Manual of Information Technology Audit

Volume III

Audit Programmes for Specific Applications

Office of the Comptroller & Auditor General of India

IT Audit Manual
Volume III: Audit Programmes for Specific Applications
Table of content

	Particulars	Page
1.	Audit of ERP Systems	3
	(i) Audit Programme 1 : Planning & Acquisition in Audit of ERP Systems	7
	(ii) Audit Programme 2 : Checklist for Established ERP system	32
2.	Audit Programme 3 : Computerised Inventory / Material Management Systems Audit	59
3.	Audit Programme 4 : Checklist / Guidelines for auditor's involvement in IT Systems under development	70
4.	Audit Programme 5 :Auditing E - Governance	94
5.	Audit Programme 6 : Analysing VLC Data For Audit	102
6.	Bibliography	112

1. AUDIT OF ERP SYSTEMS

Introduction

1.1 Enterprise Resource Planning (ERP) is a high-end solution featuring integration of information technology and business application. The ERP solutions seek to streamline and integrate operational processes and information flows in the organization to integrate the resources namely Personnel, Inventory, Finance and Manufacturing through information technology. A system that provides seamless integration between all of these functions into a single system, designed to serve the needs of each different department within the enterprise is called ERP. Thus in an ERP solution the whole is greater than the sum of its parts. An ERP system spans multiple departments in an organizations and in some cases an ERP will also transcend the organizational boundary to incorporate systems of partners and suppliers as well, to bring in additional functions like supply chain management. Each implementation is unique and is designed to correspond to the implementer's various business processes.

Evolution of ERP

1.2 In the ever competitive environment increasing demands are placed on organizations like aggressive cost control initiatives, need to analyze costs / revenues on a product or customer basis, flexibility to respond to changing business requirements, more informed management decision making and changes in the various ways of doing business. However, many hurdles in the growth of any business exist, such as difficulty in getting accurate data, timely information and improper interface of the complex business functions. To overcome these hurdles and achieve growth in business and depending upon the rate of change of the growing business needs, many applications, over a period of time, have been introduced by organizations such as -

- Management Information Systems (MIS)
- Integrated Information Systems (IIS)
- Executive Information Systems (EIS)
- Corporate Information Systems (CIS)
- Enterprise Wide Systems (EWS)
- Material Resource Planning (MRP)
- Manufacturing Resource Planning (MRP II)
- Money Resource Planning (MRP III)

1.3 As automated solutions were developed to cater to different activities of organizations it was only a matter of time before somebody thought of integrating all of those to give an end to end IT solution for an organization's operational and decision support needs. Thus ERP is more of a methodology than a piece of software, although it incorporates several software applications, brought together under a single, integrated interface. Most organizations across the world have

realized that in a rapidly changing environment, it is impossible to create and maintain a custom designed software package, which will cater to all their requirements, and also be completely up-to-date. Realizing the requirement of user organizations some of the leading software companies have designed Enterprise Resource Planning software which will offer an integrated software solution to all the functions of an organisation.

Features of ERP

1.4 Some of the major functionalities of ERP are as below:

- Facilitates enterprise-wide Integrated Information System covering all functional areas like Manufacturing, Sales and distribution, Payables, Receivables, Inventory, Accounts, Human resources, Purchases etc and bridges the information gap across the organisation.
- Facilitates introduction of latest technologies like Electronic Fund Transfer (EFT), Electronic Data Interchange (EDI) E-Commerce etc.
- Helps in eliminating most of the business problems like Material shortages, Productivity enhancements, Customer service, Cash Management, Inventory problems, Quality problems, Prompt delivery etc.,
- Provides avenues of continuous improvement and refinement of business processes.
- Helps in laying down Decision Support Systems (DSS), Management Information System (MIS), Reporting, Data Mining and Early Warning Systems to the organization.

Components of ERP

1.5 ERP solutions are usually divided into many sub-systems, like Sales and Marketing, Master Scheduling, Material Requirement Planning, Capacity Requirement Planning, Bill of Materials, Purchasing, manufacturing including Shop floor control, Accounts Payable/Receivable, Logistics, Asset Management and Financial Accounting

Benefits of ERP

1.6 According to the organizations to have implemented ERP some of the claimed benefits are as follows:

- Gives Accounts Payable personnel increased control on invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations.
- Reduce paper documents by providing on-line formats for quickly entering and retrieving information.
- Improves timeliness of information by permitting daily postings instead of monthly.
- Greater accuracy of information with detailed content and better presentation.

- Improved Cost Control
- Faster response and follow up on customers
- More efficient cash collection, through reduction in delay in customer payments.
- Better monitoring and quicker resolution of queries.
- Enables quick response to change in business operations and market conditions.
- Helps to achieve competitive advantage by improving business process.
- Provides a unified customer database usable by all applications.
- Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
- Improves information access and management throughout the enterprise.

Auditing ERP Systems

1.7 An ERP solution by its very nature has some peculiarities which have to be considered while planning and conducting the audit. Some of these are given below:

1.8 Implementation of an ERP solution goes closely with not only business process reengineering but also with organizational remodelling; these may be extensive in nature. Hence it is very important to evaluate whether the auditee understands the full import of going for ERP and whether it has enough organizational resilience and flexibility to undertake the project. Many ERP projects have failed not because of technical deficiencies but because of a mismatch between the management aspirations and organizational compliance.

1.9 The database is usually centralized and as the applications reside on multiple users the system allows flexibility in customization and configuration. The processing is real time online whereby the databases are updated simultaneously by minimal data entry operations. The input controls are dependent on pre data acceptance validation and rely on transaction balancing. Thus time tested controls such are batch totals etc are often no longer relevant. Since the transactions are stored in a common database the different modules update entries into the database. Thus database is accessible from different modules. Moreover the authorization controls ere enforced at the level of application and not the database. As a result the security control evaluation is of paramount importance. Accordingly the auditors have to spend considerable time understanding the data flow and transaction processing. Since the system is heavily dependent on networking on a large scale with increased access from not only users but also business associates and customer's networks and database security are important areas to look into. Vulnerability by increased access is a price that is paid for higher integration and faster processing of data in an integrated manner. Because of its very nature of having centralized database the risk of single point failures is higher in ERP solutions hence Business Continuity and Disaster Recovery should be examined closely.

1.10 The broad areas to look in the IT Audit of an ERP solution are given below:

1. The primary objective of Audit is to check whether the organization's objectives in implementing ERP have been fulfilled. Here is important that the objectives have been listed in detail and not in general terms.

2. Audit should also ensure that the organisation has followed the structured steps involved in implementation of an ERP, such as Project Planning, Business & Operational analysis including Gap analysis, Business Process Reengineering, Installation and configuration, Project team training, Business Requirement mapping, Module configuration, System interfaces, Data conversion, Custom Documentation, End-user training, Acceptance testing and Post implementation/Audit support.

3. It should be verified if the implementation was done systematically, through detailed discussions, design & customisation, implementation and production.

4. It would be advantageous if the auditor has reasonable awareness of ERP, so that he can evaluate whether system is compliant with external regulations (for e.g. the provisions of Income tax or other fiscal laws are not ignored, and the Accounting Standards are consistently followed across the company). This would enable him to achieve better quality of the audit report.

5. In a large organisation where the quantum of data processed by the ERP is extremely voluminous, the analysis of patterns and trends proves to be extremely useful in ascertaining the efficiency and effectiveness of operations.

6. The auditor can use various tools and techniques to audit an ERP environment to address entire populations, highlight potential risk areas and efficiently perform an audit. ERP not only interfaces to/from non-ERP systems, but also may serve as a web-enabled environment-where the boundaries of the processes extend beyond the ERP itself, and it becomes imperative that tools and techniques should be considered for-

    a. Data mining and analysis.

    b. Separation of duties analysis/authorisation analysis.

    c. Workflow/report delivery.

    d. Upgrades control.

1.11 An audit of an ERP thus examines area of process integrity, application security, infrastructure integrity and implementation integrity.

Planning ERP Audit

1.12 Remember that first IT Audits of an ERP system would be time consuming and would be largely an opportunity to understand the working of the system. However in cases where the audit offices are very familiar with the functioning of the auditee organizations such as in RAO/RAPs it would be comparatively easier to examine transaction processing and outputs. Otherwise at the outset of an IT audit of an ERP system or ERP system implementation project, the auditor should invest sufficient

time and effort of gathering background knowledge and understanding of the organisation's existing/planned development and gaining control of the ERP system and related sources.

1.13 The audit of ERP implementation can be carried out any time in the life cycle of the project by examining what has been done till that time and what is planned for the future. Audit of ERP solutions is not just an audit of technology but of the business process as well, hence it is important that a judicious mix of IT and auditing skills is made in an ERP audit team. Though the audit concerns may differ some of the specific concerns are: Failure to meet user requirements; Failure to integrate; Incompatibility with technical infrastructure; Vendor support problems; and Expensive and complex installations.

Audit Programme 1: Enterprise Risk Planning (ERP) – Planning & Acquisition

The focus of ERP solutions is to integrate Personnel, Inventory, Finance and Manufacturing functions through information technology. ERP implementations are critical systems and need specific focus of holistic approach and Business Process Reengineering. The Focus is on the processes of Designing and Implementation of Controls in the New System i.e. Business process Reengineering and project management.

There might be some overlap between the checklist and the Guidelines for Systems Under Development. In case an organization is clearly taking an SDLC approach towards adopting ERP application then the following programmes can be supplemented by the guidelines.

The manual presents Audit Programmes for two different kinds of audit viz.

(i) Audit/Review of the Planning and Acquisition and

(ii) Audit/Review of Established ERP System.

These programmes are based on the CoBIT framework. The IT auditors could also draw up additional auditee-specific control objectives and application-specific audit procedures for conducting IT Audit of ERP solutions.

No.	Item	Response		
		Yes	No	KD
PLANNING AND ORGANISATION				
	Strategic IT Plan			
1	Whether IT or business enterprise policies and procedures address a structured planning approach?			
	KD Reference: _____ _			
2	Whether a methodology is in place to formulate and modify the plans and at a minimum, they cover: • organisation mission and goals • IT initiatives to support the organisation mission and goals • opportunities for IT initiatives • feasibility studies of IT initiatives • risk assessments of IT initiatives			

No.	Item	Response		
		Yes	No	KD
	• optimal investment of current and future IT investments • re-engineering of IT initiatives to reflect changes in the enterprise's mission and goals evaluation of the alternative strategies for data applications, technology and organization			
	KD Reference: _____ _			
3	Whether organisational changes, technology evolution, regulatory requirements, business process re-engineering, staffing, in- and out-sourcing, etc. are taken into account and adequately addressed in the planning process?			
	KD Reference: _____ _____			
4	Whether long- and short-range IT plans exist, are current, adequately address the overall enterprise, its mission and key business functions?			
	KD Reference: _____ _			
5	Whether IT projects are supported by the appropriate documentation as identified in the IT planning methodology?			
	KD Reference: _____ _			
6	Whether checkpoints exist to ensure that IT objectives and long- and short-range plans continue to meet organisational objectives and long- and short-range plans?			
	KD Reference: _____ _			
7	Whether review and sign-off IT plan by process owners and senior management occurs?			
	KD Reference: _____ _			
8	Whether the IT plan assesses the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses?			
	KD Reference: _____ _			
9	Whether the absence of long-range planning for information systems and supporting infrastructure results in systems that do not support enterprise objectives and business processes, or do not provide appropriate integrity, security and control?			
	KD Reference: _____ _			
	Information Architecture			
10	Whether IT policies and procedures address the development and maintenance of the data dictionary?			
	KD Reference: ___ _____			

No.	Item	Response		
		Yes	No	KD
11	Whether the process used to update the information architecture model is based on long- and short-range plans, considers associated costs and risks, and ensures that senior management sign-off is obtained prior to making changes to the model?			
	KD Reference: _____			
12	Whether a process is used to keep the data dictionary and data syntax rules up to date?			
	KD Reference: _____ _			
13	Whether a medium is used to distribute the data dictionary to ensure that it is accessible to development areas and that changes are reflected immediately?			
	KD Reference: _____ _			
14	Whether IT policies and procedures address the classification of data, including security categories and data ownership, and access rules for the classes of data are clearly and appropriately defined?			
	KD Reference: _____ _			
15	Whether standards define the default classification for data assets which do not contain a data classification identifier?			
	KD Reference: _____ _			
16	Whether IT policies and procedures address the following: • authorisation process is in place requiring the owner of the data (as defined in the data ownership policy) to authorise all access to that data and to the security attributes of the data • security levels are defined for each data classification • access levels are defined and are appropriate for the data classification • access to sensitive data requires explicit access levels and data is only provided on a "need to know" basis			
	KD Reference: _____ _			
	Technology Direction			
17	Whether there is a process for creating and regularly updating the technological infrastructure plan for confirming that proposed changes are first examined to assess associated costs and risks and that senior management sign-off is obtained prior to making changes to the plan?			
	KD Reference: _____ _			
18	Whether technological infrastructure plan is compared to the IT long- and short-range plans?			
	KD Reference: _____ _			
19	Whether there is a process for evaluating the organisation's current technological status to ensure that it encompasses aspects such as systems architecture, technological direction and migration strategies?			
	KD Reference: _____ _			

No.	Item	Response		
		Yes	No	KD
20	Whether the IT policies and procedures ensure addressing the need to evaluate and monitor current and future technology trends and regulatory conditions, and that they are taken into consideration during the development and maintenance of the technological infrastructure plan?			
	KD Reference: _____ _			
21	Whether the logistical and environmental impact of technological acquisitions is planned for?			
	KD Reference: _____ _			
22	Whether the IT policies and procedures ensure that the need to systematically assess the technological plan for contingency aspects is addressed (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure)?			
	KD Reference: _____ _			
23	Whether IT management evaluates emerging technologies, and incorporates appropriate technologies into the current IT infrastructure?			
	KD Reference: _____ _			
24	Whether it is the practice for the hardware and software acquisition plans to comply with the needs identified in the technological infrastructure plan and are being properly approved?			
	KD Reference: _____ _			
25	Whether technology standards are in place for the technological components described in the technological infrastructure plan?			
	KD Reference: _____ _			
	IT Organization			
26	Whether policy statements and communications from senior management ensure the independence and authority of the IT function?			
	KD Reference: _____ _			
27	Whether membership and functions of the IT planning/steering committee have been defined and responsibilities identified?			
	KD Reference: _____ _			
28	Whether IT planning/steering committee charter aligns the committee's goals with the organisation's objectives and long- and short-range plans, and the IT objectives and long- and short-range plans?			
	KD Reference: _____ _			
29	Whether processes are in place to increase awareness, understanding and skill in identifying and resolving information management issues?			
	KD Reference: _____ _			
30	Whether policies address the need for evaluation and modification of organisational structure to meet changing objectives and circumstances?			
	KD Reference: _____ _			
31	Whether processes and performance indicators exist to determine the effectiveness and acceptance of the IT function?			

No.	Item	Response		
		Yes	No	KD
	KD Reference: _____ _			
32	Whether senior management ensures roles and responsibilities are carried out?			
	KD Reference: _____ _			
33	Whether policies exist for outlining roles and responsibilities for all personnel within the organisation with respect to information systems, internal control and security?			
	KD Reference: _____ _			
34	Whether regular campaigns exist to increase internal control and security awareness and discipline?			
	KD Reference: _____ _			
35	Whether quality assurance function and policies exist?			
	KD Reference: _____ _			
36	Whether quality assurance function has sufficient independence from system development personnel, and adequate staffing and expertise to perform its responsibilities?			
	KD Reference: _____ _			
37	Whether processes are in place within quality assurance to schedule resources and ensure completion of quality assurance testing and sign-off before systems or system changes are implemented?			
	KD Reference: _____ _			
38	Whether management has formally assigned organisation-wide responsibility for formulation of internal control and security (both logical and physical) policies and procedures to a security officer?			
	KD Reference: _____ _			
39	Whether security officer's understanding of the office's roles and responsibilities are adequately understood and demonstrated as consistent with the organisation's information security policy?			
	KD Reference: _____ _			
40	Whether organisation's security policy clearly defines responsibilities for information security that each information asset owner (e.g., users, management, and security administrators) is required to perform?			
	KD Reference: _____ _			
41	Whether policies and procedures exist, covering data and system ownership for all major data sources and systems?			
	KD Reference: _____ _			
42	Whether procedures exist to review and maintain changes in data and system ownership on a regular basis?			
	KD Reference: _____ _			
43	Whether policies and procedures exist for describing supervisory practices to ensure that roles and responsibilities are properly exercised, and all personnel have sufficient authority and resources to perform their roles and responsibilities?			
	KD Reference: _____ _			

No.	Item	Response		
		Yes	**No**	**KD**
44	Whether segregation of duties exists between the following pairs of units: • systems development and maintenance • systems development and operations • systems development/maintenance and information security • operations and data control • operations and users • operations and information security			
	KD Reference: _____ _			
45	Whether IT staffing and competence is maintained to ensure its ability to provide effective technology solutions?			
	KD Reference: _____ _			
46	Whether policies and procedures exist for the evaluation and re-evaluation of IT position (job) descriptions?			
	KD Reference: _____ _			
47	Whether appropriate roles and responsibilities exist for key processes, including system development life cycle activities (requirements, design, development, testing), information security, acquisition and capacity planning?			
	KD Reference: _____ _			
48	Whether appropriate and effective key performance indicators and/or critical success factors are used in measuring results of the IT function in achieving organisational objectives?			
	KD Reference: _____ _			
49	Whether IT policies and procedures exist to control the activities of consultants and other contract personnel, and thereby ensure the protection of the organisation's assets?			
	KD Reference: _____ _			
50	Whether procedures applicable to contracted IT services for adequacy and consistency with organisation acquisition policies?			
	KD Reference: _____ _			
51	Whether processes exist to coordinate, communicate and document interests both inside and outside the IT function directorate?			
	KD Reference: _____ _			
	IT Investment Management			
52	Whether the IT budgetary process is consistent with the organisation's process?			
	KD Reference: _____ _			
53	Whether policies and procedures are in place to ensure the preparation and appropriate approval of an annual IT operating budget which is consistent with the organisation's budget and long- and short-range plans, and the IT long- and short-range plans?			

No.	Item	Response		
		Yes	No	KD
	KD Reference: _____ _			
54	Whether the budgetary process is participatory with the management of the IT function's major units contributing in its preparation?			
	KD Reference: _____ _			
55	Whether policies and procedures are in place to regularly monitor actual costs and compare them with the projected costs, and the actual costs are based on the organisation's cost accounting system?			
	KD Reference: _____ _			
56	Whether policies and procedures are in place to guarantee that the delivery of services by the IT function is cost justified and in line with industry costs?			
	KD Reference: _____ _			
	Communicate management aims and direction			
57	Whether organisation policies and procedures create a framework and awareness programme, giving specific attention to information technology, fostering a positive control environment, and addressing such aspects as: • integrity • ethical values • code of conduct • security and internal controls • competence of personnel • management philosophy and operating style • accountability, attention and direction provided by the board of directors or its equivalent			
	KD Reference: _____ _			
58	Whether top management promotes a positive control environment by example?			
	KD Reference: _____ _			
59	Whether management has accepted full responsibility for formulating, developing, documenting, promulgating, controlling and regularly reviewing policies governing general aims and directives?			
	KD Reference: _____ _			
60	Whether formal awareness programme exists to provide ongoing communication and training related to management's positive control environment?			
	KD Reference: _____			
61	Whether organisation policies and procedures exist to ensure that appropriate and adequate resources are assigned to implement the organisation's policies in a timely manner?			
	KD Reference: _____ _			
62	Whether appropriate procedures are in place to ensure personnel understand the implemented policies and procedures, and that the policies and procedures are being followed?			

No.	Item	Response		
		Yes	**No**	**KD**
	KD Reference: _____ _			
63	Whether IT policies and procedures define, document and maintain a formal philosophy policies and objectives governing quality of systems and services produced which are consistent with the organisation's philosophy, policies and objectives?			
	KD Reference: _____ _			
64	Whether IT management ensures that the quality philosophy, policies and objectives are understood, implemented and maintained at all levels of the IT function?			
	KD Reference: _____ _			
65	Whether procedures exist which address the need to periodically review and re-approve key standards, directives, policies and procedures relating to information technology?			
	KD Reference: _____ _			
66	Whether senior management has accepted full responsibility for developing a framework for the overall approach to security and internal control?			
	KD Reference: _____ _			
67	Whether security and internal control framework document specifies the security and internal control policy, purpose and objectives, management structure, scope within the organisation, assignment of responsibilities, and definition of penalties and disciplinary actions associated with failing to complying with security and internal control policies?			
	KD Reference: _____ _			
68	Whether formal security and internal control policies identify the organisation's internal control process and includes control components such as: • control environment • risk assessment • control activities • information and communication • monitoring			
	KD Reference: _____ _			
69	Whether issue specific policies exist to document management decisions addressing particular activities, applications, systems or technologies?			
	KD Reference: _____ _			
	Human Resources Management			
70	Whether criteria are used for recruiting and selecting personnel to fill open positions?			
	KD Reference: _____ _			
71	Whether specifications of required qualifications for staff positions take into account relevant requirements of professional bodies where appropriate?			
	KD Reference: _____ _			
72	Whether management and employees are accepting of the job competency process?			

