सत्यमेव जयते

INDIAN AUDIT AND ACCOUNTS DEPARTMENT

Regional Training Institute, Chennai

(Centre for Excellence)

In Search of Excellence Series – Research - Study Material No.17

RESEARCH - STUDY MATERIAL ON

INFORMATION SYSTEMS AUDIT – A CHECK LIST

361, Anna Salai, Chennai 600 018.

Preface

Information Systems have been introduced in most of the Government Departments thereby increasing the necessity for the Auditors to be equipped in IS Audit and to carry out reviews of the Information Systems during the regular transaction audits. The Research ï Study material is prepared based on the analysis of various Information System Audit engagements conducted by leading Institutions, Professional Bodies and the experience of our own Department. We have consulted KPMG, Ernst & Young and referred the AICPA Guidelines, ASOSAI Research Material and IA&AD IS Audit manual. With the intention of helping the Auditors, this Research ï Study material has been compiled by RTI, Chennai.

I hope, this Research - Study material will definitely be of much help to the readers as the previous study materials.

S.Prabhu
Principal Director

INFORMATION SYSTEM AUDIT - CHECK LIST

INTRODUCTION

The use of Information and Communication Technology (ICT) within government entities has become increasingly significant in recent years, particularly following greater use of the Internet and organisational intranets. Technology has increased the amount of data and information being processed and it has significantly impacted the control environment. ICT is also now a key component of government entitiesô business strategies and core business processing activities.

As computer technology has advanced, Government organisations have become increasingly dependent on computerised information systems to carry out their business operations and service delivery and to process, maintain and report essential information. There are also an increasing range of ICT vulnerabilities and threats that have to be effectively and efficiently managed. As a consequence, **the confidentiality, integrity, availability and reliability of computerised data and of the systems that process, maintain and report these data are a major concern to audit**. IT auditors evaluate the effectiveness and efficiency of IT controls in information systems and related operations to ensure they are operating as intended.

IS AUDIT

IS audit is '*the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organisational goals to be achieved effectively and uses resources efficiently*'. An effective information system leads the organisation to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives.

Use of computer facilities has brought **about radically different ways of processing, recording and controlling information and has combined many previously separated functions.** The potential for material systems error has thereby been greatly increased causing great costs to the

organisation. **The IS internal controls** are of great value in any computerised system and it is an important task for an auditor to see that not only adequate controls exist, but that they also work effectively to ensure results and achieve objectives.

NEED FOR IS AUDIT

Typically, managementôs goals and objectives in utilising technology to support business processes include:

- **Confidentiality;**
- **Integrity;**
- **Availability;**
- **Reliability; and**
- **Compliance with legal and regulatory requirements**.

Underpinning these goals and objectives is the need to ensure information technology, and the controls supporting such technology, assists the organisation to achieve its business objectives (effectiveness) with appropriate use of resources (efficiency).

IS AUDIT OBJECTIVES

The objective of undertaking an IS audit is to evaluate an auditee's computerised information system (CIS) in order to ascertain whether the CIS produces timely, accurate, complete and reliable information outputs, as well as ensuring confidentiality, integrity, availability and reliability of data and adherence to relevant legal and regulatory requirements. Audit objectives will vary according to the nature or category of audit i.e. a financial statement or performance audit. For example if the audit has a financial focus, then the primary objective will be to offer an opinion as to whether the financial statements reflect a true and fair view of the entityôs financial position.

The objectives of undertaking an IS audit as components of a financial statement audit include:

- **To understand how well management capitalises on the use of information technology to improve its important business processes;**
- **To understand the pervasive effect of information**

technology on the client's important business processes, including the development of the financial statements and the business risks related to these processes;

- **Understand how the client's use of information technology for the processing, storage and communication of financial information affects the internal control systems and our consideration of inherent risk and control risk;**
- **Identify and understand the controls that management uses to measure, manage and control the information technology processes; and**
- **Conclude on the effectiveness of controls over the information technology processes that have a direct and important impact on the processing of financial information.**

The following steps provide an overview of the tasks involved in process of IS Audit:

PRELIMINARY DATA GATHERING CHECK LIST

1. Determine the personnel responsible

Determine the IT staff and primary users responsible for the oversight of IT Application(s) being audited.

