adequate?	☐ Yes ☐ No		
Is there an effective system of password administration consisting of security of password tables, password encryption, periodic changing of passwords by users and strict policy for password non-disclosure?	☐ Yes ☐ No		
Is there a mechanism for account lockout after a number of failed log on attempts	☐ Yes ☐ No		
Is there a method of logging a monitoring failed log on attempts by user account and by location?	☐ Yes ☐ No		
Is the password files encrypted and access to password file restricted? Is access to password files logged and monitored?	☐ Yes ☐ No		
Have the users been properly trained about the necessity of maintaining security and the use of strong passwords? Have they been warned about bad password maintenance and change practices such as writing down or sharing passwords?	☐ Yes ☐ No		
Is there a mechanism for transmitting the passwords securely?	☐ Yes ☐ No		
Are audit log files of system and resource usage maintained and are these log files secured?	☐ Yes ☐ No		

Key control questions	*Yes/No*	*Remarks*	*WP ref*
Are security events like unsuccessful attempts to gain access to system resources logged and investigated regularly? Has the management established a framework of adequate preventive, detective and corrective control measures to protect the IT systems from malicious software, such as computer viruses or Trojan horses?	☐ Yes ☐ No ☐ Yes ☐ No		

SECTION B: IT OPERATIONS CONTROLS

Control Objective:

1. To ensure efficient operation of IT facilities and monitoring of systems
2. To safeguard the integrity computer files against unauthorized access, loss, theft etc.

For this section supply brief details of the controls identified in relation to the following questions

Key control questions	*Yes/No*	*Remarks*	*WP ref*
B 1 IT Operations Are the data processing tasks performed by the Information Services Department scheduled to assure the efficient use of its facilities and to meet the requirements of its users? Are there documented procedures for the detailed execution of each job, which include following items: • Instructions for handling errors or other exceptional conditions which might arise when jobs are run? • Support contacts in the event of unexpected operational or technical difficulties? **B 2 System restart and recovery procedures?** Have the responsibilities for media library management been assigned to specific members of the Information Services	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

Key control questions	***Yes/No***	***Remarks***	***WP ref***
Department staff, and procedures designed to protect media library contents been established? Is a report of computer usage produced and scrutinized by management?	☐ Yes ☐ No		
Is there a process to ensure that the performance of information technology resources is continuously monitored and exceptions are reported in a timely and comprehensive manner?	☐ Yes ☐ No		
B 3 FILE CONTROL Are the password tables and system log files adequately secured? Are there general procedures which properly restrict and control logical access to data files? **B 4 SYSTEM /NETWORK ADMINISTRATION** Are the activities of the Information Systems Administration and Network Administration functions properly restricted and monitored by management with regard to the following criteria: • Availability, reliability and performance? • Levels of support provided to users? • Continuity planning and security? • Minimum acceptable level of satisfactorily delivered system: functionality • Change procedures?	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

SECTION C. ENTITY AND MANAGEMENT CONTROL

High level Control Objectives:

1. To ensure efficient and effective use of IT resources towards achievement of entity objective*
2. To provide an effective separation of duties within the Information Technology.

For this section supply brief details of the controls identified in relation to the following questions Supply relevant organizational charts where available

Key control questions	***Yes/ No***	***Remarks***	***WP ref***
C. 1 Strategic Planning			
Is an IT strategic planning process undertaken at regular intervals giving rise to long-term plans which are periodically translated into operational plans setting clear and concrete short-term goals?	☐ Yes ☐ No		
Has the management established an IT steering committee comprising representatives from senior management, the Information Service Department and user department to oversee Information Service Department Activities?	☐ Yes ☐ No		
Has the information services function created a Technological Infrastructure Plan which in regularly updated in accordance with the Information Technology long and short-range plans?	☐ Yes ☐ No		
If major new IT system are being acquired, has the IS Management ensured that hardware and software acquisition plans are established and reflect the needs identified in the technological infrastructure plan?	☐ Yes ☐ No		
C. 2 Segregation of duties			
Is the IT Department physically and separate from the User sections?	☐ Yes ☐ No		

Key control questions	***Yes/ No***	***Remarks***	***WP ref***
Have policies and Procedures describing the manner and responsibilities for performance governing relations between the Information Services Department and user departments been established and communicated to all affected departments Is there adequate segregation of duties within the Information Systems Division between the following functions: • Systems design and programming • Systems administration and support • IT operations • Network management • Data input and data control • Media Library management • System security • Database administration • Change management	☐ Yes ☐ No ☐ Yes ☐ No		

SECTION D. SYSTEMS CHANGE CONTROL

Control Objective:

1. To ensure that all changes to IT systems are properly authorized, tested and that an audit trail of the changes made is maintained

For this section supply brief details of the controls identified in relation to the following questions

Key control questions	***Yes/No***	***Remarks***	***WP ref***
D. 1 Change controls For proposed changes to applications, do the procedures provide for the analysis, implementation and follow-up of all changes requested and do take into consideration the following	☐ Yes ☐ No		

Key control questions	*Yes/No*	*Remarks*	*WP ref*
• Identification of changes? categorization, prioritization and emergency procedures • Impact assessment? Change authorization? Thorough testing before acceptance? • Management of release from development to production? • Adequate audit trail of the changes?			
Are there procedures to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails?	☐ Yes ☐ No		
Are the above procedures or similar controls, applied to amendments to operating system software?	☐ Yes ☐ No		
Is the use of any Special Amendment facilities: • Properly recorded? • Restricted by management authorization and subsequent review?	☐ Yes ☐ No		