No.	Item	Response		
		Yes	No	KD
	KD Reference: _____ _			
73	Whether training programmes are consistent with the organisation's documented minimum requirements concerning education and general awareness covering security issues?			
	KD Reference: _____ _			
74	Whether management is committed to personnel training and career development?			
	KD Reference: _____ _			
75	Whether technical and management skill gaps are identified and appropriate actions are taken to address these gaps?			
	KD Reference: _____ _			
76	On-going cross-training and back-up of staff for critical job functions occurs			
	KD Reference: _____ _			
77	Whether enforcement of uninterrupted holiday policy occurs?			
	KD Reference: _____ _			
78	Whether organisation's security clearance process is adequate?			
	KD Reference: _____ _			
79	Whether employees are evaluated based on a standard set of competency profiles for the position and evaluations are held on a periodic basis?			
	KD Reference: _____ _			
80	Whether human resources management policies and procedures are in accordance with applicable laws and regulations?			
	KD Reference: _____ _			
	Compliance with External Requirements			
81	Whether job change and termination processes ensure the protection of the organisation's resources?			
	KD Reference: _____ _			
82	Whether policies and procedures are in place for: • ensuring appropriate corrective action in relation to the external requirements review is undertaken on a timely basis and procedures are in place to ensure continuous compliance • coordinating the external requirements review, to ensure that corrective actions are taken on a timely basis which guarantee compliance with external requirements • addressing appropriate safeguards, and safety and health objectives • ensuring appropriate safety and health training and education is provided to all employees • monitoring compliance with applicable safety and health laws and regulations			

No.	Item	Response		
		Yes	No	KD
	• providing adequate direction/focus on privacy in order that all legal requirements fall within its scope • informing the insurers of all material changes to the IT environment • ensuring compliance with the requirements of the insurance contracts ensuring updates are made when a new/modified insurance contract is entered into			
	KD Reference: _____ _			
83	Whether security procedures are in accordance with all legal requirements and are being adequately addressed, including: • password protection and software to limit access • authorisation procedures • terminal security measures • data encryption measures • firewall controls • virus protection • timely follow-up of violation reports			
	KD Reference: _____ _			
	Risk Assessment			
84	Whether systematic risk assessment framework is in place, incorporating the relevant information risks to the achievement of the organisation's objectives and forming a basis for determining how the risks should be managed to an acceptable level?			
	KD Reference: _____ _			
85	Whether risk assessment approach provides for regularly updated risk assessments at both the global and system specific levels?			
	KD Reference: _____ _			
86	Whether risk assessment procedures are in place to determine that identified risks include both external and internal factors, and take into consideration results of audits, inspections and identified incidents?			
	KD Reference: _____ _			
87	Organisation-wide objectives are included in the risk identification process?			
	KD Reference: _____ _			
88	Whether procedures for monitoring changes in systems processing activity determine that system risks and exposures are adjusted in a timely manner?			
	KD Reference: _____ _			
89	Whether procedures exist for ongoing monitoring and improving of the risk assessment and mitigating controls creation processes?			

No.	Item	Response		
		Yes	**No**	**KD**
	KD Reference: _____ _			
90	Whether the risk assessment documentation includes: • a description of the risk assessment methodology • the identification of significant exposures and the corresponding risks • the risks and corresponding exposures which are addressed			
	KD Reference: _____ _			
91	Whether probability, frequency and threat analysis techniques are included in the identification of risks?			
	KD Reference: _____ _			
92	Whether qualifications of risk assessment staff are adequate?			
	KD Reference: _____ _			
93	Whether formal quantitative and/or qualitative (or combined) approach exists for identifying and measuring risks, threats, and exposures?			
	KD Reference: _____ _			
94	Whether calculations and other methods are used in the measurement of risks, threats, and exposures?			
	KD Reference: _____ _			
95	Whether risk action plan is used in implementing appropriate measures to mitigate the risks, threats and exposures?			
	KD Reference: _____ _			
96	Whether acceptance of residual risk, takes into account: • organisational policy • risk identification and measurement • uncertainty incorporated in the risk assessment approach itself • cost and effectiveness of implementing safeguards and controls			
	KD Reference: _____ _			
97	Whether insurance coverage offsets the residual risk?			
	KD Reference: _____ _			
98	Whether formal quantitative and/or qualitative approaches exist to select control measures that maximize return on investment?			
	KD Reference: _____ _			
99	Whether there is a balance between the detection, prevention, correction and recovery measures used?			
	KD Reference: _____ _			
100	Whether formal procedures exist to communicate the purpose of the control measurers?			
	KD Reference: _____			

No.	Item	Response		
		Yes	No	KD
	Project Management			
101	Whether project management framework: • defines scope and boundaries for managing projects • provides for project requests to be reviewed for their consistency with the approved operational plan and projects prioritised according to this plan			
	• defines the project management methodology to be adopted and applied to each project undertaken, including: • project planning • staffing • allocation of responsibilities and authorities			
	• task breakdown • budgeting of time and resources • milestones • checkpoints • approvals • is complete and current			
	• provides for participation by the affected user department (owner/sponsor) management in the definition and authorisation of a development, implementation or modification project • specifies the basis on which staff members are assigned to projects • defines responsibilities and authorities of project team members •			
	• provides for the creation of a clear written statement defining the nature and scope of the project before work on the project begins • provides for an initial project definition document which includes a clear statement of the nature and scope of the project			

No.	Item	Response		
		Yes	No	KD
	• includes the following reasons for undertaking the project: • a statement of the problem to be remedied or process to be improved • a statement of the need for the project expressed in terms of enhancing the organisation's ability to achieve its goals • an analysis of the deficiencies in relevant existing systems			
	• the opportunities that would be provided for increasing economy or efficiency of operation • the internal control and security need that would be satisfied by the projects • addresses the manner in which proposed project feasibility studies are to be prepared, reviewed and approved by senior management, including the:			
	• environment of the project - hardware, software, telecommunications • scope of the project - what it will include and exclude in the first and following implementations • constraints of the project - what must be retained during this project, even if short-term improvement opportunities seem apparent • benefits and costs to be realised by the project sponsor or owner/sponsor			
	• delineates the manner in which each phase of the development process (i.e., preparation of feasibility study, requirements definition, system design, etc.) is to be approved prior to proceeding to the next phase of the project (i.e., programming, system testing, transaction testing, parallel testing, etc.) • requires the development of an SPMP for each project and specifies the manner in which control will be maintained throughout the life of the project, and project timeframes (milestones) and budgets			

No.	Item	Response		
		Yes	No	KD
	• complies with either the organisation standard for SPMPs or, if none exists, an appropriate standard is used • requires the development of an SQAP for each project and ensures that this is integrated with the SPMP and formally reviewed and agreed to by all involved parties •			
	• delineates the manner in which the formal project risk management programme eliminates or minimises the risks associated with the project • provides for the development of a test plan for every development, implementation and modification project • provides for the development of an adequate plan for training the owner/sponsor staff and IT staff for every development, implementation and modification project			
	KD Reference: _____			
102	Whether budgeted versus actual project milestones and costs are monitored and reported to senior management throughout every major project phase (i.e., software purchase, hardware purchase, contract programming, network upgrades, etc.)?			
	KD Reference: _____			
103	Whether project milestones and costs in excess of budgeted timeframes and amounts are required to be approved by appropriate organisation management?			
	KD Reference: _____			
104	Whether SQAP complies with either the organisation standard for SQAPs or if none exists, the criteria selected above?			
	KD Reference: _____			
105	Whether SQAP assurance tasks support the accreditation of new or modified systems and assure that internal controls and security features meet requirements?			
	KD Reference: _____			
106	Whether all project owners/sponsors had input into both the SPMP and SQAP and all agreed to final deliverables?			
	KD Reference: _____			
107	Whether Post-implementation process is an integral part of the project management framework to ensure that new or modified information systems have delivered the planned benefits?			

No.	Item	Response		
		Yes	No	KD
	KD Reference: _____			
	Quality Management			
108	Whether quality plan is: • based on the organisation's long- and short-range plans • promoting the continuous improvement philosophy and answers the basic questions of what, who and how • complete and current			
	KD Reference: _____			
109	Whether IT quality plan is: • based on the organisation's overall quality plan and the IT long- and short-range plans • promoting the continuous improvement philosophy and answers the basic questions of what, who and how • complete and current • Standard approach to quality assurance exists, and that the approach is: • applicable to both general and project-specific quality assurance activities • scaleable and thus applicable to all projects • understood by all individuals involved in a project and quality assurance activities • applied throughout all phases of a project			
	KD Reference: _____			
110	Whether standard approach to quality assurance prescribes the types of quality assurance activities (and specific reviews, audits, inspections, etc.) to be performed to achieve the objectives of the overall quality plan?			
	KD Reference: _____			
111	Whether quality assurance planning prescribes the scope and timing of quality assurance activities?			
	KD Reference: _____			
112	Whether quality assurance reviews evaluate general adherence to the IT standards, policies and procedures?			
	KD Reference: _____			
113	Whether senior management has defined and implemented IT standards, policies and procedures, including a formal system development life cycle methodology purchased, developed in-house or combination of the two?			
	KD Reference: _____ _			

No.	Item	Response		
		Yes	No	KD
114	Whether system development life cycle methodology: • governs the process of developing, acquiring, implementing and maintaining computerised information systems and related technology • supports and encourages development/modification efforts that comply with the organisation's and IT long- and short-range plans • requires a structured development or modification			
	• process with contains checkpoints at key decision points and requires authorisation to proceed with the project at each checkpoint • is complete and current • is capable of being tailored/scaled to accommodate all types of development that is occurring within the organisation • is applicable for both in-house and purchased software creation and maintenance • has documented provisions for technological change • has built in a general framework regarding the acquisition and maintenance of the technology infrastructure • has steps to be followed (such as acquiring; programming, documenting and testing; parameter setting; maintaining and applying fixes) should be governed by, and in line with, the acquisition and maintenance framework for the technology infrastructure			
	• calls for provisions outlining third-party implementer acceptance criteria, handling of changes, problem handling, participant roles, facilities, tools and software standards and procedures • requires the maintenance of detailed programme and system documentation (i.e., flow-charts, data flow diagrams, written programme narratives, etc.) and these requirements have been communicated to all concerned staff • requires that documentation be kept current as changes occur			

No.	Item	Response		
		Yes	No	KD
	• requires the application of rigorous and robust programme/system testing • defines circumstances under which parallel or pilot testing of a new or modified system will be conducted			
	• requires, as part of every system development, implementation or modification project that tests are independently verified, documented and retained • requires authorisation for undertaking projects • requires cost benefit analysis for developing new systems and modifying existing systems			
	KD Reference: _____ _			
115	Whether organisation's quality assurance approach: • requires that a post-implementation review be performed to ensure that all new or modified systems are developed and put into production in compliance with and the project team adhered to the organisation's system development life cycle methodology			
	• requires a review of the extent to which new or modified systems have achieved the objectives established for them by management • results in reports, making system development and effectiveness recommendations to management (both user and IT function) as appropriate			
	• has recommendations that are periodically followed-up and reported to appropriate senior management officials • Senior IT management reviews and appropriately updates the system development life cycle methodology on a regular basis to ascertain its sufficiency for new development/modification and new technology			
	• Varying levels of control exist for various types of development and maintenance projects (for example, large projects receive more control than small ones) • Achievement of close coordination and communication throughout the entire system development life cycle occurs between customers of the IT function and system implementers			

No.	Item	Response		
		Yes	**No**	**KD**
	KD Reference: _____ _			
116	Whether appropriate involvement exists from different functions/individuals within the organisation (e.g., IT management, security officer, legal staff, quality assurance staff, auditor staff, users, etc.)?			
	KD Reference: _____ _			
117	Whether metrics exist to measure the results of activities, allowing an assessment of whether quality goals have been achieved?			
	KD reference:			
Acquisition and Implementation				
	Identification of IT Solutions			
118	Whether policies and procedures exist requiring that: • user requirements satisfied by the existing system or to be satisfied by the proposed new or modified system be clearly defined before a development, implementation or modification project is approved • the user requirements documentation be reviewed and approved in writing by the cognisant owner/sponsor prior to the development, implementation or modification project being approved			
	• the solution's functional and operational requirements be satisfied including performance, safety, reliability, compatibility, security and legislation • alternative solutions to user requirements are studied and analysed prior to choosing one software solution over another • the identification of commercial software packages that satisfy user requirements for a particular system development or modification project before a final selection decision is made • alternatives for the acquisition of software products are clearly defined in terms of off-the-shelf, developed internally, through contract, or by enhancing the existing software, or a combination of all of these			
	• a technical feasibility study of each alternative for satisfying the user requirements established for the development of a proposed new or modified system project be prepared, analysed and approved by the cognisant owner/sponsor			

No.	Item	Response		
		Yes	No	KD
	• in each proposed system development, implementation and modification project, an analysis be performed of the costs and benefits associated with each alternative being considered for satisfying the user requirements • an economic feasibility study be prepared, analysed and approved by the cognisant owner/sponsor prior to making the decision whether to develop or modify a proposed new or modified system project from a designated member of the IT function			
	• attention is paid to the enterprise data model while solutions are being identified and analysed for feasibility • in each proposed system development, implementation or modification project, an analysis is prepared and documented of the security threats, potential vulnerabilities and impacts, and the feasible security and internal control safeguards for reducing or eliminating the identified risk • the costs and benefits of security are carefully examined to guarantee that the costs of controls do not exceed the benefits • formal management sign-off of the cost/benefit study • appropriate audit trails and controls are required to be built into all proposed new or modified systems during the design phase of the project			
	• audit trails and controls provide the possibility to protect the users against discovery and misuse of their identity by other users (e.g., by offering anonymity, pseudonymity, unlinkability or unobservability), without jeopardising the systems security each proposed system development, implementation or modification project pay attention to ergonomic issues associated with the introduction of automated systems • IT management identify all potential system software programmes that will satisfy its operational requirements • products be reviewed and tested prior to their use and financial settlement			

No.	Item	Response		
		Yes	No	KD
	• software product acquisitions follow the organisation's procurement policies setting the framework for the creation of the request for proposal, the selection of the software product supplier and the negotiation of the contract • for licensed software acquired from third-party providers, the providers have appropriate procedures to validate, protect and maintain the software product's integrity rights • procurement of contract programming services be justified with a written request for services from a			
	• an acceptance plan for facilities is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria • the end products of completed contract programming services be tested and reviewed according to the related standards by the IT quality assurance group and other concerned parties before payment for the work and approval of the end product • an acceptance plan for specific technology is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria the procurement of contract programming services be justified with a written request for services designated member of the IT function			
	KD Reference: _____			
119	Whether risk analysis is performed in line with the overall risk assessment framework?			
	KD Reference: _____			
120	Whether mechanisms exist to assign or maintain security attributes to exported and imported data, and to interpret them correctly?			
	KD Reference: _____			
121	Whether management has developed and implemented a central procurement approach, describing a common set of procedures and standards to be followed in the procurement of IT hardware, software and services?			
	KD Reference: _____			
122	Whether contracts stipulate that the software, documentation and other deliverables are subject to testing and review prior to acceptance?			
	KD Reference: _____			

No.	Item	Response		
		Yes	No	KD
123	Whether testing included in contract specifications consists of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, regression testing, user acceptance testing and, finally, pilot testing of the total system to avoid any unexpected system failure?			
	KD Reference: _____			
124	Whether facilities acceptance tests are performed to guarantee that the accommodation and environment meet the requirements specified in the contract?			
	KD Reference: _____			
125	Whether specific technology acceptance tests should include inspection, functionality tests and workload trials?			
	KD Reference: _____			
	Acquisition and Maintenance of Application Software			
126	Whether policies and procedures ensure that: • the organisation's system development life cycle methodology applies to both the development of new systems and major changes to existing systems, and user participation			
	• close liaison with the user in creating the design specifications and verifying the design specifications against user requirements • in the event of major changes to existing systems, a similar system development life cycle process is observed as in the case of the development of new systems • design specifications are signed-off by management, the affected user departments and the organisation's senior management, when appropriate for all new system development and modification projects			
	• an appropriate process is being applied for defining and documenting the file format for each new system development or modification project, including a requirement that the data dictionary rules are respected • detailed written programme specifications are prepared for each information development or modification project and these programme specifications agree with the system design specifications			

No.	Item	Response		
		Yes	No	KD
	• adequate mechanisms for the collection and entry of data are specified for each new system development or modification project • adequate mechanisms for defining and documenting the input requirements for each new system development or modification project exist			
	• the development of an interface between the user and the machine exists which is easy to use and self-documenting (by means of online help functions) • adequate mechanisms for defining and documenting internal and external interfaces for each new system development or modification project exist • adequate mechanisms for defining and documenting the processing requirements for each new system development or modification project exist • adequate mechanisms for defining and documenting the output requirements for each new system development or modification project exist			
	• adequate mechanisms for ensuring internal control and security requirements are specified for each new system development or modification project • the internal control and security requirements include application controls which guarantee the accuracy, completeness, timeliness and authorisation of inputs and outputs • availability is considered in the design process of new or modified systems at the earliest possible stage, and this consideration should analyse and, if necessary, increase through maintainability and reliability improvements			
	• applications programmes contain provisions which routinely verify the tasks performed by the software and which provide in the restoration of the integrity through rollback or other means • application software is tested according to the project test plan and established testing standards before being approved by the user			

No.	Item	Response		
		Yes	No	KD
	• adequate user reference and support manuals are prepared (preferably in electronic format) as part of every system development or modification process • the system design is re-assessed whenever significant, technological and/or logical discrepancies occur during system development or maintenance			
	KD Reference: _____			
127	Whether system development life cycle methodology ensures that user reference and support materials are updated in an accurate and timely manner?			
	KD Reference: _____			
128	Whether sensitivity assessment is required by the system development life cycle methodology to be performed during the initiation of new system development or modification?			
	KD Reference: _____			
129	Whether system development life cycle methodology requires that basic security and internal control aspects of a new system to be developed or modified be assessed along with the conceptual design of the system in order to integrate security concepts in the design as early as possible?			
	KD Reference: _____			
130	Whether logical security and application security issues are required by the system development life cycle methodology to be addressed and included in the design of new systems or modifications of existing ones?			
	KD Reference: _____			
131	Whether the assessment of the security and internal control aspects is based on a sound framework?			
	KD Reference: _____			
132	Whether Artificial Intelligence systems are placed in an interaction or control framework with human operators to ensure that vital decisions are approved?			
	KD Reference: _____			
133	Whether disclosure of sensitive information used during application testing is mitigated by either strong access limitations or depersonalisation of the used historical data?			
	KD Reference: _____			
	Acquisition and Maintenance of Technology Infrastructure			

No.	Item	Response		
		Yes	No	KD
134	Whether policies and procedures exist to ensure that: • a formal evaluation plan is prepared to assess new hardware and software for any impact on the overall performance of the system • ability to access system software and thereby interrupt the operational information systems environment is limited • set-up, installation and maintenance of system software does not jeopardise the security of the data and programmes being stored on the system			
	• system software parameters are selected in order to ensure the integrity of the data and programmes being stored on the system • system software is installed and maintained in accordance with the acquisition and maintenance framework for the technology infrastructure • system software vendors provide integrity assurance statements with their software and all modifications to their software • the thorough testing (i.e., using a system development life cycle methodology) of system software is occurring before it is introduced into the production environment • vendor provided system software installation passwords are changed at the time of installation and system software changes are controlled in line with the organisation's change management procedures			
	KD Reference: _____			
135	Whether policies and procedures exist for the preventive maintenance of hardware (both operated by the IT function and affected user functions) to reduce the frequency and impact of performance failures?			
	KD Reference: _____			
136	Whether vendor prescribed preventative maintenance steps and frequency for each hardware device operated by the IT function and the affected user functions are adhered to?			
	KD Reference: _____			
137	Whether policies and techniques exist for using and monitoring the use of system utilities?			
	KD Reference: _____			
138	Whether responsibilities for using sensitive software utilities are clearly defined, understood by programmers, and use of the utilities is monitored and logged?			