2. Technical Information about the Systems

- **Determine what hardware is used to run the system,**
- **Classify the system as micro, LAN, client/server or mainframe based.**
- **Determine what operating system is used to control the environment.**
- **Determine if the software was purchased or developed in-house.**
- **When it was developed and what modifications have been made since the initial development?**
- **If the software was purchased, determine if any vendor warranties are still in force.**
- **Verify that the software was developed and updated based on a sound "Systems Development" methodology.**

- **Identify the programming languages used in the application.**
- **Determine who is responsible for normal and abnormal maintenance.**
- **If responsibility is in-house, determine if the IT department has programming staff knowledgeable in these programming languages.**
- **Determine whether the system processes data on-line, by batch or in combination.**
- **Identify the types of data files used in processing (database, sequential files, disk tape).**
- **Identify the primary transaction, master and reference files used in processing and where they come from (data entry, automatic transfer, etc.).**
- **Determine how the IT department controls and secures access to the application programmes and data.**
- **Identify the access facility to control basic sign-on and any others such as database task definitions, file and record restrictions, etc.**
- **Browse the programmers' Application Documentation (This should include system and program flowcharts, decision tables, file layouts, data element definitions narratives, source program listing, and record of changes. The documentation should also indicate on which platform the various portions of the system operate).**
- **Browse and evaluate the quality of the application operations documentation. (This should include job and system flowcharts, input and output descriptions, job frequency and sequence of operation, job restart / recovery procedures, file backup requirements and procedures, error messages and reconciliation techniques, report distribution procedures, data capture instructions).**
- **Determine if backup copies of application program and**

operations documentation are stored off-site.

- **Determine** if the IT department monitors processing flows to verify application program run according to schedule

3. End User Computing Information

- **Interview** a sample of end-user managers to determine end-user management attitudes regarding the quality and effectiveness of the system.
- **Determine** from end-user management what they perceive to be the risks, exposures and limitations associated with the system.
- **Determine** the number of end-users working with the system, their locations and responsibilities associated with the system.
- **Obtain** an organisation chart for these positions and people.
- **Determine** if this application generates data for legal or regulatory agencies.
- **Evaluate** the quality of end-user documentation (This should include description of the system, description of source documents and procedures for their preparation, job submission procedures, control procedures, error identification and correction procedures, description of output reports and their use).
- **Identify** the application training available for end-users.
- **Evaluate** this training to determine if it is adequate, current and available for new people.
- **Determine** how much training has actually been provided.
- **Determine** if end-user activity is adequately supervised.

4. Information about System Interfaces

- Are there interfaces of the Application being audited with other applications. If yes, then what is received from and what is sent to these other applications.
- **Determine** how end users verify or assure that the interfaces are providing complete, accurate, and authorised data

5. Information about File Handling

- **Determine the retention periods for the various key application data files.**
- **Evaluate if the retention periods satisfy management reporting, and other legal and internal accounting requirements.**
- **Determine if management and data owners are aware of the retention periods of the various key application data files, and if these managers are satisfied with the length of retention.**
- **Determine whether actual retention is consistent with requirements.**

6. Backup and Recovery Procedures

- **Identify the key system files**
- **Determine how often key files are backed up.**
- **Determine if copies of these backup files are stored at a suitable off-site location.**
- **Assess whether that the off-site backup files storage facilities are secure.**
- **Determine if application recovery plans exist (both technical and end-user) for restoring from short-term and long-term interruption of computer processing.**
- **Verify whether these plans address both technical restoration needs and alternative end-user processing procedures.**
- **Determine if these application recovery plans have been tested regularly.**
- **Establish how long the organisation could comfortably function and avoid significant financial loss if the computerised aspects of this application failed.**
- **Verify that restart/recovery and disaster recovery plans provide for restoring this application the time needed to avoid significant financial loss.**