SECTION E. BUSINESS CONTINUITY AND DISASTER RECOVERY CONTROLS

Control Objective:

1. To make IT services available as required and to ensure minimum business impact in the event of a major disruption

2. To ensure data can be reconstituted following file loss or corruption

For this section supply brief details of the controls identified in relation to the following questions

Key control questions	*Yes/ No*	*Remarks*	*WP ref*
E. 1 Business Continuity and Disaster Recovery Planning			

Key control questions	***Yes/ No***	***Remarks***	***WP ref***
Is there a written Information Technology Continuity Plan or written procedure which provide for the following: • Emergency procedures to ensure the safety of all affected staff members • Response procedures to continue critical IT applications? • Recovery procedures meant to bring the business to the state it was in before the incident or disaster?	☐ Yes ☐ No		
Is the system continuity and disaster recovery plan adequately documented and tested at least annually?	☐ Yes ☐ No		
E. 2 Data Back Up			
Is adequate data file back-up procedures followed to ensure data can be reconstituted in the event of file loss or damage?	☐ Yes ☐ No		
Are copies of programmes and back up data files held in a remote facility?	☐ Yes ☐ No		
E. 3 Standby Facilities			
Are there formalized and properly documented arrangements to enable critical processing to continue in the event of prolonged system failure? • Do these arrangements cover data preparation where appropriate? • Do these arrangements provide for adequate operational control at the back-up site? • Are the standby arrangements tested at least annually?	☐ Yes ☐ No		

SECTION F : REVIEW OF APPLICATION CONTROLS

The audit objectives of an application systems controls review are to:

1. Ensure that all input data are authorized and complete, and data are consistently recorded, accumulated, processed, and reported in a controlled environment to produce timely and accurate information by the concerned applications.

2. Ensure that the output produced is complete, accurate, and useful for its intended purposes. The goal is to minimize potential risks, exposures, and losses due to processing errors, omissions, and irregularities

Identify the major financial applications. For each application supply brief details of the controls identified in relation to the following questions

Key control questions	***Yes/ No***	***Remarks***	***WP ref***
Data capture and preparation Control objective : Adequate controls and procedures over data origination and preparation activities exist to ensure completeness ,accuracy and validity of captured transactions			
Is there a procedure for capturing input data on pre-designed forms? Are the input documents are being authorized by officers at appropriate levels?	☐ Yes ☐ No ☐ Yes ☐ No		
Data Input Control objective : Adequate controls and procedures over data input activities exist to ensure completeness , accuracy and validity of inputs			
Batch controls Have the batch controls over input documents been established? If yes, are procedures relating to establishing batch control totals and hash totals and preparation of batch headers being followed? Are there programmed procedures to automatically calculate the batch totals from the batch input documents and compare it with the manually established batch totals?	 ☐ Yes ☐ No ☐ Yes ☐ No		
Is there is a procedure for correcting and resubmitting rejected batches? If yes is this procedure is being followed?	☐ Yes ☐ No		

Key control questions	***Yes/ No***	***Remarks***	***WP ref***
Are there validation programs such as range checks, formats checks, limit checks, check digits for detecting and correcting errors in batch data input? <u>Online systems</u> For on-line terminals, are input data validated and errors corrected as data are entered into the computer system? For on-line systems, are the methods to prevent data entry errors such as self-help features, pre-selected formats or menu selection, and operator prompting, effective? For transactions entered through on-line terminals, are all input transactions automatically logged with date and time of transmission, Are information relating to user department, terminal, and user identification captured as part of the input transaction record ? Are transaction logs for on-line input terminals being reviewed by users to detect any unauthorized access and entry of data? Do the computer programs include automated internal program processing controls in the form of data input edit and validation routines (such as check digits, reasonableness tests, batch totals, and record counts). IF yes are these control effective? Are input error correction and resubmission procedures adequate and effective?	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
When a correction is reentered into the system, is it subject to the same program edit and validation controls as the original transaction? <u>Controls over master files and tables</u> Are there strong controls over data entry into master files such as *one for one check, validation programmes, edits and error correction and resubmission*? Are these adequate?	☐ Yes ☐ No ☐ Yes ☐ No		

Key control questions	***Yes/ No***	***Remarks***	***WP ref***
Are master files and internal tables reviewed periodically to ensure the accuracy of their values?	☐ Yes ☐ No		
Have access to master files data and internal tables restricted to authorized personnel only?	☐ Yes ☐ No		
Have adequate audit trails been incorporated in the application system?	☐ Yes ☐ No		
<u>Data Output</u>			
Do the users reconcile input control totals to output control and report totals?	☐ Yes ☐ No		
Do data control personnel scan output reports to detect obvious errors such as missing data fields, unreasonable values, and incorrect report format before distributing to users?	☐ Yes ☐ No		
Is the system of identification of e.g. report name and number, date produced, accounting month-end or other effective date, Entity name and department name and number, page number, program number (if necessary), subtotals, and report totals, adequate ?	☐ Yes ☐ No		
Is a report distribution lists being used to prevent reports being received by unauthorized users ?	☐ Yes ☐ No		
Are outdated and unneeded output reports destroyed by shredding instead of placing them in a waste container?	☐ Yes ☐ No		

CONCLUSION: Are the following objectives achieved and if not what is the severity of identified risks.

	High	Medium	Low
Section A . IT Security			

Section B: IT Operations Controls			
Section C. Organization and Management Control			
Section D. Systems Change Control			
Section E . Business Continuity and Disaster Recovery Controls			
Section F : Review of Application Controls			

	Date	Initials
Prepared by		
Reviewed by		