No.	Item	Response		
		Yes	No	KD
	KD Reference: _____			
	Development and Maintenance of Procedures			
139	Whether operational requirements are determined with historical performance statistics available and user input regarding increases/decreases expected?			
	KD Reference: _____			
140	Whether service level and performance expectations are at sufficient detail to allow tracking, reporting and improvement opportunities?			
	KD Reference: _____			
141	Whether operational requirements and service levels are determined using historical performance, user adjustments, and industry benchmarks?			
	KD Reference: _____			
142	Whether service levels and processing requirements are an integral step in planning for new systems?			
	KD Reference: _____			
143	Whether user procedures manuals, operations manual and training materials are developed as part of every information system development, implementation or modification project, and are kept up-to-date?			
	KD Reference: _____			

Audit Programme 2 : Checklist for Established ERP system

Focus, apart from the area mentioned in Planning and Organization and Acquisition and implementation, is on evaluation of General and application controls implementation in the complex IT environment.

No.	Item	Response		
		Yes	**No**	**KD**
PLANNING AND ORGANISATION				
	Define the IT organization and relationships			
Refer Items No. 26 to 51 of IT Organization of (i) Audit/Review checklist for ERP Planning and Acquisition				
	KD Reference: _____			
	Manage the IT investment			
Refer to items No. 52 to 56 of IT Investment Management of (i) Audit/Review checklist for ERP Planning and Acquisition				
	Manage human resources			
Refer to items No. 70 to 80 of Human Resources Management of (i) Audit/Review checklist for ERP Planning and Acquisition.				
	KD Reference: _____			
	Ensure compliance with external requirements			
Refer to Items No. 81 to 83 of Compliance with External Requirements of (i) Audit/Review checklist for ERP Planning and Acquisition				
	KD Reference: _____			
	Assess risk			
Refer to Items No. 84 to 100 of Compliance with External Requirements of (i) Audit/Review checklist for ERP Planning and Acquisition.				
	KD Reference: _____			
	Manage quality			
Refer to Items No. 108 to 117 of Quality Management of (i) Audit/Review checklist for ERP Planning and Acquisition				
ACQUISITION AND IMPLEMENTATION				
	Acquire and maintain application software			
Refer to Items No. 126 to 133 of Acquisition and Maintenance of Application Software of (i) Audit/Review checklist for ERP Planning and Acquisition.				
	KD Reference: _____			
	Acquire and maintain technology architecture			
Refer to Items No.134 to 138 of Acquisition and Maintenance of technology Infrastructure of(i) Audit/Review checklist for ERP Planning and Acquisition				
	KD Reference: _____ _			

No.	Item	Response		
		Yes	**No**	**KD**
	Develop and maintain IT procedures			
Refer items No. 139 to 143 of Development and Maintenance of Procedures of (i) Audit/Review checklist for ERP Planning and Acquisition				
	Manage changes			
1	Whether methodology for prioritising system change requests from users exists and is in use?			
	KD Reference: _____			
2	Whether emergency change procedures are addressed in operation manuals?			
	KD Reference: _____			
3	Whether change control is a formal procedure for both user and development groups?			
	KD Reference: _____			
4	Whether change control log ensures all changes shown were resolved?			
	KD Reference: _____			
5	Whether user is satisfied with turnaround of change requests - timeliness and cost?			
	KD Reference: _____			
6	Whether for a selection of changes on the change control log: • that change resulted in programme and operations documentation change • that changes were made as documented • current documentation reflects changed environment			
	KD Reference: _____			
7	Whether change process is being monitored for improvements in acknowledgment, response-time, response-effectiveness and user satisfaction with the process?			
	KD Reference: _____			
8	Whether maintenance to Private Branch Exchange (PBX) system is included in the change control procedures?			
	KD Reference: _____			
DELIVERY AND SUPPORT				
	Define service levels			
9	Whether a service level agreement process is identified by policy?			
	KD Reference: _____			
10	Whether user participation in process is required for creation and modification of agreements?			
	KD Reference: _____			

No.	Item	Response		
		Yes	No	KD
11	Whether responsibilities of users and providers are defined?			
	KD Reference: _____			
12	Whether management monitors and reports on the achievement of the specified service performance criteria and all problems encountered?			
	KD Reference: _____			
13	Whether regular review process by management exists?			
	KD Reference: _____			
14	Whether recourse process is identified for non-performance?			
	KD Reference: _____			
15	Whether service level agreements include, but are not limited to having: • definition of service • cost of service • quantifiable minimum service level • level of support from the IT function • availability, reliability, capacity for growth • continuity planning • security requirements • change procedure for any portion of the agreement • written and formally approved agreement between provider and user of service • effective period and new period review/renewal/non-renewal • content and frequency of performance reporting and payment for services • charges are realistic compared to history, industry, best practices • calculation for charges • service improvement commitment			
	KD Reference: _____			
	Manage third party services			
16	Whether IT policies and procedures relating to third-party relationships exist and are consistent with organisational general policies?			
	KD Reference: _____			
17	Whether policies exist specifically for addressing need for contracts, definition of content of contracts, owner or relationship manager responsible for ensuring contracts are created, maintained, monitored and renegotiated as required?			
	KD Reference: _____			

No.	Item	Response		
		Yes	No	KD
18	Whether interfaces are defined to independent agents involved in the conduct of the project and any other parties, such as subcontractors?			
	KD Reference: _____			
19	Whether contracts represent a full and complete record of third-party supplier relationships?			
	KD Reference: _____			
20	Whether contracts are established for continuity of services specifically, and that these contracts include contingency planning by vendor to ensure continuous service to user of services?			
	KD Reference: _____			
21	Whether contract contents include at least the following: • formal management and legal approval • legal entity providing services • services provided • service level agreements both qualitative and quantitative • cost of services and frequency of payment for services • resolution of problem process • penalties for non-performance • dissolution process • modification process • reporting of service - content, frequency, and distribution • roles between contracting parties during life of contract • continuity assurances that services will be provided by vendor • user of services and provider communications process and frequency • duration of contract • level of access provided to vendor • security requirements			
	• non-disclosure guarantees • right to access and right to audit			
	KD Reference: _____			
22	Whether escrow agreements have been negotiated where appropriate?			
	KD Reference: _____			
23	Whether potential third-parties are properly qualified through an assessment of their capability to deliver the required service (due diligence)?			

No.	Item	Response		
		Yes	No	KD
	KD Reference: _____			
	Manage performance and capacity			
24	Whether time frames and level of service are defined for all services provided by the IT function?			
	KD Reference: _____			
25	Whether time frames and service levels reflect user requirements?			
	KD Reference: _____			
26	Whether time frames and service levels are consistent with performance expectations of the equipment potentials?			
	KD Reference: _____			
27	Whether an availability plan exists, is current and reflects user requirements?			
	KD Reference: _____			
28	Whether ongoing performance monitoring of all equipment and capacity is occurring, reported upon, lack of performance addressed by management and performance improvement opportunities are formally addressed?			
	KD Reference: _____			
29	Whether optimal configuration performance is being monitored by modeling tools to maximize performance while minimizing capacity to required levels?			
	KD Reference: _____			
30	Whether both users and operational performance groups are pro-actively reviewing capacity and performance and workload schedule modifications are occurring?			
	KD Reference: _____			
31	Whether workload forecasting includes input from users on changing demands and from suppliers on new technology or current product enhancements?			
	KD Reference: _____			
	Ensure continuous services			
32	Whether organisational policies require a continuity framework and plan to be part of normal operational requirements for both the IT function and all organisations dependent on IT resources?			
33	KD Reference: _____			
34	Whether IT policies and procedures require: • a consistent philosophy and framework relating to development of continuity plan development • a prioritisation of applications with respect to timeliness of recovery and return •			

No.	Item	Response		
		Yes	No	KD
	• risk assessment and insurance consideration for loss of business in continuity situations for the IT function as well as users of resources • outline specific roles and responsibilities with respect to continuity planning with specific test, maintenance and update requirements • formal contract arrangements with vendors to provide services in event of need to recover, including back-up site facility or relationship, in advance of actual need • in each continuity plan minimum content to include:			
	➢ Emergency procedures to ensure the safety of all affected staff members ➢ Roles and responsibilities of the IT function, vendors providing recovery services, users of services and support administrative personnel ➢ A recovery framework consistent with long-range plan for continuity ➢ Listing of systems resources requiring alternatives (hardware, peripherals, software) ➢ Listing of highest to lowest priority applications, required recovery times and expected performance norms ➢ Administrative functions for communicating and providing support services such as benefits, payroll, external communications, cost tracking, etc., in event of need to recover ➢ Various recovery scenarios from minor to loss of total capability and response to each in sufficient detail for step-by-step execution			
	➢ Specific equipment and supply needs are identified such as high speed printers, signatures, forms, communications equipment, telephones, etc., and a source and alternative source defined ➢ Training and awareness of individual and group roles in continuity plan ➢ Testing schedule, results of last test and corrective actions taken based on prior test(s			

No.	Item	Response		
		Yes	**No**	**KD**
	➢ Itemisation of contracted service providers, services and response expectations ➢ Logistical information on location of key resources, including back-up site for recovery operating system, applications, data files, operating manuals and programme/system/user documentation ➢ Current names, addresses, telephone/pager numbers of key personnel ➢ Reconstruction plans are included for re-recovery at original location of all systems resources ➢ Business resumption alternatives for all users for establishing alternative work locations once ➢ IT resources are available; i.e., system recovered at alternative site but user building burned to the ground and unavailable			
	KD Reference: _____			
35	Whether regulatory agency requirements with respect to continuity planning are met?			
	KD Reference: _____			
36	Whether user continuity plans are developed based on unavailability of physical resources for performing critical processing - manual and computerised?			
	KD Reference: _____			
37	Whether the telephone system, VoiceMail, fax and image systems are part of the continuity plan?			
	KD Reference: _____			
38	Whether image systems, fax systems, paper documents as well as microfilm and mass storage media are part of the continuity plan?			
	KD Reference: _____			
	Ensure system security			
39	Whether strategic security plan is in place providing centralised direction and control over information system security, along with user security requirements for consistency?			
	KD Reference: _____			
40	Whether centralised security organisation is in place responsible for ensuring only appropriate access to system resources?			
	KD Reference: _____			
No.	**Item**	**Response**		
		Yes	**No**	**KD**

41	Whether data classification schema is in place and being used, that all system resources have an owner responsible for security and content?			
	KD Reference: _____			
42	Whether user security profiles are in place representing "least access as required" and profiles are regularly reviewed by management for re-accreditation?			
	KD Reference: _____			
43	Whether employee indoctrination includes security awareness, ownership responsibility and virus protection requirements?			
	KD Reference: _____			
44	Whether reporting exists for security breaches and formal problem resolution procedures are in place, and these reports include: • unauthorised attempts to access system (sign on) • unauthorised attempts to access system resources • unauthorised attempts to view or change security definitions and rules • resource access privileges by user ID • authorised security definitions and rule changes • authorised access to resources (selected by user or resource) • status change of the system security • accesses to operating system security parameter tables			
	KD Reference: _____			
45	Whether cryptographic modules and key maintenance procedures exist, are administered centrally and are used for all external access and transmission activity?			
	KD Reference: _____			
46	Whether cryptographic key management standards exist for both centralised and user activity?			
	KD Reference: _____			
47	Whether change control over security software is formal and consistent with normal standards of system development and maintenance?			
	KD Reference: _____			
48	Whether the authentication mechanisms in use provide one or more of the following features: • single-use of authentication data (e.g., passwords are never re-usable) • multiple authentication (i.e., two or more different authentication mechanisms are used)			

No.	Item	Response		
		Yes	No	KD
	• policy-based authentication (i.e., ability to specify separate authentication procedures for specific events) • on-demand authentication (i.e., ability to re-authenticate the user at times after the initial authentication)			
	KD Reference: _____			
49	Whether the number of concurrent sessions belonging to the same user is limited?			
	KD Reference: _____			
50	Whether at log-on, an advisory warning message to users regarding the appropriate use the hardware, software or connection logged on?			
	KD Reference: _____			
51	Whether a warning screen is displayed prior to completing log-on to inform reader that unauthorised access may result in prosecution?			
	KD Reference: _____			
52	Whether upon successful session establishment, a history of successful and unsuccessful attempts to access the user's account is displayed to the user?			
	KD Reference: _____			
53	Whether password policy includes: • initial password change on first use enforced • an appropriate minimum password length • an appropriate and enforced frequency of password changes • password checking against list of not allowed values (e.g., dictionary checking) • adequate protection of emergency passwords			
	KD Reference: _____			
54	Whether formal problem resolution procedures include: • User ID is suspended after 5 repeated unsuccessful log-on attempts • Date, time of last access and number of unsuccessful attempts is displayed to authorised user at log-on • Authentication time is limited to 5 minutes, after which the session is terminated • User is informed of suspension, but not the reason for it			
	KD Reference: _____			

No.	Item	Response		
		Yes	No	KD
55	Whether dial in procedures include dial-back or token based authentication, frequent changes of dial-up numbers, software and hardware firewalls to restrict access to assets and frequent changes of passwords and deactivation of former employees' passwords?			
	KD Reference: _____			
56	Whether location control methods are used to apply additional restrictions at specific locations?			
	KD Reference: _____			
57	Whether access to the VoiceMail service and the PBX system are controlled with the same physical and logical controls as for computer systems?			
	KD Reference: _____			
58	Enforcement of sensitive position policies occurs, including: • employees in sensitive job positions are required to be away from the organisation for an appropriate period of time every calendar year; during this time their user ID is suspended; and persons replacing the employee are instructed to notify management if any security-related abnormalities are noted • unannounced rotation of personnel involved in sensitive activities is performed from time to time			
	KD Reference: _____			
59	Whether security-related hardware and software, such as cryptographic modules, are protected against tampering or disclosure, and access is limited to a "need to know" basis?			
	KD Reference: _____			
60	Whether access to security data such as security management, sensitive transaction data, passwords and cryptographic keys is limited to a need to know basis?			
	KD Reference: _____			
61	Whether trusted paths are used to transmit non-encrypted sensitive information?			
	KD Reference: _____			
62	Whether to prevent denial of service due to an attack with junk faxes, protective measures are taken such as: • limiting the disclosure of fax numbers outside the organisation to a "need-to-know" basis • fax lines used for solicitation of business are not used for other purposes			
	KD Reference: _____			

No.	Item	Response		
		Yes	**No**	**KD**
63	Whether preventative and detective control measures have been established by management with respect to computer viruses?			
	KD Reference: _____			
64	Whether to enforce integrity of electronic value, measures are taken such as: • card reader facilities are protected against destruction, disclosure or modification of the card information • card information (PIN and other information) is protected against insider disclosure • counterfeiting of cards is prevented			
	KD Reference: _____			
65	Whether to enforce protection of security features, measures are taken such as: • the identification and authentication process is required to be repeated after a specified period of inactivity • a one-button lock-up system, a force button or a shut-off sequence can be activated when the terminal is left alone			
	KD Reference: _____ _			
	Identify and allocate costs			
66	Whether IT function has a group responsible for reporting and issuing chargeback bills to users Procedures are in place that: • develop a yearly development and maintenance plan with user identification of priorities for development, maintenance and operational expenses • allow for a very high level of user determination of where IT resources are spent • generate a yearly IT budget including: ➢ Compliance to organisational requirements in budget preparation ➢ Consistency with what costs are to be allocated by the user departments ➢ Communication of historical costs, assumptions for new costs- for understanding by users of what costs are included in chargeback			

No.	Item	Response		
		Yes	No	KD
	➢ User sign-off on all budget costs to be allocated by IT function ➢ Frequency of reporting and actual charging of costs to users • track allocated costs of all IT resources of, but not limited to: ➢ Operational hardware ➢ Peripheral equipment ➢ Telecommunications usage ➢ Applications development and support ➢ Administrative overhead ➢ External vendor service costs ➢ Help desk ➢ Facilities and maintenance ➢ Direct/indirect costs ➢ Fixed and variable expenses Sunk and discretionary costs			
	• for regular reporting to users on performance for the various cost categories • report to users on external benchmarks regarding cost effectiveness so as to allow comparison to industry expectations, or user alternative sourcing for services • for timely modification to cost allocations to reflect changing business needs formally approve and accept charges as received			
	• identify IT improvement opportunities to reduce chargebacks or get greater value for chargebacks			
	KD Reference: _____ _			
67	Whether reports provide assurance that chargeable items are identifiable, measurable and predictable?			
	KD Reference: _____ _			
68	Whether reports capture and highlight changes in the underlying cost components or allocation algorithm?			
	KD Reference: _____ _			
	Educate and train users			
69	Whether policies and procedures relating to ongoing security and controls awareness exist?			
	KD Reference: _____ _			
70	Whether there is an education/training programme focusing on information systems security and control principles?			
	KD Reference: _____ _			
71	Whether new employees are made aware of security and control responsibility with respect to using and having custody of IT resources?			
	KD Reference: _____ _			

No.	Item	Response		
		Yes	No	KD
72	Whether there are policies and procedures in effect relating to training and they are current with respect to technical configuration of IT resources?			
	KD Reference: _____ _			
73	Whether availability of in-house training opportunities and frequency of employee attendance?			
	KD Reference: _____ _			
74	Whether availability of external technical training opportunities and frequency of employee attendance?			
	KD Reference: _____ _			
75	Whether a training function is assessing training needs of personnel with respect to security and controls, and translating those needs into in-house or external training opportunities?			
	KD Reference: _____ _			
76	Whether all employees are required to attend security and control awareness training on an ongoing basis that would include, but not be limited to: • general system security principles • ethical conduct related to IT • security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner • responsibilities associated with custody and use of IT resources • security of information and information systems when used off-site			
	KD Reference: _____ _			
77	Whether security awareness training includes a policy on preventing the disclosure of sensitive information through conversations (e.g., by announcing the status of the information to all persons taking part in the conversation)?			
	KD Reference: _____ _			
	Assist and advise customers			
78	Whether nature of help desk function (i.e., how requests for assistance are processed and assistance is provided) is effective?			
	KD Reference: _____ _			
79	Whether actual facilities, divisions or departments are performing the help desk function and the individuals or positions responsible for the help desk?			
	KD Reference: _____ _			
80	Whether level of documentation for help desk activities is adequate and current?			
	KD Reference: _____			
81	Whether actual process for logging or registering requests for service and use of logs exists?			
	KD Reference: _____			

No.	Item	Response		
		Yes	No	KD
82	Whether process for query escalation and management intervention for resolution is sufficient?			
	KD Reference: _____			
83	Whether time frame for clearing queries received is adequate?			
	KD Reference: _____			
84	Whether procedures for tracking trends and reporting on help desk activities exist?			
	KD Reference: _____			
85	Whether performance improvement initiatives are formally identified and executed?			
	KD Reference: _____			
86	Whether service level agreements and performance standards are being met?			
	KD Reference: _____			
87	Whether user satisfaction level is periodically determined and reported?			
	KD Reference: _____			
	Manage the configuration			
88	Whether process for creating and controlling configuration baselines (the cut-off point in the design and development of a configuration item beyond which evolution does not occur without undergoing strict configuration control) is appropriate?			
	KD Reference: _____			
89	Whether functions for maintaining configuration baseline exist?			
	KD Reference: _____			
90	Whether process for controlling status accounting of purchased and leased resources - including inputs, outputs and integration with other processes - exists?			
	KD Reference: _____			
91	Whether configuration control procedures include: • configuration baseline integrity • programmed access authorisation controls over the change management system • the recovery of configuration items and change requests at any point in time • completion of configuration and reports assessing the adequacy of configuration recording procedures •			

No.	Item	Response		
		Yes	No	KD
	• periodic evaluations of the configuration recording function • individuals responsible for reviewing configuration control have the requisite knowledge, skills and abilities • procedures exist for reviewing access to software baselines • results of reviews are provided to management for corrective action			
	KD Reference: _____ _			
92	Whether periodic review of configuration with inventory and accounting records is performed on a regular basis?			
	KD Reference: _____ _			
93	Whether configuration baseline has sufficient history for tracking changes?			
	KD Reference: _____ _			
94	Whether software change control procedures exist for: • establishing and maintaining licensed application programme library • ensuring licensed application programme library is adequately controlled • ensuring the reliability and integrity of the software inventory • ensuring the reliability and integrity of the inventory of authorised software used and checking for unauthorised software • assigning responsibility for unauthorised software control to a specific staff member • recording use of unauthorised software and reporting to management for corrective action • determining whether management took corrective action on violations			
	KD Reference: _____ _			
95	Whether process for migrating developmental applications into the testing environment and ultimately into production status interacts with configuration reporting?			
	KD Reference: _____ _			
96	Whether the software storage process includes: • defining a secure file storage area (library) for all valid software in appropriate phases of the system development life cycle • requiring that software storage libraries are separated from each other and from development, testing and production file storage areas			