- **Evaluate alternate plans of the management, should the application not be able to be restored in time.**
- **Determine if the IT department has established data file and record retention periods.**
- **Determine if these retention periods are reasonable for backup, disaster/recovery and audit purposes.**
- **Verify that restart/recovery plans from short-term computer interruptions include the ability to identify the status of all processing to the point of application failure to establish a cutoff for transaction re-entry.**

7. Identify all Sub-systems

- **Identify all subsystems associated with this application and the objectives of each sub-system**

8. Information about Data Input

- **Determine whether data entry procedures and controls are effective to ensure complete and accurate input of data.**
- **Determine that online edit routines identify inaccurate data as early as possible and prevent the entry of invalid / duplicate / out of period data into the system.**
- **Determine that invalid data is properly rejected during subsequent processing of data input.**
- **Review transactions and determine that the screens are effective and useful.**
- **Determine that controls over correcting errors are effective and that errors are corrected and resubmitted on a timely basis. Identify any cost beneficial improvements in error correction procedures.**

9. Processing Information

- **Determine that job documentation is accurate and effective for proper scheduling and restart/recovery.**
- **Review user and IT data control procedure relating to job scheduling to ensure that jobs are run in the correct sequence, and that no data is inappropriately added,**

changed or lost during processing.

- Review the IT problem reports to identify problems relating to the application system.
- Determine that end user problems are identified and resolved on timely basis.
- Determine if any significant problems are not reflected on the problem reports and follow up as required.

10. Information about Output

- Review output distribution to determine that output is distributed on a timely basis only to authorised personnel and that restricted output is properly labeled.
- Review user balancing and reconciliation procedures to ensure that out of balance conditions are resolved on a timely basis.
- Reviews reports generated with users and determine their necessity and usefulness.
- Determine if any reports could be eliminated or if any additional reports could be beneficial.
- Determine that reports are retained for proper periods of time.

11. Change Management Information

- Determine program change requests are documented in writing that users assist in developing test data, review test results, and approve all program changes in writing prior to being placed into production.
- Review controls over changes to user developed programs (if these programs perform significant processing).

General IS Controls: A Check List

A performance of IS Audit General Controls review will include all IS related policies, procedures, data security administration, data center operations, system development / maintenance, the IS Disaster / Recovery plan and its relation to the Corporate Business Continuity plan.

IS GENERAL CONTROLS	YES	NO	Remark
Planning			
Determine if committees review, approve, and report to the board on: • Short and long term information systems plans • IT operating standards • Data security policies and procedures • Resource allocation (major hardware/software acquisition and project priorities) • Status of major projects • IT budgets and current operating cost			
Policies, Standards, and Procedures			
• Determine whether the board of directors has reviewed and approved ITôs policies			
Examine how IT management has defined standards and adopted a methodology governing the process of developing, acquiring, implementing, and maintaining information systems and related technology. Determine if IT management has adequate standards and procedures for: • Systems development • Program change control • Data Center operations • Data Base administration • Performance monitoring • Capacity planning • Network administration • Information security • Contingency planning/disaster recovery			
Assess compliance with these policies and procedures.			
Data Security Administration and Accountability			
Verify the names associated with the DBA function. Determine that the DBA is prohibited from routine operating duties in the computer facility. (this person should not have system operating duties and should be sufficiently independent from the computer operation to ensure that he/she cannot create, delete, or suppress passwords in order to cover improper activities.)			

Security Policy			
Review the data security policy Determine if the security procedures cover: • Physical protection of the facility. • Designation and duties of the security officer(s). • Authorised data and program access levels. • Requirements for password creation and change procedures. • Requirements for access via terminals, modems or computer system (LAN) connection. • Monitoring and follow-up of security violations. Determine whether procedures are in place to update the security policy. Ensure updates to the policy and procedures are distributed to and reviewed by management. Determine if an education program has been implemented to promote user awareness about security policies and procedures.			
Data and Program Security			
Determine how access levels are granted. • Whether all access is restricted unless specifically authorised. • If the password file is controlled (e.g., encryption). • How security violations are detected and reported. Determine that password security is in effect on all applications. Assess the adequacy of controls over: • Development and test programs. • Identify whether levels of access are periodically reviewed. • Assess whether passwords, user IDs are adequately controlled • for: • Changing on a regular basis • Suppressing passwords on a terminal. Determine that passwords are removed as soon as an individual's employment is terminated to ensure that a terminated employee cannot gain access to the computer files through an outside terminal.			

Security Controls	YES	NO	Remark
• Obtain copies of the security access and control files for the operating system. • Obtain a list of data altering utilities, user exits, user interface programs, and privileged commands. Using these documents, determine: • Whether the data security administration function is independent of systems and programming. • If all programmers have unique user IDs and passwords. • If system access levels are consistent with job functions. • If all changes to the system security software are approved by the system security administrator. • If security software provides an adequate audit trail to identify the programmer, the programs or utilities used, the files or programs accessed and the nature of the access. • The adequacy of segregation of duties for application programming, systems programming, computer operation, and system security functions. • If physical or logical separation between the production and test environments is maintained. • The adequacy of controls over dial-up access.			
IT Servicing			
Provider			
• Obtain a list of services performed by the data processing center. • Determine if written contracts are in effect for all customers. • Review a copy of the contract(s) used.			
Receiver			
If receives major support from one or more outside service provider(s): • List the name(s) and location(s) of the service provider(s). • Prepare a listing of the services outside vendors provide. • Assess the adequacy of the procedure for monitoring the financial condition of its service provider(s) and whether the procedure is sufficient to project the continued viability of contracted services.			

Insurance	YES	NO	Remark
Review the adequacy of insurance coverage (if applicable) for: • Employee fidelity (blanket-bond) • IT equipment and facilities • Loss resulting from business interruptions Determine whether the board of directors has approved requirements for related insurance coverage. Examine the business-interruption coverage limits.			
Recovery Planning			
• Determine if IT has a documented disaster recovery plan. • Verify that the IT disaster recovery plan supports the goals and priorities found in the corporate business continuity plan. • Review the IT disaster recovery plan to determine if it: o Clearly identifies the management individuals who have authority to declare a disaster. o Clearly defines responsibilities for designated teams or staff members. o Explains actions to be taken in specific emergency situations. o Allows for remote storage of emergency procedures manuals. o Defines the conditions under which the backup site would be used. o Has procedures in place for notifying the backup site. o Has procedures for notifying employees. o Establishes processing priorities to be followed. o Provides for reserve supplies. • Determine if all critical resources are covered by the plan. • Determine if a copy of the IT contingency plan is stored off-site. • Determine if the backup site: o Has the ability to process the required volume. o Provides sufficient processing time for the anticipated workload based on emergency priorities. o Allows the subsidiary to use the facility until it achieves a full recovery from any interruption. • Determine if there is physical security at the recovery			

site.
• Determine what agreements, commitments, or projections have been made with and by hardware vendors regarding the period of time required to replace hardware.
• Verify that vendors has been identified.
• Determine if:
  ○ Duplicates of the operating system are available on and off site.
  ○ Duplicates of the production programs are available on and off site (including both source and executable versions).
• Determine if all master files and transaction files are backed up adequately to facilitate recovery.
• Determine if the IT disaster recovery plan is tested at least annually, including critical applications and services
• Determine if the tests include:
  ○ Setting goals in advance.
  ○ Realistic conditions and activity volumes.
  ○ Use of actual backup system and data files from off-site storage.
  ○ Participation and review by internal audit.
  ○ A post-test analysis report and review process that includes a comparison of test results to the original goals.
  ○ Development of a corrective action plan for all problems encountered.
• Determine if several user departments have been involved in testing at the same time to uncover potential conflicts.			