No.	Item	Response		
		Yes	No	KD
	• requiring existence within source libraries that allow temporary location of source modules moving into production cycle period • requiring that each member of all libraries has an assigned owner • defining logical and physical access controls • establishing software accountability • establishing an audit trail • detecting, documenting and reporting to management all instances of non-compliance with this procedure determining whether management took corrective action			
	KD Reference: _____			
97	Whether coordination is occurring among applications development, quality assurance and operations with respect to updating configuration baseline upon change?			
	KD Reference: _____			
98	Whether software is labeled and periodically inventoried?			
	KD Reference: _____			
99	Whether library management software is used to: • produce audit trails of program changes • maintain program version numbers • record and report program changes • maintain creation/date information for production modules • maintain copies of previous versions • control concurrent updates			
	KD Reference: _____			
	Manage problems and incidents			
100	Whether there is a problem management process that ensures all operational events which are not part of standard operations are recorded, analysed and resolved in a timely manner, and incident reports are generated for significant problems?			
	KD Reference:			
101	Whether problem management procedures exist for: • defining and implementing a problem management system • recording, analysing, resolving in a timely manner all non-standard events			
	• establishing incident reports for critical events and reporting to users • identifying problem types and prioritisation methodology allowing for varying resolution efforts based on risk			

No.	Item	Response		
		Yes	No	KD
	• defining logical and physical control of problem management information distributing outputs on a "need to know" basis • tracking of problem trends to maximise resources, reduce turnaround • collecting accurate, current, consistent and usable data inputs to reporting			
	• notifying appropriate level of management for escalation and awareness • determining if management periodically evaluates the problem management process for increased effectiveness and efficiency • sufficiency of audit trail for system problems • integration with change, availability, configuration management systems and personnel			
	KD Reference: _____			
102	Whether emergency processing priorities exist, are documented and require approval by appropriate program and IT management?			
	KD Reference: _____			
103	Whether there are emergency and temporary access authorisation procedures which require: • documentation of access on standard forms and maintained on file • approval by appropriate managers • secure communication to the security function • automatic access termination, after a predetermined period of time			
	KD Reference: _____ _			
	Manage data			
104	For data preparation: • data preparation procedures ensure completeness, accuracy and validity • authorisation procedures for all source documents exist • separation of duties between origination, approval and conversion of source documents into data is occurring			
	• authorised data remains complete, accurate and valid through source document origination • data is transmitted in a timely manner • periodic review of source documents for proper completion and approvals occurs			

No.	Item	Response		
		Yes	No	KD
	• appropriate handling of erroneous source documents • adequate control over sensitive information exists on source documents for protection from compromise • procedures ensure completeness and accuracy of source documents, proper accounting for source documents and timely conversion • source document retention is sufficiently long to allow reconstruction in event of loss, availability for review and audit, litigation inquiries or regulatory requirements			
	KD Reference: _____ _			
105	For data input: • appropriate source document routing for approval prior to entry • proper separation of duties among submission, approval, authorisation and data entry functions • unique terminal or station codes and secure operator identification • usage, maintenance and control of station codes and operator IDs • audit trail to identify source of input • routine verification or edit checks of inputted data as close to the point of origination as possible • appropriate handling of erroneously input data • clearly assign responsibility for enforcing proper authorisation over data			
	KD Reference: _____ _			
106	For data processing: Whether programmes contain error prevention, detection, correction routines: • programmes must test input for errors (i.e., validation and editing) • programmes must validate all transactions against a master list of same • programmes must disallow override of error conditions			
	KD Reference: _____			
107	Whether error handling procedures include: • correction and resubmission of errors must be approved • individual responsibility for suspense files is defined			

No.	Item	Response		
		Yes	No	KD
	• suspense files generate reports for non-resolved errors suspense file prioritisation scheme is available based on age and type			
	KD Reference: _____			
108	Whether logs of programmes executed and transactions processed/rejected for audit trail exist?			
	KD Reference: _____			
109	Whether a control group for monitoring entry activity and investigating non-standard events, along with balancing of record counts and control totals for all data processed?			
	KD Reference: _____			
110	Whether that all fields are edited appropriately, even if one field has an error?			
	KD Reference: _____			
111	Whether tables used in validation are reviewed on a frequent basis?			
	KD Reference: _____			
112	Whether written procedures exist for correcting and resubmitting data in error including a non-disruptive solution to reprocessing?			
	KD Reference: _____			
113	Whether resubmitted transactions are processed exactly as originally processed?			
	KD Reference: _____			
114	Whether responsibility for error correction resides with original submitting function?			
	KD Reference: _____			
115	Whether Artificial Intelligence systems are placed in an interactive control framework with human operators to ensure that vital decisions are approved?			
	KD Reference: _____			
116	For output, interfacing, and distribution: • Access to output is restricted physically and logically to authorised people • Ongoing review of need for outputs is occurring • Output is routinely balanced to relevant control totals •			

No.	Item	Response		
		Yes	No	KD
	• Audit trails exist to facilitate the tracing of transaction processing and the reconciliation of disrupted data • Output report accuracy is reviewed and errors contained in output is controlled by cognisant personnel • Clear definition of security issues during output, interfacing and distribution exist • Communication of security breaches during any phase is communicated to management, acted upon and reflected in new procedures as appropriate • Process and responsibility of output disposal is clearly defined • Destruction is witnessed of materials used but not needed after processing • All input and output media is stored in off-site location in event of later need • Information marked as deleted is changed in such a way that it can no longer be retrieved			
	KD Reference: _____ _			
117	For media library: • Contents of media library are systematically inventoried • Discrepancies disclosed by the inventory are remedied in a timely manner • Measures are taken to maintain the integrity of magnetic media stored in the library			
	• Housekeeping procedures exist to protect media library contents • Responsibilities for media library management have been assigned to specific members of IT staff • Media back-ups and restoration strategy exists • Media back-ups are taken in accordance with the defined back-up strategy and usability of back-ups is regularly verified			
	• Media back-ups are securely stored and storage sites periodically reviewed regarding physical access security and security of data files and other items			

No.	Item	Response		
		Yes	No	KD
	• Retention periods and storage terms are defined for documents, data, programmes, reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication			
	• In addition to the storage of paper source documents, telephone conversations are recorded and retained - if not in conflict with local privacy laws - for transactions or other activities that are part of the business activities traditionally conducted over telephones • Adequate procedures are in place regarding the archival of information (data and programmes) in line with legal and business requirements and enforcing accountability and reproducibility			
	KD Reference: _____ _			
118	For information authentication and integrity: • The integrity of the data files is checked periodically • Requests received from outside the organisation, via telephone or VoiceMail, are verified by call-back or other means of authentication			
	• A prearranged method is used for independent verification of the authenticity of source and contents of transaction requests received via fax or image system • Electronic signature or certification is used to verify the integrity and authenticity of incoming electronic documents			
	KD Reference: _____			
	Manage facilities			
119	Whether facility location is not obvious externally, is in least accessible area or organisation and access is limited to least number of people?			
	KD Reference: _____			
120	Whether logical and physical access procedures are sufficient, including security access profiles for employees, vendors, equipment and facility maintenance staff?			
	KD Reference: _____			
121	Whether "Key" and "including ongoing card reader" management procedures and practices are adequate, update and review on a least-access-needed basis?			

No.	Item	Response		
		Yes	No	KD
	KD Reference: _____ _			
122	Whether access and authorisation policies on entering/leaving, escort, registration, temporary required passes, surveillance cameras as appropriate to all and especially sensitive areas are adequate?			
	KD Reference: _____			
123	Whether periodic and ongoing review of access profiles, including managerial review is occurring?			
	KD Reference: _____			
124	Whether revocation, response and escalation process occurs in event of security breach?			
	KD Reference: _____			
125	Whether security and access control measures include portable and/or off-site used information devices?			
	KD Reference: _____			
126	Whether signage exists with respect to not identifying sensitive areas and being consistent with insurance, local building code and regulatory requirements?			
	KD Reference: _____ _			
127	Whether review occurs of visitor registration, pass assignment, escort person responsible for visitor, log book to ensure both check in and out occurs and receptionist's understanding of security procedures?			
	KD Reference: _____ _			
128	Whether review of fire, weather, electrical warning and alarm procedures and expected response scenarios for various levels of environmental emergencies is occurring?			
	KD Reference: _____ _			
129	Whether review occurs of air conditioning, ventilation, humidity control procedures and expected response scenarios for various loss or unanticipated extremes?			
	KD Reference: _____ _			
130	Whether review exists of security breach alarm process, including: • definition of alarm priority (i.e., wind blowing door open to armed bomber on premises) • response scenarios to each priority alarm • responsibilities of in-house personnel versus local or vendor security personnel • interaction with local authorities • review of most recent alarm drill			
	KD Reference: _____ _			
131	Whether organisation is responsible for physical access within the IT function that includes: • development, maintenance and ongoing review of security polices and procedures			

No.	Item	Response		
		Yes	No	KD
	• establishes relationships with security-oriented vendors • liaisons with facility management on technology issues related to security • coordinates security awareness and training for the organisation • coordinates activities affecting logical access control via centralised application and operating system software • provides security awareness and training not only within the IT function, but for users of services			
	KD Reference: _____ _			
132	Whether vending machine and janitorial services practices for screening staff in organisation's facility occur?			
	KD Reference: _____ _			
132	Whether security service contracts content, updating and negotiations occur?			
	KD Reference: _____			
133	Whether penetration test procedures and results • coordinates physical penetration test scenarios • coordinates physical penetration test, with vendors and local authorities			
	KD Reference: _____			
134	Whether health, safety and environmental regulations are being complied with?			
	KD Reference: _____			
135	Whether physical security is addressed in the continuity plan and ensures similar physical security over supplier facilities?			
	KD Reference: _____			
136	Whether specific existence of alternative infrastructure items necessary to implement security: • uninterruptible power source (UPS) • alternative or rerouting of telecommunications lines • alternative water, gas, air conditioning, humidity resources			
	KD Reference: _____			
	Manage operations			
137	Whether there is evidence of: • completeness of all processing performed, cold starts and restarts and recoveries • initial programme load (IPL) and shut down procedural sufficiency			

No.	Item	Response		
		Yes	No	KD
	• schedule completion statistics to confirm successful completion of all requirements • physical and logical separation of source and object, test/development/production libraries and change control procedures for moving programmes among libraries			
	• performance statistics for operational activities, including but not limited to: ➢ Hardware and peripheral capacity, utilisation and performance ➢ Memory utilisation and performance ➢ Telecommunications utilisation and performance • extent that performance is matching product performance norms, internally defined performance standards and user service level agreement commitments • operating logs are maintained, retained and reviewed on an ongoing basis • maintenance is being performed on all equipment in a timely manner • operators are rotating shifts, taking holidays and vacations and maintaining competencies			
	KD Reference: _____ 86+7 _			
MONITORING				
	Monitor the process			
138	Whether data identified for monitoring IT resources is appropriate?			
	KD Reference: _____ _			
139	Whether key performance indicators and/or critical success factors are used to measure IT performance against target levels?			
	KD Reference: _____ _			
140	Whether internal reporting of IT resource utilisation (people, facilities, applications, technology, and data) is adequate?			
	KD Reference: _____ _			
141	Whether managerial review of IT resource performance reporting exists?			

No.	Item	Response		
		Yes	No	KD
	KD Reference: _____ _			
142	Whether monitoring controls exist to provide reliable and useful feedback in a timely manner?			
	KD Reference: _____ _			
143	Whether response of organisation to quality control, internal audit and external audit improvement recommendations is appropriate?			
	KD Reference: _____ _			
144	Whether target performance improvement initiatives and results exist?			
	KD Reference: _____ _			
145	Whether organisational performance against stated goals of all groups within the organisation is occurring?			
	KD Reference: _____ _			
146	Whether user satisfaction analysis exists?			
	KD Reference: _____ _			
147	Whether reliability and usability of performance reporting for non-users such as external auditor, audit committee and senior management of the whole organisation is sufficient?			
	KD Reference: _____ _			
148	Whether timeliness of reporting allows for rapid response to identified performance shortcomings or exceptions?			
	KD Reference: _____ _			
149	Whether reporting against policies and procedures established for the performance of activities; (i.e., performance reporting) is sufficient?			
	KD Reference: _____ _			
	Assess internal control adequacy			
150	Whether data identified for monitoring IT internal controls is appropriate?			
	KD Reference: _____ _			
151	Whether internal reporting of IT internal control data is adequate?			
	KD Reference: _____ _			
152	Whether managerial review of IT internal controls exists?			
	KD Reference: _____ _			
153	Whether monitoring controls exist to provide reliable and useful feedback in a timely manner?			
	KD Reference: _____ _			
154	Whether response of organisation to quality control, internal audit and external audit improvement recommendations is appropriate?			
	KD Reference: _____ _			
155	Whether target internal control improvement initiatives and results exist?			
	KD Reference: _____ _			
156	Whether organisational performance against stated goals of internal controls is occurring?			
	KD Reference: _____ _			

No.	Item	Response		
		Yes	No	KD
157	Whether information regarding internal control errors, inconsistencies and exceptions is systematically kept and reported to management?			
	KD Reference: _____			
158	Whether reliability and usability of internal control reporting for non-users such as external auditor, audit committee and senior management of the whole organisation is sufficient?			
	KD Reference: _____ _			
159	Whether timeliness of reporting allows for rapid response to identified internal control shortcomings or exceptions?			
	KD Reference: _____ _			
160	Whether internal control reporting against policies and procedures established for the performance of activities (i.e., internal control reporting) is sufficient?			
	KD Reference: _____ _			
	Obtain independent assurance			
161	Whether independent assurance charters/contracts are appropriately established/executed to ensure adequate review coverage (e.g., certification/accreditation, effectiveness evaluation and compliance assessments)?			
	KD Reference: _____ _			
162	Whether independent certification/accreditation is obtained prior to implementing critical new IT services?			
	KD Reference: _____ _			
163	Whether independent re-certification/re-accreditation of IT services is obtained on a routine cycle after implementation?			
	KD Reference: _____ _			
164	Whether independent certification/accreditation is obtained prior to using IT service providers?			
	KD Reference: _____ _			
165	Whether independent re-certification/re-accreditation is obtained on a routine cycle?			
	KD Reference: _____ _			
166	Whether independent evaluation of the effectiveness of IT services is obtained on a routine cycle?			
	KD Reference: _____ _			
167	Whether independent evaluation of the effectiveness of IT service providers is obtained on a routine cycle?			
	KD Reference: _____ _			
168	Whether independent reviews of IT compliance with legal and regulatory requirements and contractual commitments is obtained on a routine cycle?			
	KD Reference: _____ _			
169	Whether independent review of third-party service providers' compliance with legal and regulatory requirements and contractual commitments is obtained on a routine cycle?			
	KD Reference: _____ _			
170	Whether independent assurance staff is competent and performing per appropriate professional standards?			
No.	**Item**	**Response**		

		Yes	No	KD
	KD Reference: _____ _			
171	Whether professional continuing education programme assists in providing technical competence of independent assurance staff?			
	KD Reference: _____			
172	Whether management proactively seeks out audit involvement prior to finalising IT service solutions?			
	KD Reference: _____ _			
	Provide for independent audit			
173	Whether audit committee is appropriately established and meeting regularly, if appropriate?			
	KD Reference: _____ _			
174	Whether internal audit organisation is appropriately established?			
	KD Reference: _____ _			
175	Whether external audits contribute to the accomplishment of the audit plan?			
	KD Reference:			
176	Whether audit adherence to applicable professional codes of conduct is sufficient?			
	KD Reference: _____ _			
177	Whether independence of auditor is confirmed by signed conflict of interest statements?			
	KD Reference: _____ _			
178	Whether audit plan is based on risk assessment methodology and overall sufficiency of the plan?			
	KD Reference: _____ _			
179	Whether audits are adequately planned and supervised?			
	KD Reference: _____ _			
180	Whether evidence is sufficient enough to support findings and conclusions?			
	KD Reference: _____ _			
181	Whether professional continuing education programme assists in providing technical competence of auditors?			
	KD Reference: _____ _			
182	Whether audit staff is competent and performing per professional auditing standards?			
	KD Reference: _____ _			
183	Whether an adequate reporting process of audit findings to management exists?			
	KD Reference: _____			
184	Whether follow-up of all control issues is occurring in a timely manner?			
	KD Reference: _____ _			
185	Whether audit coverage includes the full range of information systems audits (i.e., general and application controls, system development life cycle, value for money, economy, efficiency, effectiveness, proactive audit approach, etc.)?			
	KD Reference: _____ _			

Audit Programme 3 :Computerised Inventory / Material Management Systems Audit

A scrutiny of the major IT Applications being used by various auditee organizations falling under the different wings (Commercial, Defence, Railways, P&T, Civil Audit) indicates that one of the most commonly used IT Application is in Inventory Management.

The present checklist on Computerised Inventory Systems is intended to help in conducting the Information Technology Audit of specific applications being used by various auditee organizations for managing the inventories. It will assist in determining the existence of internal controls and also the reliance that can be placed on the Inventory Management system being audited. It is stated that not all aspects as highlighted in the check list may be applicable for a particular IT Application depending on the environment in auditee organization and objectives of the system.

The auditor should obtain sufficient and appropriate audit evidence through the performance of compliance and substantive procedures to draw reasonable audit conclusions thereon and to base audit opinion on the financial information. Experience shows that use of CAATs may be very helpful in gathering the audit evidence in support of the audit observations.

Checklist for Auditing Computerised Inventory Systems

No	Item	KD Reference
A.	**Inventory System Requirements (Needs determination function)**	
1.	Does the system record customer/consuming agency demand and replenishment lead-time data for a period, analyze the data for anomalies, and compute demand and lead time forecasts on a regular basis? Computer-generated forecasts generally should be changed only when information is available to the manager that is not available to the automated system	
2.	Does the system compute and routinely update the ordering costs, which may vary depending on the methods of procurement and other factors? The ordering costs should include costs of: o Reviewing the stock position; o Preparing the purchase request; o Selecting the supplier; receiving, inspecting, and placing the material in storage; and o Paying the vendor.	
3.	Does the system estimate and routinely update the per unit inventory holding cost, which is an estimate of the cost to hold each additional unit of inventory? Its primary elements are storage space, obsolescence, interest on inventory investment, and inventory shrinkage (due to deterioration, theft, damage, etc.).	
4.	Does the system re-compute the Economic Order Quantity (EOQ) on a regular basis using the demand forecast, ordering cost, inventory holding cost, and unit cost of the material? In lieu of the EOQ, any other optimum order quantity calculation may be used, provided that it is based on sound principles and it minimizes total cost, including the ordering and inventory holding costs.	
5.	Does the system compute the reorder point level on a regular basis, considering stock available for issue, backorders, quantities on hold, and quantities due for delivery?	
6.	Does the system provide information on current inventories and historical usage to be used in capacity planning?	
7.	Does the system establish overall production/purchase targets necessary to fill customer/consuming agency orders and meet operating schedules?	
8.	Does the system support predefined inspection plans and quality standards?	

No	Item	KD Reference
9.	Does the system support the budgeting of resources for inventories? Normally, budgeted resources for inventories are determined by considering: (a) projected customer/consuming agency orders based on historical customer/consuming agency activity and (b) management decisions projecting future inventory needs.	
10.	Does the system identify available funds by inventory commodity and distinguish available funds for items that are slow moving and are carried in the inventory for more than one accounting cycle?	
11.	Does the system access the core financial system to ensure that funds are available prior to the approval of a request for acquisition of inventory items? There must be a validation of available funds prior to release of requisition orders or purchase requests for inventory items.	
12.	Does the system provide for reducing or terminating acquisitions when funds are limited or not available for new buys?	
13.	Does the system identify funds used and rates of fund use by inventory commodity?	
14.	Does the system calculate fund usage and project the date on which funds will be exhausted at the current rate of usage?	
15.	Does the system provide on a periodic or requested basis, the following types of management information: o Demand? o Procurement lead-time? o Procurement cycle? o Requirements? o Assets? o Available funds? o Budget versus actual? o Rates of fund utilization?	
	B. Inventory System Requirements (Inventory Storage function)	
16.	Is the system integrated with the acquisition and core financial systems to share information of items ordered, received, in storage, and sold/issued or otherwise disposed of.	
17.	Does the system record information on material returned by customer/consuming agency?	
18.	Does the system record information on the receipt in sufficient detail to allow matching of receipt, purchase order/contract, and invoice for payment purposes? Examples of data to collect included item numbers, quantities, units of measure, vendors, and purchase order numbers.	