SYSTEMS DEVELOPMENT AND PROGRAMMING			
Project Management and Control			
Determine whether there is a written plan for future changes to current hardware, software, or the addition of new applications. Obtain a copy of the plan and note major items.			
Standards			
Determine whether policies and procedures are adequate for: • Application systems / program development • Operating system maintenance • Program change control • Testing • Program and system documentation • Implementation			

Application Systems Development			
Obtain a list of all application systems currently in use or under development. Indicate if the applications were purchased or developed in-house. Determine whether: • All required documentation is present and sufficiently detailed to evidence complete compliance with established standards. • The structure of the System Development Life Cycle (SDLC) planning includes all appropriate phases and whether they were completed as prescribed by the plan. • The audit trails, exception reports and system security designs are adequate. • User manuals are adequate. • The board, senior management, applicable committees, computer operations, user departments, and audit were involved in all phases of the development process. For purchased software: • Determine whether new releases are tested before installation. • Determine if the most recent release is being used. Application Program Development Review selected documentation for at least one in-house developed program. Trace the program's development from the initial request through the post implementation review process. Determine: • If all required documentation is present and sufficiently detailed to evidence compliance with established programming procedures. • Whether the program meets the objectives of the original request, based on test results and user feedback. • For program requests, determine: • Whether program request procedures were followed. • If a user department was affected, whether there was appropriate consultation between users and the IT department. • Whether appropriate documentation and training was provided to users and computer operators.			
Operating System Maintenance			
Obtain and review the operating system installation plan, the system generation report, the system log, and other system related activity reports. Review changes made to the operating system and supporting system software to determine compliance with procedures.			

Determine if: • The overall supervision by management over system programmer activities is adequate. • Controls over the following are adequate: • New system installation • Implementation of new releases • In-house enhancements • Emergency fixes and other temporary modifications • Documentation of changes • System testing • Management or supervisory approvals.			
Program Maintenance			
Review program changes to determine compliance with procedures and the adequacy of internal control. Determine: • If the program change control procedures provide adequate guidelines to control the function. • If change standards and procedures are adhered to. • If documentation is complete. • The adequacy of involvement of users, audit, and IT management in the request and approval processes. • For emergency program fixes and other temporary changes, determine if: • Prescribed procedures are followed. • Documentation is sufficiently detailed to explain the nature of the emergency change, the immediate action taken to address the problem, and subsequent actions to permanently correct the problem			
Testing			
Determine whether procedures require that: • The scope of testing includes all functions, programs, and interface systems. • All test discrepancies are adequately documented and resolved. Users participate in the actual testing phase • All test plans and results are documented and retained			
Documentation			
Determine if: · Overall systems and program documentation adheres to standards. · Documentation is complete and current.			
Implementation			
Review documentation generated from the implementation process and determine if:			

· Controls ensure complete integrity of programs between the test and the production environments. · System level implementations are subject to the same controls as application level activity.			
Vendor Software/Support			
Obtain and review copies of all vendor and consultant contracts, available financial statements and escrow agreements. Ensure software purchase and selection procedures require: • Clear definition of user requirements • Clear definition of system requirements (equipment, interface, etc.) • Cost/benefit analysis. • Software support (in-house or vendor provided) • Financial condition of vendor. • Escrow agreements. • User documentation and training.			

Evaluation of Organizational and Management Controls

OVERALL POLICY, MANAGEMENT AND CONTROL	YES	NO	Remark
1 IT Strategy How appropriate is the audited bodyôs IT strategy? ♦ Has it been approved? ♦ Is it kept up to date? ♦ Does it cover the financial information systems? ♦ Are staff informed of the issues? ♦ Are there procedures for monitoring its implementation? *A poor or absent IT strategy could lead to the development of systems which are unsuitable for business needs. An IT strategy can help the auditor identify new systems at an early stage.*			
2 Senior Management Involvement How does senior management maintain an appropriate level of interest in the audited bodyôs IT functions? (E.g. IT steering committees.) *Management disinterest may lead to uncontrolled systems development and unauditable systems. Senior management can also provide impetus to the development and operation of other computer controls.*			

3 Documentation Policies Does the client have adequate IT documentation policies? Policies should ensure that documentation is up to date, comprehensive and available to appropriate staff. *Inadequate documentation policies increase the risk of unauthorised working practices being adopted, and may render the system difficult to maintain.*			
4 Record/Document Retention Are there appropriate policies for retaining electronic documents and computer prints? E.g. ♦ Electronic records ♦ Old Trial Balances ♦ Capacity planning *The lack of such policies could result in difficulty in obtaining audit evidence, e.g. if records are deleted or archived.*			
5 Internal Audit Involvement Does the organisationôs internal audit function carry out IT reviews of the computerised financial systems? Å What are its remit and scope? Å IT skills/training/experience *It may be possible to place reliance on the work of internal audit. They may be able to identify particular audit risks. The auditor may need to refer to the annual review of IA's work.*			
6 Personnel Policies Are policies appropriate for the IT environment? E.g. high turnover: Årecruitment screening Ådisciplinary policies *Inadequate personnel policies increase the risk of poorly trained staff making mistakes, fraud by unvetted employees and sabotage by disgruntled staff.*			

7 Computer Security Policies Is the security police adequate? Å Is it based on risk assessment? Å Has it been circulated to staff? Å Is it kept up to date? Å Does it cover the reporting of incidents and security weaknesses? Å Is there IT security training? Å Who is responsible for security? Å What compliance checking is done? *Inadequate security policies may lead to staff and management being unaware of security risks and their responsibilities.*			
8 Legal and Regulatory Issues Does the organisation have appropriate policies and procedures for ensuring that its IT facilities comply with legal and regulatory requirements? *The absence of appropriate policies increases the risks of irregular operations (i.e. failure to comply with legislation or regulations, e.g.* · *The Data Protection Act* · *Health and Safety Regulations*			
9. Market Testing/Outsourcing/Facilities Management Does the audited body receive IT services from external sources? Have appropriate procedures been developed to meet identified risks (e.g. access rights)? Are there any plans to use third party IT service providers? *The use of independent service providers, both internal and external, can increase the risks to data availability and integrity. Without appropriate controls, it may not be possible to place reliance on the data supplied by the external service suppliers*			

Evaluation of Input Controls

INPUT CONTROLS	YES	NO	Remark
1 What procedures/controls are there to ensure that data input is authorised and accurate? E.g. ♦ ÅAuthorised user lists ♦ ÅStandard input forms ♦ ÅFormat checks ♦ ÅRange checks ♦ ÅReasonableness checks ♦ ÅDependency checks ♦ ÅUse of check digits *Inadequate input controls increase the risk of erroneous or fraudulent data being input for processing.*			
2 What measures have been adopted to prevent the duplicate input of transactions? E.g. ♦ Use of unique reference numbers ♦ Physical cancellation of source documents ♦ Logical rejection of duplicate input *There should be manual and/or computer controls to reduce the risk of duplicate transaction processing*			
3 How are staff assured that all valid transactions have been input? What controls are there to ensure that all input documents have been received, i.e. completeness and accuracy checks. Å Batch totals Å Hash totals Å Sequence checks Completeness and accuracy controls reduce the risk of incomplete or missing input data.			
4 What procedures are there to deal with rejected transactions? *Inadequate procedures increase the risk of incomplete financial statements.*			
5 What actions are there taken by management to monitor data input? *Management monitoring and review reduces the risk of unauthorised data input. Management review also ensures that established input procedures are being followed.*			

6 Is data required to be converted before input? If so, what measures are taken to ensure that converted data is accurate and complete? *Data transferred from one computer system may have to be converted before it can be input into another. Inadequate conversion controls increase the risk of inaccurate or incomplete transaction data*			

Evaluation of Processing Controls

PROCESSING CONTROLS	YES	NO	Remark
1 What controls are there to ensure that all transactions have been processed? E.g. ♦ Input/output reconciliation ♦ Sequence checking ♦ Control totals *Inadequate controls over processing data increase the risk of incomplete, erroneous or fraudulent transactions being processed.*			
2 What controls are there to ensure that the correct files are processed, e.g. pay-roll runs, weekly runs, etc.? Controls can be physical or logical in nature. E.g. ♦ Disk/tape labels ♦ Use of file headers ♦ Marking of previously run files *Inadequate controls over data files increases the risk of the wrong transaction data being processed*			
3 How do the application and staff deal with processing errors? Are invalid transactions rejected and operators informed? *Inadequate controls to follow up rejected transactions increases the risk of rejected, but valid transactions being excluded from the financial statements.*			
4 What controls are there to ensure the accuracy of processing? E.g. Å Control totals Å Range/validity checks Å Use of check digits *Inadequate controls increase the risk of undetected and uncorrected processing errors*			