No	Item	KD Reference
19.	Does the system record the date of receipt to be used for purposes of the prompt payment and to monitor the timeliness of placing items into inventory and the age of inventory items?	
20.	Does the system provide information on items received and accepted necessary to support the payment management function of the core financial system?	
21.	Does the system differentiate between partial receipts against an undelivered order and full receipts?	
22.	Does the system record items in transit and the quantities of each if title to inventory items transfers at the point of origin?	
23.	Does the system record the acceptance or rejection of new or returned items at their destination and the quantities of each? Does it update inventory on hand information as a result?	
24.	Does the system identify shipping discrepancies and product quality deficiencies between the items received and the information provided on shipping documents and purchase orders? Does it support the follow-up on discrepancies conducted by the procurement and finance offices?	
25.	Does the system identify the intended location of the item and track its movement from the point of initial receipt to its final destination?	
26.	Does the system classify inventory items by commodity class to meet agency needs for management and control?	
27.	Does the system maintain sufficient information to support the inventory valuation method chosen in the Program Planning and Monitoring function (e.g., historical cost using First-In First-Out (FIFO), weighted average, or moving average cost flow assumptions or the latest acquisition cost)?	
28.	Does the system allow the cost of an item to include all appropriate purchase and transportation costs incurred?	
29.	Does the system provide financial information in the appropriate format and using the appropriate method to other financial management systems used by the agency?	
30.	Does the system provide information needed to support reconciliation between the inventory system's records and other systems' records?	
31.	Does the system provide support for physical verification of inventory balances by location and type?	
32.	Does the system record changes in the location of an inventory item, such as from one warehouse to another, and any associated changes in the person or organization responsible for stewardship of the item?	

No	Item	KD Reference
33.	Does the system record changes in physical condition (e.g., excellent, good, fair, or poor), quantities, etc., based on the results of physical inventory verifications?	
34.	Does the system provide for the matching of physical counts with inventory quantity and financial records through cycle counting or other inventory management techniques if the agency maintains perpetual inventory records?	
35.	Does the system allow the cost of an item to include all appropriate purchase and transportation costs incurred?	
36.	Does the system provide for reconciliation using beginning of period inventory balances, receipts, and dispositions up to the cut-off point for the physical inventory if the agency does not maintain perpetual inventory records?	
37.	Does the system ensure the retention of records of physical inventory counts until (a) the count is reconciled, (b) all adjusting entries for the physical count are resolved and entered into the financial records, and (c) the next physical count is accomplished, reconciled, and entered into the records?	
38.	Does the system provide for identification of all errors arising from reconciliation processes that apply to a time period prior to the last inventory adjustment? All such errors must be corrected to include appropriate adjustments to prior gains and losses.	
39.	Does the system record the value and quantities of items in transit from one location to another?	
40.	Does the system record losses from the recognition of destroyed, lost, or pilfered items?	
41.	Does the system send the appropriate information to the core financial system and cost accounting system to ensure that they stay in balance with the inventory system if financial adjustments are required as a result of a physical verification?	
42.	Does the system adjust inventory item costs for significant differences between the amount recorded for the items upon receipt and the invoiced amounts paid for the goods?	
43.	Does the system value excess, obsolete, and unserviceable inventory at expected net realizable value? The difference between the carrying amount of the inventory before identification as excess, obsolete, or unserviceable and its expected net realizable value shall be recognized as a loss (or gain) and either separately reported or disclosed. Any subsequent adjustments to its net realizable value or any loss (or gain) upon disposal shall also be recognized as a loss (or gain).	

No	Item	KD Reference
44.	Does the system record the value and quantity of items shipped from the inventory organization to another organization for which accountability has been retained by the inventory organization until receipt by the recipient?	
45.	Does the system record the value and quantity of items identified as in transit being moved from one inventory storage location to another?	
46.	Does the system provide the following types of management information?	
	o Unfulfilled orders?	
	o Discrepancies?	
	o Acceptance and rejection summary?	
	o Days supply?	
	o Inactive stock?	
	o Item expiration/shelf life?	
	o Cycle count?	
C. Inventory System Requirements (Inventory undergoing repair or in production function)		
47.	Does the system record the transfer of an inventory item from its current status to the status of "in repair?" Does it provide information to the core financial system to record the change in financial category?	
48.	Does the system establish an allowance for repairs consistent with the estimated annual cost of repairs if using the allowance method?	
49.	Does the system identify the costs of repair activities?	
50.	Does the system record the transfer of an inventory item from the status of "in repair" to its proper status and location? Provide information to the core financial system to record the change in financial category?	
51.	Does the system transfer items determined to be unserviceable to the disposal process?	
52.	Does the system support the establishment (including technical specifications and accounting classification needed by the inventory system) of orders to be placed with a contractor or other government entity to perform production work on items needed?	
53.	Does the system project the production elements necessary to complete the production cycle? These production elements must reflect bills of material, manufacturing requirements, and production time to produce or repair products.	

No	Item	KD Reference
54.	Does the system provide financial information in the appropriate format and method to other financial management systems used by the agency?	
55.	Does the inventory system accept cost and other appropriate information from the agency's cost system if the agency has a separate cost accounting system to support cost accumulation by work elements, such as job order, activities, products, etc.?	
56.	Does the system track accumulated costs, which should include the value of direct materials, direct labour, and overhead where applicable (including standard costs and rates, if applicable) for work in process? Percentage of completion information should be used to value work in process.	
57.	Does the system provide features to record unit costs and prices of products and services?	
58.	Does the system transfer work in process to finished goods for inventory categorization and accounting purposes?	
59.	Does the system identify the intended location of the item and track its movement from the point of initial receipt to its final destination?	
60.	Does the system record identifiers, quantities, condition, location, and other elements necessary to establish physical control?	
61.	Does the system classify inventory items by commodity class or type to meet agency needs for management and control?	
D. Inventory System Requirements (Inventory disposition function)		
62.	Does the system record changes in the location of the inventory items and the associated changes in the person or organization responsible for stewardship of the item?	
63.	Does the system record the value and quantities of items in transit from one location to another?	
64.	Does the system generate the appropriate financial transactions if the financial category needs to be changed to "held for repair" or "excess, obsolete, or unserviceable?"	
65.	Does the system verify that the customer/consuming agency order is received from an eligible customer/consuming agency who is authorized to use the system and order the items?	
66.	Does the system ensure that inventory items issued are limited to available funds provided by the customer/consuming agency?	

No	Item	KD Reference
67.	Does the system establish and maintain customer/consuming agency records if customer/consuming agency are billed or if tracking of individual customer/consuming agency data, business history, and preferences are important to the program?	
68.	Does the system record relevant information on the customer/consuming agency order, including items ordered; quantities requested; customer/consuming agency name and address; specifications, if appropriate; date received; and other data needed consistent with the inventory program?	
69.	Does the system facilitates recording of details in respect of Cheque or cash received with the customer/consuming agency order against the customer/consuming agency order and send the information to the Receipt Management function of the core financial system?	
70.	Does the system use inbuilt picking list of the stored items for selecting inventory items from storage for issue or other purposes?	
71.	Does the system automatically reduce quantities on hand by the number of items issued/removed?	
72.	Does the system provide advice to customer/consuming agency on shipments of material so that the customer/consuming agency may establish financial controls, as applicable, over shipments in transit from suppliers, and to establish the point of transfer of title? Title to inventory items may be passed to the customer/consuming agency at the point of sale or the point of destination, depending on the agreement with the demanding agency/department.	
73.	Does the system maintain records of items issued, including quantities, shipment methods, dates, destinations, etc., to assist in the reconciliation activities?	
74.	Does the system compare customer/consuming agency order records to issue records and flag any differences for follow-up?	
75.	Does the system determine the appropriate price for a particular customer/consuming agency order using the pricing models and formulas defined in the Pricing Method Definition activity?	
76.	Does the system develop the information necessary to prepare an initial invoice for a customer/consuming agency that provides adequate support for the prices charged?	
77.	Does the system prepare either the initial invoice itself or pass the information required to the core financial system for it to prepare the invoice?	

No	Item	KD Reference
78.	Does the system provide the core financial system with the data necessary to establish the receivable and support subsequent administration of the receivables management and collection process?	
79.	Does the system decrease the inventory of finished goods account and increase the cost of goods sold account by the amount at which the inventory are valued?	
80.	Does the system record revenue and the appropriate offsetting account (e.g., cash, receivables, or advances) in the amount for which the inventory items are sold/issued (price) in case of inventory of finished goods?	
81.	Does the system record the value of items issued from storage or shipped to customer/consuming agency for which title does not pass to the customer/consuming agency until a subsequent event occurs?	
82.	Does the system decrease the quantity of the inventory item on hand by the number of items sent to the disposal organization?	
83.	Does the system record confirmation of receipt of the items by the disposal organization?	
84.	Does the system transfer balances between financial categories, for example, from "inventory held for sale/issue" to "excess, obsolete, and unserviceable inventory?"	
85.	Does the system account for the proceeds resulting from disposition of inventory items as scrap?	
86.	Does the system provide the following types of management information?	
	o Stock availability?	
	o Customer/consuming agency order?	
	o Inventory turnover?	
	o Stock usage?	
	o Losses?	
	o Disposals?	
E. Inventory System Requirements (Program planning and monitoring function)		
87.	Does the system establish price computation models or formulas to be used in the Bill Calculation activity? Pricing models for entities are usually based on costs incurred, but may be based on other factors, such as specific norms and regulations for the agency, utility, and condition.	
88.	Does the system provide methods to support pricing by groupings or commodities of items?	

No	Item	KD Reference
89.	Does the system identify separate methods of pricing needed based on statutory authority or other agency policy? For example, the pricing method used may depend on the nature of the customer/consuming agency, such as within the same agency, another Government agency, corporation etc.	
90.	Does the system establish methods or formulas to be used in valuing and accounting for inventory based on cost? Costs to be considered for inventory held for sale include appropriate purchase, transportation, and production costs incurred to bring the items to their current condition and location.	
91.	Does the system establish appropriate cost methods that apply to the various types of inventories held by an agency? Different methods might also be needed for inventory held for sale/issue based on the type of items, such a medical supplies, perishable goods, and hazardous materials.	
92.	Does the system establish methods to maintain the net realizable value of inventory items?	
93.	Does the system establish methods or formulas to be used in valuing and accounting for inventory in the process of production based on cost? Costs to be considered for inventory in repair or in the process of production (work in process) include materials, labour, and overhead used to convert the items to a finished product.	
94.	Does the system establish appropriate cost methods that apply to the various types of inventories involved in the production process? Different methods might be needed to assign costs to raw materials, work in process, and finished goods in a manufacturing entity.	
95.	Does the system establish methods to capture and accumulate costs for work in process that account for repair or manufacturing performed by an independent third party, such as contractors or other government activities? The cost for work in process will be based on documented cost incurred. The process used to validate such work-in-process costs should be based, to the maximum extent possible, on reporting mechanisms used for contract management, project management, or other similar purposes.	
96.	Does the system provide the ability, where the standard cost method is being used to record costs for work in process, to record standard costs and actual costs for each inventory item, in order to support usage and cost variance analysis? Standard costs will include the anticipated amounts of material, labour, overhead, and other applicable factors.	

No	Item	KD Reference
97.	Does the system track actual and standard cost variances for materials (price and usage), labour (rate and efficiency), and overhead (actual and applied) when a standard cost method is used?	
98.	Does the system record reasons for significant deviations between standard and actual costs?	
99.	Does the system provide capabilities to support adjustments of rates and dispositions of variances by performing periodic allocations?	
100.	Does the system match costs and revenues within the periods they were incurred or realized to identify gains or losses from sales/issual?	
101.	Does the system support analysis of operations on an annual basis to determine if revenues are sufficient to cover the costs of the entire inventory program?	
102.	Does the system provide sufficient transaction audit trails to support balances of inventory shown on the agency's general ledger and changes in those balances?	
103.	Does the system maintain the documentation supporting inventory transactions until it is audited for accuracy and approved by external auditors, but not for less than 3 years? Retention may be longer when (a) required by regulations, (b) there is a possibility of legal action involving the inventories, or (c) contract terms or modifications require longer retention.	
104.	Does the system provide the following types of management information? (a) Cost per rupee of sales/issual? (b) Operations cost?	

Audit Programme 4 :Checklist / Guidelines for auditor's involvement in IT Systems under development

Introduction

1. In November 2003, all the Chief Secretaries and Expenditure Secretary in the Central Government were requested to involve audit in various phases of system development. Consequent to that, several State Governments have requested the local Accountant General to be involved in the development of specific systems. These guidelines are issued in order to assist field offices to effectively and constructively audit the process of system development in the auditee units.

2. The guidelines and programmes are comprehensive and relate to all the phases of the system development life cycle and are more useful when applied in context of development of large systems of capital intensive nature. In case of all systems, all of these may not be applicable. The field offices and particularly the officer who is associated with the audit of the system development process should decide which ones would be applicable.

3. System development has become critical to government departments and organizations hoping to improve governance and the delivery of services to its citizens and clients by investing in large software applications. Yet, often expensive applications development projects fail to deliver on the promises. Government departments and organizations can reduce the risk of such failures by adopting a structured approach such as System Development Life Cycle (SDLC) Methodology to guide themselves and the developers.

4. **Definition of System Development Life Cycle (SDLC) Methodology**

   System Development Life Cycle Methodology (SDLC) is defined as, "a structured approach that divides an information systems development project into distinct stages which follow sequentially and contain key decision points and sign-offs. This permits an ordered evaluation of the problem to be solved, an ordered design and development process, and an ordered implementation of the solution. A final stage allows for management feedback and control through a post-installation evaluation".

5. In practice, however, the process of development of any system tends to take an unstructured path. Problems that might not have been anticipated earlier may compell the system development team to retrace some of the route already trodden. Other methodologies like Rapid Application Development, Joint Application Design Methodology, Soft Systems Methodology etc.often are combined with the structured system development process.

6. Audit must take great care in associating itself only with such systems where a development methodology is distinctly discernible. If the methodolody adopted is purely ad hoc without any clear structure and adequate documentation, it would be extremely risky to offer any comments on such systems.

7. When Audit is involved in the System Development Phase of Information Technology systems it should not take up the role of a consultant or that of an internal auditor but should remain a keen observer whose findings are reported from time to

time to the appropraite level of management for further action. Moreover it should be made clear to the auditee that audit involvement is not to be construed as an 'audit certificate' and the system performance and functioning will be open to audit in future as well.

Audit of Systems under Development

8. The audit of Systems Under Development has three main thrusts: first, to provide an opinion on the efficiency, effectiveness, and economy of project management (Project Controls); second, to assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored (Data Controls); and third to assess the controls being provided for the management of the system's operation (System Management Controls). The first thrust is pursued by having the auditor attend project and steering committee meetings, examining project control documentation and conducting interviews. As for the second thrust, the auditor is limited to examining system documentation, such as functional specifications, to arrive at an opinion on controls.. The same is true for the third thrust, the system's operational controls.

Audit Checklist :

I PROJECT INITIATION PHASE (PI)

At this stage, terms of reference for the project should be formally defined and the project control parameters established. Procedures involve performing a preliminary review of the existing system (including manual system) to assess the need for change and the nature of the suggested changes. The "problem" must be defined. A potential solution should be conceptualized for reference during the feasibility study phase. The description of the solution need not be so detailed that it prejudices the alternatives examined during the feasibility study. At this time all external and internal constraints (cost, time, legislation, departmental guidelines, user needs, etc.) should be identified along with their impact on the problem and the solution. This phase produces a Project Initiation Report.

Audit objective: To establish that project is formally initiated and that appropriate project control measures exist.

Checklist (PI)

PI.1. Review the business and ensure a formal business case exists for the project.

PI.2. Ensure that a Project Initiation document exists and it has the approval of the competent authority.

PI.3 If yes, then verify that the Project Initiation document contains at least the following features:

➔ Broad reasons for undertaking the Project, such as:

- ❖ The problem to be remedied or process to be improved, and/or
- ❖ Enhancing the organisation's ability to achieve its goals, and/or
- ❖ Description of the deficiencies in relevant existing system; and/or
- ❖ The opportunities that would be provided for increasing economy or efficiency of operations; and/or
- ❖ Internal controls and security needs that would be satisfied by the Project.

➔ A clear statement of the project definition.

➔ The project initiation document is in consonance with the Policy on the subject;

➔ In case, the project is Centrally sponsored or institution-aided, then the conditions of such grants/ aid have been followed;

➔ Major risks have been identified such as staff resistance, hardware/software obsolescence, and technological constraints like communication infrastructure etc. along with a statement of internal and external constraints, such as organizational changes required & impact on other systems.

PI.4. Ensure that the Project Initiation document has been reviewed and approved by the competent authority.

PI.5. Ensure that an appropriate project organization has been outlined in the Project Initiation documentation. Determine by examining the Project Initiation document that:

- ➔ Project Team members and representatives and their responsibilities have been named including:
  - ❖ Project Director /Manager
  - ❖ User Manager/Director
  - ❖ Technical Representatives
  - ❖ User Functional Representatives
- ➔ Steering Committee/ Sign Off Authority has been established and they have been delegated requisite powers.
- ➔ Evaluate the background and qualifications of project members for their assignment to specific project tasks.

PI.6. Ensure that the user department management has appointed personnel from its department to participate in the project.

PI.7. Verify that the Project Manager or one of the team members is responsible to ensure the complete and accurate accumulation of project costs.

PI.8. Determine from the Project Initiation document that a work plan, including target dates and resource requirements has been prepared. It delineates the manner in which each phase of the development process (the preparation of feasibility study, requirement definition, system design etc) is to be approved prior to proceeding to the next phase of the project (programming, system testing, transaction testing, parallel testing etc.).

PI.9. Verify that the target dates indicated in the work plan are in keeping with the resource requirements outlined and any constraints involved.

II FEASIBILITY STAGE (FS)

When this stage is complete an appropriate solution to the problem should have been determined and a preliminary plan for it implementation designed. User Requirements may be documented or established thus providing a basis for identifying the solution. It is of prime importance that enough alternative approaches be examined. A detailed analysis, at the conceptual level, of the various alternatives should support a formal justification for the suggested solution. This analysis should include cost benefit analysis, consideration of financial and operational controls, and organization compatibility. As in the project initiation phase, care must be taken that evaluations are objective and complete and that there is no "built-in" bias towards one particular solution. Resource requirements for the remainder of the project should be identified and time and costs estimated for management approval. Broken into appropriate project phases, these factors will be used to maintain and monitor project development. Documentation of the above should be contained in a Feasibility Study Report.

Audit objective: To establish that a feasibility study, including an Overall Project Plan, has been undertaken to determine the most appropriate solution to a stated problem in terms of organizational capability, economic justification, and technical suitability.

FS.1 Ensure that steps have been taken by the project team to identify and consult all affected parties?

FS.2 Ensure that a Technological Feasibility Study been prepared and documented?

- ➔ Is the proposed technology feasible, considering the technical sophistication existing or available through the organization?

FS.3 Review the technology feasibility report to see if it has adequately addressed:

- ➔ Hardware needs and availability.
- ➔ System software needs and availability.
- ➔ Communications hardware and software needs availability. Valid time constraints in the user department's information requirements and the manner of satisfying them.
- ➔ Operational feasibility (compliance with information architecture e.g. whether the new project fits into the current mix of hardware, software, and communications).

FS.4 Verify that there is a consensus among user departments and designers concerning the technological aspects of the system's configuration.

FS.5 Determine the organizational capability to manage the related technologies and to decide whether the technologies should be developed or bought, operated in-house or out, and maintained in-house or out.

FS.6 Has a User Requirements document been prepared and released? Does it include the following expression of need in terms of the organization's mission:

- ➔ A description of the current function.
- ➔ Analysis of the deficiencies of the current function.
- ➔ Resources expended on the current function.
- ➔ Volume of work produced with the current function, including peak processing performance and projected growth.
- ➔ Internal control and security requirements.
- ➔ Justification for improvement and changes.
- ➔ Scope and objectives of proposed system.
- ➔ Alternative solutions to solving the need.
- ➔ Relationships with other systems.
- ➔ Relationships with long-range plans and other information resource management initiatives.

FS.7 Has the accuracy and completeness of user requirements been acknowledged by the appropriate level of user, and by Data Processing management.

FS.8 Has the User Requirements document been reviewed by the Steering Committee/Sign off Authorities?

- ➔ Have they signified acceptance of the need to continue the project? Note any conditional acceptance for follow-up in later stages.

FS.9 Confirm, if possible, with independent sources the reliability and track record of the recommended hardware and software.

FS.10 Confirm if there is a plan to address the intellectual Property issues, including the ownership of source code in case of development of customised software being outsourced.