5 What controls are there to detect/prevent any duplicate processing? *Inadequate controls increase the risk of transactions being processed on two or more occasions*			

Evaluation of Output Controls

OUTPUT CONTROLS	YES	NO	Remark
Are there controls to ensure that computer output (printouts, cheques, invoices, purchase orders, etc.) is stored correctly and that when dispatched they reach their proper designation? *Inadequate controls increase the risk that errors in processing will not be brought to management's attention*			
Are there appropriate controls over the storage of computer stationery? E.g. Å Payable orders Å Software license *Inadequate controls increase the risk of fraudulent activity and incomplete accounting records.*			
What reasonableness, accuracy and completeness checks are carried out on output? E.g. sequential page numbering, run to run controls. *These controls are used to detect processing errors and/or unauthorised processing.*			
Are appropriate controls exercised over the production, storage and transportation of tapes and other media? *Do the controls comply with current guidance?* *Inadequate controls increase the risk of unauthorised payments.*			

Reviewing System Development

A. GENERAL				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	YES	NO	Remark
To ensure that: a. Systems are developed according to Government Rules & Regulations b. Government interest is taken care of in formulation of the contract. (* This contract should be referred to throughout the audit)	1.1 Information Strategic Plan exist. 1.2 Formation of ICT Steering Committee, ICT Technical Committee & Project Team 1.3 Ensure that all Federal Circulars pertaining to the system development are complied with 1.4 The deliverables at each phase are included in the contracts. 1.5 Transfer of Technology (TOT). Auditeeôs ICT personnel are able to maintain and measured the basic operation of the system. 1.6 Training. 1.7 Ownership. 1.8 Audit requirements: Å Unlimited Access to the system Å Audit trails Å Embedded audit module Å Security 1.9 Progress payment. 1.10 Disaster Recovery Plan.			
B. INITIATION				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**			
To ensure that: 1. Systems developed are approved and implemented if they are justifiable for economic or other sound reasons	2.1 Analysis of the project costs and benefits prepared to evaluate the economic feasibility of each alternative. Å Costs & benefit analysis Å Time & costs estimates Å Impact study Å Technological advance Å User requirements Å Risk for successful completion 2.2 The feasibility study reports are reviewed by ICT Steering Committee and that decision has been made. 2.3 Resources required to support systems after being developed.			

	2.4 The project team should have the skill and time to accomplish all designated responsibility. 2.5 The existing system should be adequately reviewed: · Existing problem vs user needs · New system to be based on the review and the feasibility study			
C. SYSTEM ANALYSIS				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	YES	NO	Remark
Systems are developed according to approved plans and procedures	3.1 Detailed statement of User Requirement Specification (URS): ♦ Description of current problem ♦ Narrative describing requirements of proposed system ♦ System acceptance criteria ♦ Involvement of all users ♦ URS must be documented and approved by ICT Steering Committee 3.2 URS is translated into Functional Requirement Specification (FRS). 3.3 The URS are translated into logical and physical design/system. 3.4 The design are properly documented. 3.5 The conceptual system design should include the following: ♦ Context Diagram ♦ Entity Relationship Diagram ♦ Data Flow Diagram ♦ Processing times and general methods of operation ♦ Interface manually and with other systems ♦ Responsibility for completeness and accuracy of data ♦ User participation in design process 3.6 Physical design should include : ♦ Physical flow ♦ Hardware configuration ♦ System flow ♦ Files and data base specification ♦ Computer programme specification			

	3.7 To determine that the detail design includes all material items regarding the systems and the operations of the organisation: ♦ File design should be consistent and all disk and tape files should be completely described and documented ♦ Sufficient audit trails should exist and access controls should be well defined ♦ Input formats & source documents are defined in detail ♦ Validation provisions and operational controls on source documents and input (e.g. batching, balancing, edit checks) ♦ Input, processing, output and operational controls should be adequate and properly documented ♦ Outputs are defined in detail, should meet user needs (in terms of content usefulness) and also meets security provisions			
D. SYSTEM DEVELOPMENT				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	YES	NO	Remark
To ensure that design and development of the system reflect the user requirements	Programming is completed according to detailed design and has been adequately tested to conform with specifications. Å Detailed systems and sub-systems specification should be developed for the systems. They should include: - an overall narrative description of the systems - the equipment configuration needed to process the systems - the systems software needed to support the systems - the interfaces with other systems - the security and privacy requirements of the systems - the operational controls over the systems - the design characteristics of the systems, including a system flowchart			

	Å Detailed programme specifications should be developed for all programmes of the systems. These specifications should include the following: - a general narrative description of the programme and its functions - the equipment required to operate the programme - the system software needed to support the programme - the storage requirements of the programme, including the amount of internal storage and the amount and type of offline storage the security and privacy requirements of the programme - the control over and within the programme lists of constants, codes and tables used, the operating procedures of the programme - the input record formats and descriptions - a description of the programmeôs logic, including flowcharts and decision tables, supplemented by narrative explanations - the output record formats and description - the logical and physical characteristics of all data bases used by the programme, including file layout and data element definitions - source programme listing - object programme listing Å Detailed specifications should be developed for databases used by the computer-based system. These specification should include the following: - the data base identification - the system using the data base - the labelling and tagging convention used when the data base is accessed - any special instruction for using it - the system software needed to support it - its logical characteristics - its physical characteristics • Systems and programmes should be			

	adequately tested by ICT personnel and should be acceptable to the users: - Detail development testing o unit testing o integration test o system test - test data prepared to test the wide range of valid and invalid transactions. - test results to be reviewed and approved by users and ICT Technical Committee (results can be compared with planned or parallel system results) complete record of problems detected during testing - sufficient resources allocated to tests - formal systems acceptance procedures - sign off by users Å System Documentation, such as users Manuals, Operational Manual are produced Å Procurement of hardware and software according to specification • Training for various users delivered			
E. IMPLEMENTATION				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	YES	NO	Remark
To ensure that: 1.The management acceptance over the systems is secured. (Only tested and approved systems are accepted and established). 2.All programmes documentations, operation manuals and user manuals are complete and ready for use.	5.1 Detailed implementation plan is prepared to ensure adequate control is maintained during the conversion from the old systems to the new systems. Å Detailed implementation plan to include phases such as, functional specifications, programming, testing parallel running, conversion, training and documentation, impact of hardware/software, site preparation and forms design Å Formal procedures for approval and acceptance by all parties (management, ICT department, users) Å Detailed conversion plan which cover systems testing, initial files creation, reconciliation, training of ICT and user personnel, time and manpower requirements, and instructions or user manuals Å Adequate back-up is available to recreate files in the event there are			

	problems encountered during conversion (unmatched totals, missing data, etc) Å Pilot testing on the system prototype Å Final acceptance test - stress test - volume test - security test Å End user training are given			
MAINTENANCE				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	YES	NO	Remark
To ensure that procedures are in place so that processing may be done smoothly and accurately. System modifications are appropriately authorised.	6.1. Cost of operation should be recorded analyses and monitored 6.2. Procedures to monitor and control system are established and record of the charges are properly kept 6.3. Disaster recovery plan should be frequently reviewed and tested			
G. POST IMPLEMENTATION REVIEW				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	YES	NO	Remark
To ensure that systems meet user requirements and achieved their objectives	7.1 The effectiveness of systems are regularly monitored and that system meets users requirement Å Interviewing users Å Reviewing output reports Å Examination of computer usage reports Å System response time Å Examine error rates on edit and file maintenance report 7.2 Aspect of project management • Time over run • Cost over run • Performance standard met			

References:

www.ISACA.org
ASOSAI Research paper, Project 6
WWW.Protiviti .com
www.knowledgeleader.com
www.theiia.org
www.sans.org
www.citehr.com
www.auditnet.org