FS.11 Check whether a Cost/Benefit document has been prepared and released? Are all costs identified as operating or capital?

FS.12 Ensure that the analysis of the project costs and benefits was prepared to evaluate the economic feasibility of each alternative; check that

- ➔ the assumptions and constraints in the cost/benefit analysis are reasonable
- ➔ the user and system costs cover all stages of the life cycle
- ➔ the estimated costs for each alternative include hardware and software enhancements needed to support that alternative
- ➔ estimated costs for each alternative includes cost of security and internal controls, data preparation and entry, file conversion, testing, parallel operations, acceptance, and related costs
- ➔ the basis of estimation and computation of costs is reasonable
- ➔ there is a consensus among end users, designers, and implementers concerning system costs, benefits, and contractual agreements

FS.13 Ensure that the analysis of the project costs and benefits takes into consideration the impact on human resources. Verify that estimated costs for each alternative includes:

- ➔ training,
- ➔ redeployment of staff,
- ➔ ergonomic issues.

FS.14 Check whether the accuracy and completeness of the cost/benefit analysis and acceptance of the recommended alternative has been acknowledged by the appropriate level of user and by Data Processing management.

FS.15 Has the Cost/Benefit document been reviewed by the Steering Committee/Sign off Authorities?

- ➔ Have they signified acceptance of the recommended alternative and the need to continue the project? Note any conditional acceptance for follow-up in later stages.

FS.16 Check whether the users of an appropriate level and Data Processing management have acknowledged that the analysis of processing alternatives is accurate and complete and agrees with the recommendations.

FS.17 Check whether steps been taken by the project team to identify and consult all affected parties?

FS.18 Does the Project documentation show that the skills of the staff employed on the project meet the requirements specified in the Personnel Skills Summary?

FS.19 Has a Steering Committee Meeting Schedule document been prepared and released to all interested parties, including EDP and user management?

FS.20 Review the minutes of the Committee meetings and note the following:

- ➔ that EDP and user management were represented at each meeting, and
- ➔ that meetings were held regularly.

FS.21 Has a Feasibility Stage Status document been prepared and released? Verify that it contains at least the following:

- ➔ actual resources used to date, compared to planned, with reasons for variance
- ➔ actual milestones achieved to date, compared to planned, with reasons for variance
- ➔ plan for the next stage including reference to the following:
  - ❖ analyzing and specifying the user's detailed requirements
  - ❖ establishing change control processes
  - ❖ updating the cost/benefit analysis
  - ❖ obtaining management approval
  - ❖ updated budget and reasons for any changes
  - ❖ updated schedule and reasons for any changes
  - ❖ recommendation to continue or discontinue the project

FS.22 Check whether the Feasibility Study identifies the need for a System Processing Controls Specifications or similar document?

FS.23 Determine that a statement of the level of security, privacy and accessibility needed for system's data conforms to the government Acts, and that the statement is included with the documentation to be reviewed by the Steering Committee/Sign off Authorities.

III SYSTEM DESIGN STAGE (SD)

Work during this phase will translate the proposed conceptual solution, determined during the feasibility study, into a workable solution ready for detailed design and implementation.

This will require:

- **The preparation of a system outline, including flowcharts, system performance criteria and the identification, definition and preliminary formatting of all inputs, outputs and files used or produced by the system. (This will require extensive liaison with users.)**
- **An overview of the internal control framework and operating procedures to ensure that they meet the objectives of the system being developed (The proposed system should satisfy all user requirements.)**
- **The selection of facilities and job specifications for suppliers.**
- **An outline of all functional specifications to ensure that the general design meets all system objectives that have been determined.**
- **The revised costs, time estimates, and other criteria relating to future phases for management approval.**

Audit objective: To ensure that the general design of the system expands on the findings of the feasibility study, produces a functional description of manual and EDP processes, and devises an overall system design that can be used to obtain a commitment for Detailed Design Stage.

SD.1 Check whether the organization has adopted any system development methodology and framework to ensure that a process is in place that appropriately addresses all system design issues (i.e. input, processing, output, internal controls, security, disaster recovery, response time, reporting, change control etc.)

SD.2 Check whether a Systems Specifications document has been prepared and released? Verify that it contains at least the following specifications/features:

- ➔ system objectives and scope
- ➔ general system concept and design considerations
- ➔ chart showing function structure in terms of processes
- ➔ logical data flow diagram showing flow among processes and data stores at the data element level
- ➔ Process descriptions, including complete and detailed definitions of processes for all business cases involved.
- ➔ Appropriate audit trails and controls are built into the system
- ➔ Specifies volumes, timings, highs and lows, and quality specified for inputs, outputs, and data stores
- ➔ Service levels: Complete description of performance requirements. This will be used in later stages to confirm the technical feasibility and resources requirement of the system

SD.3 Check that the accuracy and completeness of system specifications has been acknowledged by the appropriate level of user and by Data Processing management.

SD.4 Ensure that the System Specifications document been reviewed by the Steering Committee/Sign off Authorities? Have they signified acceptance of the need to continue the project? Note any conditional acceptance for follow-up in later stages.

SD.5 Ensure that the data dictionary/ directory has been prepared or updated to contain the system specifications.

SD.6 Ensure that the skills of the staff being employed on the project (as Team Members or Steering Committee/Sign off Authority members) continue to meet the requirements envisaged in the Project Initiation report or Feasibility Report.

SD.7 Has a General Design Stage Status document been prepared and released? Verify that it contains at least the following:

- ➔ actual resources used to date, compared to planned, with reasons for variance
- ➔ actual milestones achieved to date, compared to planned, with reasons for variance
- ➔ a roadmap for the Detailed Design Stage, including the following activities:

    - ❖ updating the data dictionary/directory
    - ❖ carrying out the final design of all inputs and outputs
    - ❖ verification of security concerns having been met
    - ❖ need for a detailed testing plan.
    - ❖ estimating performance and resource requirements
    - ❖ updating project plans and budgets
    - ❖ updating the cost/benefit analysis
    - ❖ obtaining management approval
    - ❖ the preliminary plan for the Implementation Stage, including the following:

- identification of manual procedures to be developed
- manuals that will be affected
- facilities needs
- communications needs
- training

➔ an updated budget and reasons for any changes
➔ an updated schedule and reasons for any changes
➔ an updated cost/benefit analysis
➔ a recommendation to continue or discontinue the project

SD.8 Verify actual resources used in source documents.

SD.9 Verify that the updated budget and schedule is in keeping with the updated cost/benefit analysis.

SD.10 Verify the updated cost/benefit analysis against the cost/benefit analysis from the previous stage and from source documents.

SD.11 Determine that the updated cost/benefit analysis has taken into consideration the human resource impact requirements.

SD.12 Check the accuracy and completeness of the General Design Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

SD.13 Ensure that the General Design Stage Status document has been reviewed by the Steering Committee/Sign off Authorities and have they signified acceptance of it?

SD.14 Ensure that a System Processing Controls Specifications or similar document been prepared and released? Verify that it addresses at least the following issues

Completeness

➔ Ensuring that all data are initially recorded and identified.
➔ Control should be established close to the source of the transaction.
➔ Output should be reconciled to input.
➔ Ensuring that corrections for all identified errors are re-entered into the system.
➔ The timing of input submissions and output distribution should be properly coordinated with processing.
➔ Procedures are needed to ensure that output reports are independently reviewed for completeness and form.

Accuracy

➔ Procedures should exist to prevent errors in the preparation of input or source data, and to detect and correct any significant errors that do occur.
➔ Procedures should exist to prevent errors arising when data are converted to machine processable form, and to detect and correct any significant errors that do occur.
➔ There should be procedures to ensure that data are transmitted accurately to the computer centre.
➔ Procedures should ensure that only valid files are used.
➔ Controls must ensure that the accuracy of data is maintained during processing.
➔ Procedures should ensure that program computations are performed correctly.
➔ There should be a system of control over the physical operations of the computer system.

- ➔ Procedures should exist to ensure that all significant errors that have been identified at various stages in the system have been corrected, re-entered and properly reflected in the output.
- ➔ Procedures are needed to ensure that all required output reports are delivered to the proper user departments.

Authorization

- ➔ To ensure that only authorized data is processed.
- ➔ Security, privacy, and accessibility level classifications for data related to the system should be determined and appropriate measures devised to ensure proper storage, transmittal, access, privacy and destruction.
- ➔ There should be a method of identifying and locating the component file records and input/output documents involved in the processing of a given transaction or in the accumulation of a given total.

Backup/Recovery

- ➔ Procedures for system backup/recovery should be documented and related training plans prepared.
- ➔ Procedures for data preparation, transcription, data control, and output distribution should be documented and related training plans prepared.

Audit Trail

- ➔ There should be logs to identify and locate the component file records and input/output documents involved in the processing of a given transaction or in the accumulation of a given total.

SD.15 Ensure that the system will operate efficiently and effectively check whether:

A System Management Controls Specifications Report or similar document has been prepared and released and verify that it addresses at least the following:

Efficiency

- ➔ There should be a standard or set of standards to determine system efficiency.
- ➔ There should be a mechanism to compare performance with standards and to report variances.
- ➔ There should be procedures for managers to follow up on variances from standards and for recording action taken.

Effectiveness

- ➔ Effectiveness standards for the system's objectives should be established.
- ➔ There should be a mechanism to determine and report situations where systems are no longer able to meet their original objectives.

Economy

- ➔ Management should have formal procedures to review projects and their resulting applications system regularly for economy.

IV DETAILED DESIGN STAGE (DD)

Based on the functional specifications from the System design stage, detailed procedures and computer specifications are produced. All controls, procedures, work flows, input/output documents, processing logic, file/data base layouts, and data elements will be finalized. Management and user approval of this design stage is paramount. Therefore, the final product of this phase, the Detailed Design Report, should contain, in addition to detailed program specifications,

workflows, etc., a non-technical description of the entire system. This should encompass:

- **a system description, objectives, inputs, outputs**
- **a system flowchart illustrating the conceptual design**

Appropriate members of management should review the detailed specifications and technical requirements. Documented system test plans and implementation and conversion plans should also be produced at this stage, and, in addition, a plan on how the activities in the implementation and installation phases will be coordinated.

Audit Objective: To ascertain that a detailed system design is developed from the functional specification created in the general system design.

DD.1 Has a Detailed Systems Design document been prepared and released? Verify that it covers at least the following:

- ➔ system flow and description, by function
- ➔ data dictionary
- ➔ system files
- ➔ system inputs, including design of forms and video screens
- ➔ system outputs, including design of forms, reports and video screens
- ➔ system interface specifications
- ➔ system software specifications
- ➔ hardware specifications
- ➔ communications specifications
- ➔ system management utility specifications
- ➔ audit, control, and security specifications
- ➔ conversion specifications
- ➔ Ensures that file requirements for at least the following files are being structured as per system and user requirement and the organizations data dictionary rules: master, transaction, command, programme, control, table, report, print, log, transmission.
- ➔ common processing module specifications
- ➔ Input control and output control issues like :
  - ❖ does the application include control features, to help ensure that only specifically authorised persons can input transaction and master data into the system, such as access control matrix and logical access controls (including passwords and biometrics) are in place depending on the security needs of the organization.
  - ❖ do audit trails and controls provide the possibility of protecting the users against discovery and misuse of their identity by other end users (e.g. by offering anonymity, pseudonymity, unlinkability or unobservability) without jeopardising the systems security.
  - ❖ do input routines trap the userid, logon etc that permit authorised persons to identify the end user responsible for that element
  - ❖ are controls in place to ensure that all items entered can be accounted for, such as having the system automatically attach a sequential number to each item;

- ❖ are there procedures in place to help ensure that all successfully entered transactions are processed fully or followed up to ensure their proper final disposition;
- ❖ does the application include procedures that should ensure transaction are recorded into the proper period,
- ❖ does the application system include automated or manual procedures to identify transaction designed to circumvent automated controls?
- ❖ are application logs inbuilt to keep track of the transactions done? Are there controls designed to ensure that data stored in the application is protected from unauthorised changes or deletion;
- ❖ does the application system have automated or manual features designed to backup all or changed application system data at regular intervals.

DD.2 Review system specifications for each application within the system for clarity, completeness, and consistency.

DD.3 Review flow charts, decision tables, or narratives to assess the reasonableness of program logic incorporated in applications.

DD.4 Check whether the accuracy and completeness of Detailed System Design specifications has been acknowledged by the appropriate level of user and Data Processing management**.**

DD.5 Check that the Detailed System Design document has been reviewed by the Steering Committee/Sign off Authorities? Have they signified acceptance? Note any conditional acceptance for follow-up in later stages.

DD.6 Check whether a program and system test plan has been developed and released? Verify that it covers at least the following both for program and system testing, and for volume and operational testing:

- ➔ overview of the software to be tested, including vendor software and conversion software and the work environment it operates in
- ➔ test schedule
- ➔ materials and supplies including equipment, software, storage facilities, documentation, test input, sample output, and special forms
- ➔ training requirements
- ➔ list of user requirements to be tested
- ➔ list of operational requirements to be tested
- ➔ overview of test progression
- ➔ description of the test to be performed on each requirement including the type of input to be used, the method for recording results, constraints such as equipment or personnel availability, evaluation criteria and any data manipulation required for reporting purposes

DD.8 Check whether the accuracy and completeness of the Test Plan has been acknowledged by the appropriate level of user and by Data Processing management.

DD.9 Check that the Test Plan document has been reviewed by the Steering Committee/Sign off Authorities?

DD.10 Check about all of the items in the User Requirements document being tested? Appropriate tests may include: walk throughs, simulations and prototypes. Ensure that each module program, interrelated subsystem and the system as a whole are

thoroughly tested. Sufficient time is allowed and sufficient staff (both in number and qualifications) is allocated for testing purposes. Where items are not being tested, check that a suitable explanation has been provided and accepted by the Steering Committee/Sign off Authorities.

DD.11 Check that the skills of the staff being employed on the project (as Team Members or Steering Committee/Sign off Authority members) continue to meet the requirements specified in the Personnel Skills Summary?

DD.12 Has a Steering Committee Meeting Schedule document been prepared and released to all interested parties including EDP and user management?

DD.13 Has a Detailed Design Stage Status document been prepared and released. Verify that the status document contains at least the following:

- ➔ actual resources used to date, compared to planned, with reasons for variance
- ➔ actual milestones achieved to date, compared to planned, with reasons for variance
- ➔ a roadmap for the Implementation stage, including the following activities:
  - ❖ designing the structures, logic, and flow of each system component
  - ❖ designing all data bases and files
  - ❖ estimating system performance and resource requirements and confirming that service levels will be met
  - ❖ designing conversion tools
  - ❖ coding and testing programs
  - ❖ purchasing and testing vendor software
- ➔ preliminary plan for the Installation Stage including reference to the following:
  - ❖ conversion of files
  - ❖ training
  - ❖ instruction manuals
  - ❖ redeployment of staff
- ➔ updated budget and reasons for any changes
- ➔ updated schedule and reasons for any changes
- ➔ updated cost/benefit analysis
- ➔ recommendation to continue or discontinue the project

DD.14 Verify actual resource use in source documents.

DD.15 Verify that the updated budget and schedule are in keeping with the updated cost/benefit analysis.

DD.16 Verify the updated cost/benefit analysis against the cost/benefit analysis from the previous stage and from source documents.

DD.17 Verify that the updated cost benefit analysis takes into consideration the human resource impact requirements.

DD.18 Verify the accuracy and completeness of the Detailed Design Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

DD.19 Verify that the Detailed Design Stage Status document has been reviewed by the Steering Committee/Sign off Authorities and have they signified an acceptance of it?

DD.20 To ensure that the data processed and stored by the system is complete, accurate and authorized check whether the Processing control techniques outlined in the Processing Controls Specifications Report have been included for testing in the Test Plan.

DD.21 Verify that the test plan addresses the control requirements outlined in the Processing Control Specifications

DD.22 To ensure that the system will operate efficiently and effectively check that the control techniques to satisfy the requirements outlined in the system management controls specification document have been included for testing in the test plan.

DD.23 Verify that the test plan addresses the control requirements outlined in the System Management Control Specifications document

V IMPLEMENTATION STAGE (IM)

This stage creates all computer programs, forms, manuals and training material needed for an operational system. Detailed program logic will be designed and application software coded. User, operations and training manuals will be finalized and should cover, where appropriate:

- data capture
- data validation
- system audit trails and controls
- verification of analysis report
- computer operating instructions
- back-up and re-run procedures
- security procedures

All aspects of the system, including program logic and operational procedures, should be thoroughly tested. All procedures required for the installation of the system should be defined and scheduled.

Audit objective: To establish that all appropriate forms, manuals, programs and training materials have been created from the detailed systems specifications and testing has been done according to the plan.

IM.1 Check that all manuals and other outputs required have been completed before installation begins.

IM.2 Determine that the following have been prepared:
- ➔ conversion tools
- ➔ user manuals
- ➔ conversion manuals
- ➔ training manuals
- ➔ operations manuals
- ➔ program and systems documentation.

IM.3 Verify that the user manual has at least the following specifications/ features:
- ➔ Overview of the system and the environment

- ➔ Explanation of the all system inputs, programmes, output and integration with other systems
- ➔ Explanation of all data entry screens and data display screens
- ➔ Explanation of any and all error messages and appropriate response
- ➔ Describes the functions sufficiently,
- ➔ Serves as a reference document,
- ➔ Explains how to prepare input data and parameters,
- ➔ Explains how to interpret output results,
- ➔ Provides a full description of the application,
- ➔ Describes how to correct errors,
- ➔ Describes how to recover operations.

IM.4 Ensure that an Operators manual has been prepared which includes but is not limited to:

- ➔ System name, program name and sequence of execution
- ➔ Definition of file names, input, procedure and output and media format
- ➔ Console commands and parameters requiring entry by operator
- ➔ Backup, restart, and restore procedures at various points or upon abnormal end
- ➔ Special output forms or procedures; report/output distribution
- ➔ Emergency fix procedures.

IM.5 Check whether the accuracy and completeness of the required manuals and outputs have been acknowledged by the appropriate level of user and by Data Processing management.

IM.6 Check whether the required manuals and outputs been reviewed by all members of the Project Team and have they signified acceptance? Note any conditional acceptance for follow-up in later stages.

IM.7 Check whether parallel processing is used to support the implementation of highly complex or high risk application systems?

IM.8 Check whether a Test Report has been prepared and released (consisting of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, user acceptance testing and finally pilot testing of the total system to avoid any unexpected system failure. Specific technology acceptance tests should include inspection, functionality tests and workload trials).

IM.9 Verify that the test report covers at least the following, both for program and system testing, and for volume and operational testing:

- ➔ test results
- ➔ reasons for any testing not completed
- ➔ follow-up action taken where required as indicated by test results

IM.10 Check whether the accuracy and completeness of the Test Report have been acknowledged by the appropriate level of user and by Data Processing management.

IM.11 Has the Test Report document been reviewed by the Steering Committee/Sign off Authorities and have they signified acceptance? Note any conditional acceptance for follow-up in later stages.

IM.12 Whether the status of the project compared to the budget and schedule contained in the Detailed Design Stage Status document has been addressed.

IM.13 Has an Implementation Stage Status document been prepared and released. If so, verify that it contains at least the following:

- ➔ actual resources used to date, compared to planned, with reasons for variance

- ➔ actual milestones achieved to date, compared to planned, with reasons for variance
- ➔ a road map for the Installation stage, including the following:
  - ❖ file conversion, including any reconciliations and sampling of results
  - ❖ training, including schedules and distribution of materials
  - ❖ distribution of user and operations manuals
  - ❖ redeployment of staff
  - ❖ updated budget and reasons for any changes
  - ❖ updated schedule and reasons for any changes
  - ❖ updated cost/benefit analysis
  - ❖ recommendation to continue or discontinue the project

IM.14 Verify actual resource use in source documents.

IM.15 Verify that the updated budget and schedule are in keeping with the updated cost/benefit analysis.

IM.16 Verify the updated cost/benefit analysis against the cost/benefit analysis from the previous stage and source documents.

IM.17 Determine that the updated cost/benefit analysis has taken into consideration the human resource impact requirements.

IM.18 Verify the accuracy and completeness of the Implementation Stage Status document and agreement with it has been acknowledged by the appropriate level of users and by Data Processing management.

IM.19 Ensure that key data controls are effective check that effective procedures are in place to ensure that no data are lost or erroneously changed during conversion to the newly designed system (e.g. the conversion date may be mistaken as the transaction date in the new system)

IM.20 To ensure that key system controls are effective ensure that

- ➔ the system acceptance is performed by quality assurance personnel by evaluating both manual and automated procedures,
- ➔ system acceptance was performed using data similar to, but independent of program testing data.
- ➔ the quality assurance group certifies in writing that the system performs in accordance with the functional and performance specifications.
- ➔ the "go/no go" decision is made by the user based on the quality assurance group's certification and user satisfaction.

IM.21 Ensure that when the system is ready for initial operation its implementation is coordinated with all personnel involved and with the representatives of other systems that are affected.

VI INSTALLATION STAGE (IN)

This stage converts the system to operational status. The work includes converting existing files (if any) or creating the initial information base, training all personnel involved with the system (user and EDP), and instituting control and operational procedures through pilot or parallel run phase-in. All documentation from previous phases should be finalized. Conversion and installation procedures should be reviewed and tested. The project manager should issue a formal Project Completion Notice for approval.

Audit objective: To ensure that the system and any file conversions properly move from the development status to the operational and maintenance status.

IN.1. Whether there is a formal SDLC methodology in place for system installation, including but not limited to a phased approach of training, performance sizing, conversion plan, testing of program, group of programmes and total system, a parallel test plan, acceptance testing, security testing, operational testing, change controls, implementation and post implementation review and modification.

IN.2. Whether the accuracy, completeness, and authenticity of the files created by conversion are ensured through the use of appropriate control techniques.

IN.3. Review the conversion plan before it is executed, referring to the List of Minimum System Processing Controls.

IN.4. Verify that control techniques are being included in the conversion process to satisfy all control concerns.

☞ This is an extremely critical process. No doubt about the integrity of the data in the new files should be tolerated. Control techniques such as one-to-one checks, may have to be used.

IN.5. Verify that the conversion was carried out according to plan.

IN.6. Verify that training was carried out according to the schedule prepared in the Implementation stage and that any variations have been agreed to by user management.

IN.7. Have installations been carried out according to the schedule prepared in the implementation Stage and have any variations been agreed to by the user management?

IN.8. Has user acceptance been formally agreed to, as appropriate, according to schedule? For example, if stand-alone processing locations are being installed on an independent basis, each location should sign-off its acceptance of the system.

IN.9. Ensure that all vendor provided system software installation passwords were changed at the time of installation.

IN.10. Has an installation Stage Status document been prepared and released?

Verify that it contains at least the following:

- ➔ actual resources used to date, compared to plan, with reasons for variance.
- ➔ actual milestones achieved to date, with reasons for variance.
- ➔ updated budget and reasons for any changes.
- ➔ updated schedule and reasons for any changes.
- ➔ updated cost/benefit analysis

IN.11. Verify actual resource use in source documents.

IN.12. Verify that the updated budget and schedule are in keeping with the updated cost/benefit analysis.

IN.13. Verify the updated cost/benefit analysis against the cost/benefit analysis from the previous stage and from source documents.

IN.14. Determine that the updated cost/benefit analysis has taken into consideration the human resource impact requirements.

IN.15. Whether the accuracy and completeness of the Installation Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

VII POST-INSTALLATION STAGE (PO)

Work during this stage consists of examining the project performance and system performance against the original project documentation of system cost/benefit and project cost and time schedules. A period of settling in is normally allowed between Installation and Post-Installation audit. The audit team could be changed at this point to maximize objectivity. Thus, project reviews are important after system installation to assess the success of the systems development process and to identify any differences in control design and control operation

Audit objective: To establish that the system operates in accordance with the design objectives and other measurement criteria, and project costs/benefits have been achieved.

PO.1. Whether a formal post-installation review has been undertaken and the results reported to management.

PO.2. Has a Post-Installation report or similar document been prepared?
Verify that it contains the following:
- ➔ documentation of the system's actual achievements
- ➔ comparison of those achievements against the original objectives
- ➔ recommendations for improvements
- ➔ actual resource use, compared to the original plan, with reasons for variance
- ➔ actual milestones achieved, compared to the original plan, with reasons for variance
- ➔ updated cost/benefit analysis

PO.3. Verify actual resource use in source documents.

PO.4. Verify the updated cost/benefit analysis against source documents.

PO.5. Determine that the updated cost/benefit analysis has taken into consideration the human resource impact requirements.

PO.6. Confirm that the organization continues to have the necessary resources to manage the Project successfully.

PO.7. Have the needs of the business and/or end users changed

PO.8. Do documented procedures exist for controlling all documentation?

PO.9. Have the Project documentation, training material and training program delivered and kept upto date.

PO.10. Are copies of all documentation stored off the premises?

PO.11. Are the contractual relationships satisfactory? Verify the ownership of the source code if the customized software is outsourced.

PO.12. Have all the stakeholders' issues been addressed? These include:

- ➔ The statutory process
- ➔ Communications
- ➔ External relations
- ➔ Environmental issues
- ➔ Personnel

PO.13. Is the department setting realistic targets for continuous improvement year on year from this service?

PO.14. Is the department tracking its progress to improved performance and the flow of results through milestones and the business planning cycle?

PO.15. Does the organisation have a well defined implemented and effective process for embedding improvement based on the lessons learnt from the Project?

PO.16. Change Management:

Ensure that:

- ➔ Change control is a formal procedure for both the user and the development groups
- ➔ Change control logs ensure all changes shown were resolved
- ➔ User is satisfied with turnaround of change requests- timeliness and cost
- ➔ Changes were made as documented
- ➔ Current documentation reflects changed environment
- ➔ Change process is being monitored for improvements in acknowledgement, response time, response effectiveness and user satisfaction with the process.
- ➔ Test that for a sample of changes the following have been approved by the management:
  - ❖ Request for change
  - ❖ Specification of change
  - ❖ Access to source program
  - ❖ Programmer completion of change
  - ❖ Request to move change into test environment
  - ❖ Completion of acceptance testing
  - ❖ Request for move into production
- ➔ Overall and specific security impact has been determined and accepted
- ➔ Distribution process has been developed
- ➔ Test the review of change control documentation for inclusion of
  - ❖ Date of requested change
  - ❖ Person(s) requesting
  - ❖ Approval for change request
  - ❖ Approval for change made-IT function
  - ❖ Approval of change made-users

- ❖ Documentation update date
- ❖ Move date into production
- ❖ Quality assurance sign off of change
- ❖ Acceptance by operation

➔ Ensure that

- ❖ Code check in and checkout procedures for change exist
- ❖ Change control logs ensure that all changes on log were resolved to user satisfaction.
- ❖ Users are aware and understand need for formal change control procedures
- ❖ Staff enforcement process ensures compliance to change control procedures
- ❖ Documentation determines request or system change has been approved and prioritised by the management of the affected users and the service provider.

PO. 17. Do preventive maintenance schedules have any negative impact on critical or sensitive applications and is scheduled maintenance being scheduled for peak workload periods.

Literatures that have been consulted include COBIT (Control Objectives for Information & related Techniques) guidelines & Publications of Treasury Board of Canada Secretariat.

Appendix

Here is a Quick Diagnostic Test for any organization which is developing an Information Technology System.

THE QUICK DIAGNOSTIC

Give the project 3 points for each "yes" answer. Give the project partial credit if you feel that is most accurate—for example, give it 2 points for "probably" and 1 point for "kind of, but not really." If the project is in the early stages, answer the questions based on the project plans. If the project is well underway, answer the questions based on what has actually happened on the project. The section following the test explains how to interpret the score.

Requirements

1. ____ Does the project have a clear, unambiguous vision statement or mission statement?
2. ____ Do all team members believe the vision is realistic?
3. ____ Does the project have a business case that details the business benefit and how the benefit will be measured?
4. ____ Does the project have a user interface prototype that realistically and vividly demonstrates the functionality that the actual system will have?
5. ____ Does the project have a detailed, written specification of what the software is supposed to do?
6. ____ Did the project team interview people who will actually use the software (end users) early in the project and continue to involve them throughout the project?
7. ____ Does the project have a detailed, written Software Development Plan?
8. ____ Does the project's task list include creation of an installation program, conversion of data from previous versions of the system, integration with third-party software, meetings with the customer, and other "minor" tasks?
9. ____ Were the schedule and budget estimates officially updated at the end of the most recently completed phase?
10. ____ Does the project have detailed, written architecture and design documents?
11. ____ Does the project have a detailed, written Quality Assurance Plan that requires design and code reviews in addition to system testing?
12. ____ Does the project have a detailed Staged Delivery Plan for the software, which describes the stages in which the software will be implemented and delivered?
13. ____ Does the project's plan include time for holidays, vacation days, sick days, and ongoing training, and are resources allocated at less than 100 percent?
14. ____ Was the project plan, including the schedule, approved by the development team, the quality assurance team, and the technical writing team—in other words, the people responsible for doing the work?

Project Control

15. ____ Has a single key executive who has decision-making authority been made responsible for the project, and does the project have that person's active support?

16. ____ Does the project manager's workload allow him or her to devote an adequate amount of time to the project?

17. ____ Does the project have well-defined, detailed milestones ("binary milestones") that are considered to be either 100 percent done or 100 percent not done?

18. ____ Can a project stakeholder easily find out which of these binary milestones have been completed?

19. ____ Does the project have a feedback channel by which project members can anonymously report problems to their own managers and upper managers?

20. ____ Does the project have a written plan for controlling changes to the software's specification?

21. ____ Does the project have a Change Control Board that has final authority to accept or reject proposed changes?

22. ____ Are planning materials and status information for the project—including effort and schedule estimates, task assignments, and progress compared to the plan thus far—available to every team member?

23. ____ Is all source code placed under automated revision control?

24. ____ Does the project environment include the basic tools needed to complete the project, including defect tracking software, source code control, and project management software?

Risk Management

25. ____ Does the project plan articulate a list of current risks to the project? Has the list been updated recently?

26. ____ Does the project have a project risk officer who is responsible for identifying emerging risks to the project?

27. ____ If the project uses subcontractors, does it have a plan for managing each subcontract organization and a single person in charge of each one? (Give the project full score if it doesn't use subcontractors.)

Personnel

28. ____ Does the project team have all the technical expertise needed to complete the project?

29. ____ Does the project team have expertise with the business environment in which the software will operate?

30. ____ Does the project have a technical leader capable of leading the project successfully?

31. ____ Are there enough people to do all the work required?

32. ____ Does everyone work well together?

33. ____ Is each person committed to the project?

Total

_____ *Preliminary score.* Add up the points next to each answer.

_____ *Size multiplier.* Write in 1.5 if the project team has 3 or fewer full-time–equivalent people including developers, quality assurance personnel, and first-level management. Write in 1.25 if it has 4 to 6 full-time–equivalent people. Otherwise, write in 1.0.

_____ *Final score.* Multiply the preliminary score by the size multiplier.

Scoring Guidelines

The table below explains how to interpret the score.

Score	Comments
90+ Outstanding	A project with this score is virtually guaranteed to succeed in all respects, meeting its schedule, budget, quality, and other targets. Such a project is fully "self-actualized."
80–89 Excellent	A project at this level is performing much better than average. Such a project has a high probability of delivering its software close to its schedule, budget, and quality targets.
60–79 Good	A score in this range represents a better-than-average level of software development effectiveness. Such a project stands a fighting chance of meeting either its schedule or its budget target, but it probably won't meet both.
40–59 Fair	A project with this score will likely experience high stress and shaky team dynamics, and the software will ultimately be delivered with less functionality than desired at greater cost and with a longer schedule.
< 40 At Risk	A project with this score has significant weaknesses in the major areas of requirements, planning, project control, risk management, and personnel. The primary concern of a project in this category should be whether it will finish at all.

---

4. AUDITING E - GOVERNANCE

Definition

1 E-governance refers to the delivery of Governmental services electronically - primarily to its citizens and secondly, other clients within the Government. This is a governance process in which Information and Communications Technology (ICT) plays a significant role.

Objectives

2 E-governance seeks to transform the governance process,

- to improve the delivery of services to the citizens
- to empower citizens through access to information and knowledge and enable them to participate in and influence the decisions of the Government, which affect them closely
- to interface with businesses in private and public sector
- to ensure transparency and responsiveness in the functioning of the Government, and
- to enable the Government to work more efficiently and effectively.

3 Many countries have re-engineered their business processes and digitized a number of services that are provided to their citizens. Some of the important areas in this regard are as following:

- E- procurement – Bulgaria, Chile, Korea, Mexico and Philippines
- New business registration – China, Jamaica and Jordan
- Government Online - UAE

4 The Government of India formulated an E-Governance National Action Plan 2003-2007 to give impetus to e-governance to promote long term growth, and facilitate high quality and high speed services to its citizens. Some of the services that are currently being provided by the Central Government/State Governments through electronic means are as follows:

- Land Records –land records are digitized and Record of Right (RoR) of land is issued to the farmers in some States like Andhra Pradesh and Karnataka
- Treasuries – all the transactions taking place at the treasuries are computerised in most of the States
- Agriculture – digital Mandis have been set up and agricultural marketing system has been introduced in Madhya Pradesh
- Reservations – airline and railway reservations are available online
- Payment of Bills – a single window for payment of all utility bills has been provided by the Government of Andhra Pradesh

5 Many other areas like Customs and Central Excise, postal services, registrations, healthcare, entertainment and various other services and administrative

functions of the Government are being automated and information is being provided to the citizens through internet and mobile technologies.

6 The initiatives of both the Central and the States Governments in this regard have posed new challenges to the auditors. We need to understand the working of not just our area of focus, but also the linkages between the different departments involved in e-governance, interfaces between different systems, interaction among different agencies, expectations from different quarters etc. The audit objectives in this regard would be to,

- assess the risk management measures taken by the Government
- evaluate the extent of achievement of the objectives of e-governance projects
- provide constructive and appropriate recommendations to help the Government in doing its job better

7 The audit approach would have to be slightly different since the issues that need to be considered by auditors would be different in this context. Some of the key areas of audit focus with regard to e-governance are detailed below:

8 **Strategic Issues**

- **Vision** – does the Government have an overall vision and road map for the development of e-governance?
- **E-Governance Framework** – is there a proper e-governance framework, covering legislation, regulations, standards and infrastructure for supporting the delivery of e-government services?
- **Delivery Model** – has the Government designed/adapted a model for the delivery of e-government services and transforming the existing method of providing services?
- **Organisational Structure** – has the Government put in place an appropriate organisational framework for planning, implementing and managing e-governance?
- **Digital Divide** – how does the Government plan to tide over the digital divide in the country/State and ensure that every citizen has affordable access to computers and e-enabled services?

Audit Programme 5 : Auditing eGovernance

eGovernance or eGovernment in India have received a major impetus with the National eGovernment Action Plan 2003-2007. The focus of eGovernance has to be on governance rather than on electronics. Audit also needs to undergo a paradigm shift in its field audit procedures. The following checklist can be used as a broad framework in auditing eGovernance projects. Specific checklists for individual projects needs to be developed based on the nature of the project and domain knowledge of auditors in that area.

OPERATIONAL ISSUES	**KD reference**
Detailed plans	
• Has the strategy been translated into business needs and the necessary detailed plans?	
• Have the business processes to be digitised been clearly identified?	
• Are the objectives of e-governance articulated clearly?	
• Was a re-engineering of business processes done?	
• Are priorities determined and targets specified?	
• Are there clearly measurable deliverables?	
• Have the risks been identified, planned for and managed?	
ORGANISATIONAL ISSUES	
• Were appropriate decisions taken relating to organisational issues?	
• What is the extent of involvement of top management/political leadership?	
• Is there a unified direction for e-governance?	
• What is the extent of centralisation?	
• What are the interface requirements between the various governmental agencies/departments?	
• Is a proper project management structure in place for e-governance?	
• Are there clear job descriptions for the personnel and is accountability fixed on individuals for the success of the project?	
• Are the systems interoperable?	

OPERATIONAL ISSUES	**KD reference**
• Is the project scaleable?	
FUNDING	
• Was a cost-benefit analysis done?	
• Was the return on investment measured and monitored?	
• Are funding levels consistent with the objectives of e-governance?	
• Is funding prioritised for projects on the basis of quantifiable performance improvement in services?	
• Is funding adequate for various stages of the e-governance projects?	
IMPLEMENTATION, MANAGEMENT AND COORDINATION	
• What is the extent of coordination between the different Government agencies/departments and is the system managed effectively.	
• Is there centralised procurement?	
• Is there a common decision relating to software licensing?	
• In case of outsourcing, what is the extent of coordination between different agencies/departments?	
• What is the revenue sharing arrangement between the different agencies/departments involved in providing e-governance services?	
TECHNOLOGY RELATED ISSUES	
• **W**as the system planned and developed in a systematic manner taking into account the business and security requirements of the user departments and the ease of use by the citizens?	

OPERATIONAL ISSUES	**KD reference**
• Have the requirements of all the departments concerned been considered?	
• Is there a formal and proper process in place for procuring/developing technical solutions?	
• Are standard products and solutions used where feasible?	
• Is there a middleware in place to connect the front end with the back end systems (possibly legacy systems) in various departments?	
• Has there been adequate capacity planning for the hardware?	
• Is the application software compatible with the back end applications in the departments?	
• Is the system scaleable to include the provision of new services?	
• Is there adequate bandwidth to provide speedy services?	
• What is the periodicity of information updation?	
SECURITY ISSUES	
• Is a risk management methodology followed for identifying and addressing risks?	
• Is security considered at various stages of system design, development and implementation?	
• Are there adequate physical and logical access controls?	
• How secure is the network?	
• Are there firewalls and intrusion detection systems in place?	
• What is the mechanism for identification and authentication of citizens?	

OPERATIONAL ISSUES	**KD reference**
• Can the public view the data/update the data dynamically/transact on-line?	
BUSINESS CONTINUITY PLAN	
• Is there an approved, documented and tested business continuity/disaster recovery plan?	
• What is the timeframe for turnaround after a disaster?	
• What is the security mechanism at the alternate site?	
HUMAN RESOURCES	
• Was the staffing requirement evaluated and provided for?	
• Were the key e-government positions identified, defined and filled?	
• Do the personnel know their responsibilities and are they competent to discharge them?	
• Was there an analysis of the skills requirement of the personnel and was training provided accordingly?	
REVENUE RELATED ISSUES	
• How are the project related costs shared by the various departments?	
• Has there been an increase in the revenue collected by the various agencies/departments due to electronic delivery of services?	
• Has there been a reduction in the time taken to provide services to the public and a corresponding increase in the revenue generation to the Government?	
• What is the mode of sharing of the maintenance expenditure by the various agencies/departments?	

OPERATIONAL ISSUES	**KD reference**
LEGAL ISSUES	
• Is there a legal framework supporting e-governance?	
• Do the e-governance practices comply with legal and statutory requirements?	
• Is the legal standing of electronic transactions/contracts assured?	
• Was the legal liability and exposure to third party agencies considered?	
• Is the legal liability defined and made known to all the parties involved in e-governance?	
CITIZEN AWARENESS AND PREPAREDNESS	
• Are e-governance services available to all the parties and categories of citizens expected to be served?	
• Are citizens and other relevant parties informed about the new delivery methods and the benefits of using them?	
• Did the Government consider and provide easily accessible internet facility to the target groups?	
• Are the e-governance services easy to use and is help readily available?	
• Are customer surveys done periodically to assess the impact and usage of e-services and the need for improvement?	
• Is an awareness campaign carried out to educate and train the citizens and other target groups in electronic communication?	
• What measures are taken by the Government to educate the citizens about the need to participate in decision making process of the Government?	

OPERATIONAL ISSUES	**KD reference**
• What is the extent of public participation in the new measures initiated by the Government?	
• Does the Government conduct periodical surveys to gauge the public perception of the services provided through e-governance system?	
• Are there adequate links provided to other official websites through the e-governance system?	
QUALITY OF SERVICE	
• Has there been an improvement in the quality of service provided by the Government to its citizens?	
• Has there been an improvement in the time taken to provide services to the citizens after the introduction of e-governance system?	
• Has the public perception about the services provided by the Government improved after implementation of e-governance system?	
• Have the number of public grievances/complaints about lack of proper services by the Government been reduced?	
DATA PRIVACY	
• Does the Government have a data privacy policy consistent with the legislative requirements?	
• Is there a proper policy regarding record retention and disposal?	

Audit Programme 6 : Analysing VLC data for audit

Government Accounts form one of the most useful source of audit planning and execution. Government accounts unlike commercial accounting is not based on double entry system of booking. It uses single entry system and is a cash based system. The manual system of accounts had many limitations including non availability of data for quick analysis (eg: DDOwise expenditure figures were difficult to generate in manual system). Voucher Level Computerisation (VLC) transformed the entire system of accounting and audit is one of the greatest beneficiary. Today audit can extract and analyse very useful accounting data quickly over the computers and use it in audit planning and execution. The following checklist lists out some of the dimensions of use of VLC data in audit. Audit offices can innovate and find many other ways of making use of this wealth of information.

I Treasury Accounts Modules

1. Validate Major Heads/Minor Heads/Detailed Heads against master data tables relating to classification of accounts.
2. Validate Treasuries and Treasury codes against master data tables
3. Validate DDOs and DDO codes against master data tables.
4. Profile LOP and Cash Accounts
5. Reconcile amounts as per LOP and Cash Accounts with the amounts as per Schedules, Vouchers and Challans
6. Reconcile amounts as per LOP and Cash Account with Schedules relating to DDR Heads
7. Analyse the Treasury Suspense Account
8. Compare amounts under DAA Suspense with amounts as per LOP and CAS
9. Verify if net payments are calculated correctly (Gross Payments – Deductions)
10. Profile Expenditure
    a. Treasury-wise
    b. DDO-wise
    c. Major Head-wise
    d. Minor Head-wise
    e. Sub Head-wise
11. Profile Expenditure
    a. Charged
    b. Voted
12. Profile Receipts and Expenditure
    a. Plan-wise
    b. Non-Plan-wise
13. Validate Plan/Non-Plan receipts and expenditure items against Master Data Tables
14. Validate Charged/Voted expenditure items against Master Data Tables
15. Identify treasury-wise accounts which are consistently received late
16. Profile Objection Memo to see the extent of missing vouchers
    a. Month-wise
    b. Treasury-wise

   c. Major Head-wise
17. Check the extent of clearance of Objection Book entries
   a. Month-wise
   b. Treasury-wise
   c. Major Head-wise
18. Take a random sample and **manually** identify treasuries where large scale mis-classifications exist
19. Analyse amounts under OB Suspense
20. Review the monthly Broadsheets of OB Suspense, DAA Suspense and Treasury Suspense.

II Compilation Modules

1. Profile Voucher Types
   a. AC/DC Bills
   b. Establishment Bills
   c. Grants-in-Aid
   d. Travelling Allowance
   e. Refund vouchers etc.
2. Apply Benford's Law and analyse voucher amounts
3. Profile and analyse '**Nil**' vouchers
   a. Department-wise
   b. **Manually** check all 'Nil' vouchers above a specific amount
4. Profile and analyse '**Refund**' vouchers
   a. Department-wise
5. Profile and analyse drawal of Contingency Fund department-wise
6. Analyse vouchers with amounts in round figures
7. Analyse the amounts drawn under AC bills
   a. Treasury-wise
   b. DDO-wise
   c. Department-wise
   d. Month-wise
8. Co-relate AC Bills with the corresponding DC Bills and identify the outstanding AC Bills
9. Analyse the percentage of AC Bills against other types of bills
10. Analyse the amounts drawn on AC bills in March – especially on 30th and 31st March
11. Analyse gaps in vouchers/challans
   a. Treasury-wise
   b. Month-wise
12. Compare the DDR Heads payments in the treasuries as per the details given in the accounts bundles (BUNDL_SM table in eastern India) and vouchers
13. Reconcile the amounts in the Departmental Classified Abstract with the initial voucher data
14. Take a random sample and **manually** check the Classified Abstract for discrepancies / mispostings / mis-classifications and minus balances
15. Check if department-wise deductions relating to HBA/MCA etc are reflected properly in Classified/Consolidated Abstract

16. Check if the balances under different heads are carried forward accurately in Consolidated Abstract under both Service Heads as well as DDR Heads
    a. From month-to-month
    b. Year-to-year
17. Check if there are any negative balances in the current month and progressive figures posted in Consolidated Abstract both for Service Heads and DDR Heads
18. Verify if the progressive amount is calculated correctly (Opening Balance + Current Amount) both for Service Heads and DDR Heads
19. Analyse *plus* and *minus* memorandum

III Works and Forest Accounts Modules

1. Validate Forest and PW divisions and their codes against master data tables
2. Identify Forest and PW divisions which have not submitted monthly accounts
3. Reconcile balances relating to Forest and PWD accounts with regard to opening and closing balances
4. Verify opening balances of Forest and PWD accounts of a month with the closing balance of the previous month
5. Verify closing balances of Forest and PWD accounts of a month with the opening balance of the next month
6. Reconcile the cheques drawn by Forest and PW divisions from treasury
7. Reconcile the remittances made by Forest and PW divisions into treasury with cash accounts

IV Account Current Modules

1. Analyse Ways and Means Advances
2. Co-relate the drawal of Ways and Means Advances with the Advice Slips issued by the Account Current Section
3. Analyse Inward/Outward Settlement in Account Current
4. Where accounts are received late, verify if the Inward/Outward Settlement has been done correctly by Account Current Section
5. Analyse the nature and periodicity of items pending settlement in Account Current

V Book Section Modules

1. Check out the TEs and the Heads affected by TEs
2. Verify if adjustments made in TEs are carried out in relevant accounts Heads in monthly balances
3. Where suspense amounts are adjusted, take a random sample and **manually** verify the details of Heads in TE
4. Analyse balances under suspense month-by-month and year-by-year
5. Verify the extent of clearance of suspense amounts at regular intervals
6. Where accounts are received late, see if the adjustments are carried out correctly
7. Analyse the amounts under Suspense Heads and clearance of these Heads

VI Monthly Civil Account Modules

1. Verify if the Abstract of Major Head Totals tallies with the Consolidated Abstracts of Service Heads and DDR Heads

2. Verify if the total figures in the Abstract of Major Head Totals tally with the Statement of Disburser's Account
3. Check if there are any negative balances in the Monthly Civil Account

VII Finance Accounts Modules

1. Analyse Statements of Finance Accounts
2. Compare balances under Receipts Heads in Statement No. 1 of Finance Accounts with the progressive balances figure in March final accounts
3. Compare balances under Expenditure Heads in Statement No. 1 of Finance Accounts with the progressive balances figure in March accounts
4. Compare balances under different Heads in Statement No. 1 of Finance Accounts with the progressive balances figures in March accounts
5. Compare Current Year balances in Statement No. 1 of Finance Accounts with Previous Year's balances
6. Identify Heads in Statement No. 1 of Finance Accounts where the percentage variation between the Current Year's figures and the Previous Year's figures is more than 10 percent
7. Compare figures under Receipts and Expenditure Heads in Statement No. 1 of Finance Accounts with the Budget figures,
    a. Sector-wise
    b. Major Head-wise
    c. Part-wise (Consolidated Fund, Contingency Fund & Public Account)
8. Trace the Receipts from the Government of India as given in Statement No. 1 of Finance Accounts to monthly accounts figures
    a. Taxes
    b. Grants
    c. State Plan Schemes
    d. Central Plan Schemes
    e. Centrally Sponsored Schemes
    f. Non-Plan Grants
9. Compare Capital Outlay on different heads in Statement No.2 of Finance Accounts with the figures given in the monthly accounts
    a. Sector-wise
    b. Major Head-wise
10. Analyse the Debt position of State Government given in Statement No. 4 of Finance Accounts
11. See if the Ways and Means Advances shown in Statement No. 4 of Finance Accounts agrees with the advances taken during the year
12. See the extent of repayment of Loans and Advances by the State Government as given in Statement No. 5 of Finance Accounts
13. Cross-check the cash balances with the Forest & PWD officers as given in Statement No. 7 of Finance Accounts with the figures given in the March accounts
14. Cross-check the debit and credit balances under Consolidated Fund, Contingency Fund & Public Account as given in Statement No. 8 of Finance Accounts with monthly accounts balances
15. Compare the Charged & Voted expenditure as given in Statement No. 10 of Finance Accounts with the monthly accounts balances

16. Check if there are any minus balances in Finance Accounts and see **manually** whether these have been explained in the foot-notes.
17. Verify the balances under Debt, Deposit and Remittance Heads (DDR Heads) at the close of the year and see whether the detailed accounts of the transactions tally with the balances in the ledger.
18. Analyse the trend of the current year vis-à-vis the previous four years in respect of the followings:
    a. Assets and Liabilities
    b. Revenue Receipts
    c. Tax Revenue
    d. Non-Tax Revenue
    e. States share of Union Taxes and Duties and Grants-in-Aid from Central Government
    f. Revenue Expenditure
    g. Sectoral Expenditure
    h. Interest Payment
    i. Loans and Advances given by State Government
    j. Capital Expenditure
    k. Revenue deficit
    l. Fiscal deficit
    m. Internal Debt
    n. Other liabilities
    o. Loans and Advances from Central Government
    p. Ways and Means Advances
19. Analyse investment of cash balances and verify **manually** whether these investments are,
    a. Authorized
    b. Sound and regular and
    c. If the market price of the investment is unstable
20. Take a sample and check **manually** if the Borrowings by the State Government have exceeded the limits fixed by,
    a. Legislature
    b. Parliament
21. Take a sample of the Guarantees given by the State Government with regard to Loans and **manually** check if the conditions attached to the Guarantees are fulfilled.
22. Check if Guarantees are given for Loans raised by Public Bodies or Institutions which exceed the limits fixed by Legislature/Parliament.
23. Take a sample and check **manually** whether the Public Bodies/Institutions given Guarantees, are maintaining proper books of accounts and are subject to audit by qualified auditors.
24. Take a sample and check **manually** whether the Loans given by the Government were expended only on the objects for which the Loans were originally raised/borrowed.
25. Verify the Schedule of Repayment of Loans and identify all the cases where re-payment is due/delayed.

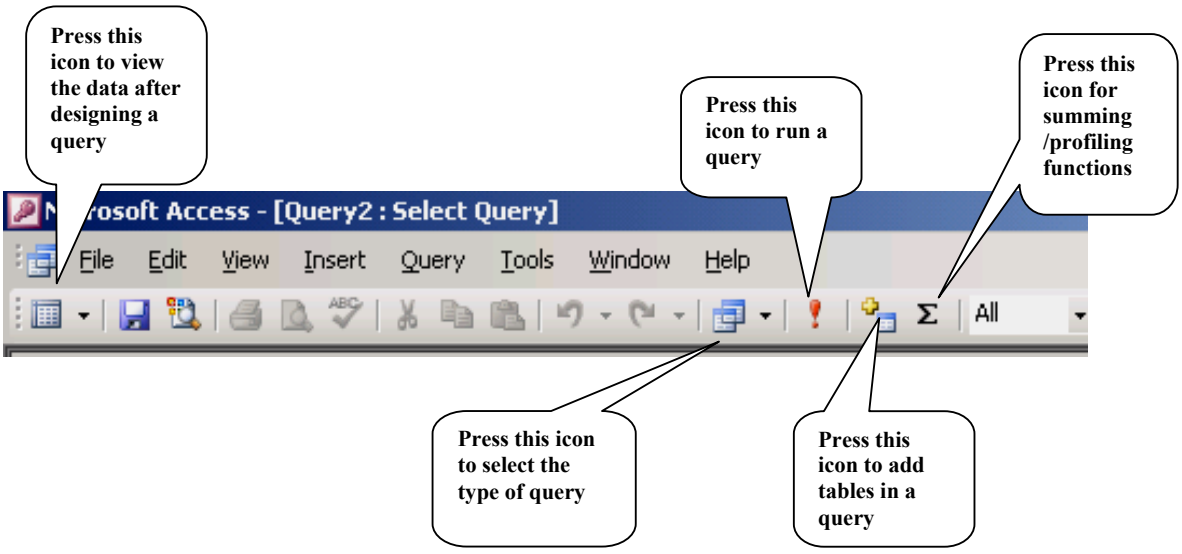
VIII Appropriation Accounts Modules

1. Analyse the Grants / Appropriation of various departments
2. Check if the net appropriations less expenditure equal savings
3. Identify the departments which have received highest Grants and compare **manually** the figures posted in VLC with actual figures in the Budget documents
4. Compare the expenditure figures given in Appropriation Accounts under different Departments with the expenditure shown in monthly accounts balances
5. Identify departments where the variation between the Original and Supplementary Grants is more than 10 percent
6. Identify departments where the variation between the Original Grant and Surrenders is more than 10 percent
7. Identify departments where the Surrenders is more than 50 percent of the Grant
8. Identify departments which have been consistently exceeding Budget allotment
9. Identify departments which have been consistently surrendering significant amounts
10. Analyse expenditure under different Programmes and Schemes and identify cases where expenditure exceeded allotment.
11. Identify Programmes and Schemes where there was no expenditure during the year.
12. Identify Programmes and Schemes where there was heavy expenditure in March
13. Often different names are given for same Schemes or the names of Schemes are not written correctly / fully although the Minor Head and Sub-Head are the same.
    a. Identify all such cases and consolidate them under the correct Head.
    b. Check the expenditure incurred on these schemes with reference to the budget allocation
    c. Identify cases where the expenditure exceeded the budget without the corresponding progress/completion of work
    d. For all such cases identified in (c) above, take a stratified sample and **manually** check the relevant records.
14. Analyse cases where funds could not be spent due to delay in allotment/release of funds/released at the fag end of the year.
15. Compare the total expenditure as per Appropriation Accounts with the expenditure figures shown in Statement No. 10 of Finance Accounts
16. Take a sample and carry out a detailed Appropriation Audit of the excess expenditure by departments over the Grants **manually**.
17. Check whether the re-appropriation orders are issued by the competent authority by taking a sample of the appropriation orders and doing an in-depth **manual** follow up. In this regard, check the following:
    a. Whether the total Grant amount was exceeded?
    b. Whether the funds were expended on New Service or New Instrument of Service?
    c. Whether amounts were transferred from one Grant to another?

d. Whether the classification of the amounts viz. Charged/Voted was done correctly?
e. Whether the classification of the amounts between Plan and Non-Plan Heads has been done correctly?

Running Queries in MS Access to Analyse VLC Data

Some of the important "**ICONS"** in MS Access Queries Module are given below:



Query - 1

Let us join '**Bundl_SM**' table (contains records for each Major Head Bundle corresponding to each of the Treasury Accounts in Jharkhand) and '**MJH_M'** table (Major Head Master) and see if there are any '***Major Head Codes'*** in '**Bundl_SM**' table, that are not available in '**MJH_M**' table.

- Open ***Access***
- Go to ***Queries*** Module
- Select ***New*** on the Menu Bar
- Select ***Design View*** and press **OK**. You will see all the tables available in the database in the Show Table dialog box
- Select **Bundl_SM** and press ***Add*** (You can also double-click the name of the table to select it). You will see the **Bundl_SM** table on the screen
- Next select **MJH_M** and press ***Add***. You will see the **MJH_M** table on the screen

- Press ***Close***
- Click on ***MJH_CD*** in **Bundl_SM** table and pull it over the ***MJH_CD*** in **MJH_M** table. You will see a link / join between the two tables on the field '***MJH_CD'***.

Note: There are three types of joins in Access *viz*.

- An ***inner join***, which is the default join and includes only rows where the joined fields from both tables are equal.
- A ***left outer join*** which includes all records from the first table (in this case, the **Bundl_SM** table) and only those records from the second table (in this case, the **MJH_M** table) where the joined fields are equal.
- A ***right outer join*** which includes all records from the second table (in this case, the **MJH_M** table) and only those records from the first table (in this case, the **Bundl_SM** table) where the joined fields are equal.

- Double click the link between the two tables. You will see a small box containing the **Join Properties**. This box gives the details of the two tables and the columns / fields on which the two tables are joined. Select number **2** from the box, whereby all the records from **Bundl_SM** table will be included and only those records from the **MJH_M** table where the joined field i.e. ***MJH_CD*** are the same.
- Next, place the required fields from the table to the query. For this, hold down the required fields from the **Bundl_SM** table, drag and drop them onto the fields in the **Query Box**. Alternatively, you can also select the required fields from within the query area by pressing on the field.
- Select the required fields from the second table also and ***run*** the query.

Query – 2

Similarly we can validate ***Treasury Codes*** from **BUNDL_SM** against **TR_M** (Treasury Master)

- Open ***Access → Queries → New → Design View***
- In the Show Table box, select **BUNDL_SM** and press ***Add***.
- Select **TR_M** and press ***Add***.
- Close the ***Show Table*** box
- Click on ***TR_CD*** in **Bundl_SM** table and pull it over the ***TR_CD*** in **TR_M** table. You will see a link / join between the two tables on the field '***TR_CD'***
- ***Double click*** the link between the two tables. Select number **2** from the box, whereby all the records from **Bundl_SM** table will be included and only those records from the **TR_M** table where the joined field i.e. ***TR_CD*** are the same.
- Next, place the required fields from the table to the query by dragging and dropping them onto the fields in the **Query Box**.
- Select the required fields from the second table also and ***run*** the query.

Query-3

Validate ***DDO*** (DDO Code) from **TA_15_SM** (contains details of all vouchers and classification) against **DDO_M** (DDO Master).

- Open ***Access → Queries → New → Design View***
- In the Show Table box, select **TA_15_SM** and press ***Add***.
- Select **DDO_M** and press ***Add***.
- Close the ***Show Table*** box
- Click on ***DDO*** in **TA_15_SM** table and pull it over the ***DDO*** in **DDO_M** table. You will see a link / join between the two tables on the field '***DDO'***
- ***Double click*** the link between the two tables. Select number **2** from the box, whereby all the records from **TA_15_SM** table will be included and only those records from the **DDO_M** table where the joined field i.e. DDO are the same.
- Next, place the required fields from the table to the query by dragging and dropping them onto the fields in the **Query Box**.
- Select the required fields from the second table also and ***run*** the query.

Query-4

Profile of ***List of Payments*** (LOP) and ***Cash Accounts*** (CAC) treasury-wise

- Open ***Access → Queries → New → Design View***
- In the ***Show Table*** box, select **BUNDL_SM** and press ***Add***.
- Close the ***Show Table*** box
- Click the Query Type icon and select ***Crosstab Query***
- Drag and drop ***TR_CD***, ***LOP_CAC***, ***G_PAYMT*** on to the Query panel
- Press the Summing Function icon **(∑)**
- Select ***Group By*** under ***TR_CD*** and ***LOP_CAC***
- Select ***Sum*** under ***G_PAYMT***
- In the Query Panel, in ***TR_CD*** field select ***Row Heading*** under Crosstab
- In the Query Panel, in ***LOP_CAC*** field select ***Column Heading*** under Crosstab
- In ***G_PAYMT***, select ***Value*** under Crosstab
- ***Run*** the Query

Query-5

Profile of ***List of Payments*** (LOP) and ***Cash Accounts*** (CAC) for the whole year.

- Open ***Access → Queries → New → Design View***
- In the Show Table box, select **BUNDL_SM** and press **Add →*Close***.
- Drag and drop ***LOP_CAC***, ***G_PAYMT*** from **BUNDL_SM** on to the Query panel
- Press the Summing Function icon **(∑)**

- Select ***Group By*** under ***LOP_CAC***
- Select Sum under ***G_PAYMT***
- Run the Query

These were only a few samples of the basic type of queries that can be run using MS Access. Numerous queries can be run to view, change and analyse data using different parameters as well as use them for forms, reports and data access pages. The results of these queries can also be exported to MS Excel to produce graphs and charts to be included in audit reports.

Bibliography

- Information Systems Audit and Control Association Standards and Guidelines
- INTOSAI IT Audit Courseware, 2001
- National Audit Office, Financial Audit Manual – Module T9 – Audit in an IT environment
- CoBIT.
- IFAC Auditing standards,
- Ron Weber, Information Systems Controls and Audit, Prentice Hall,
- Martin A Krist, Standard for Auditing Computer Applications, Auerbach Publications.
- Federal Information Systems Controls Audit Manual, GAO, 1999
- BS 7799: IT – Code of Practice for Information Security Management,
- Capability Maturity Model (SW) framework of Carnegie Mellon University
- James R Hickman, Practical IT Auditing, Warren, Gorham and Lamont,
- Donald Warren, Lynn Edelson and Xenia Parker, Handbook of IT Auditing, Warren, Gorham and Lamont,
- Doug Dayton, IT Audit Handbook, Prentice Hall,
- Jack Chaplan, Auditing Information Systems, Wiley Publications,
- Donn Barker, Fighting Computer Crime, Wiley Publications,
- System Audit, Dr. M Revathy Sriram
- Treasury Board of Canada Publications

Contributors to the IT Audit Manual :

Subhashini Srinivasan

Vani Sriram CISA, CIA

Rajesh K Goel CISA, CIA

G Srinivas CISA, CIA

Dr Ashutosh Sharma CISA

IT Audit Manual peer reviewed by

Anupam Kulshreshtha CISA, CISM, CIA

N Nagarajan CISA, CISM, CIA

Subir Mallick

A K Ojha CISA

IT Audit Manual preparation support Group

Namashivayam CISA

K P Singh

Murali Krishnan

B J Chanda

S C Naithani