කළමනාකරණ විගණන දෙපාර්තමේන්තුව
முகாமைத்துவக் கணக்காய்வுத் திணைக்களம்
DEPARTMENT OF MANAGEMENT AUDIT

මුදල් හා ක්‍රමසම්පාදන අමාත්‍යාංශය මහලේකම් කාර්යාලය, කොළඹ-01	நிதி, திட்டமிடல் அமைச்சு, செயலகம், கொழும்பு 01	**Ministry of Finance And Planning** **The Secretariat, Colombo 01**

මගේ අංකය எனது இல My No } DMA/2012/01	ඔබේ අංකය உமது இல Your No }	දිනය திகதி Date } 13.01.2012

Management Audit Circular No : DMA/07

To all Secretaries of Ministries and Heads of Department

Guidelines for Internal Auditing in a Computerized Information System (CIS) Environment

The Information and Communication Technology based computer software programmes are being widely used in government ministries, departments and institutions to deliver their services effectively and efficiently. This has been encouraged by the circular instructions issued by the Presidential Secretariat under the guidance of e-Sri Lanka programme. In accordance with such emerging situation, internal auditors in the public sector also should possess some sort of competency to examine the usefulness, accuracy, transparency and value for money (VFM) of such computer programmes. As a result of identification of those requirements, the Department of Management Audit has formulated a set of guidelines and a questionnaire.

02. The guidelines and the questionnaire issued under this circular provide a basic knowledge to conduct internal audit activities in a CIS environment. Public Sector Internal Auditors can develop their annual internal audit plans and programmes by customizing these guidelines according to the requirements of their respective organizations.

03. I wish these guidelines and questionnaire will help to perform the internal audit activities with efficacy in CIS environment.

Wasantha Ekanayake
Director General
Department of Management Audit

Cc -: Auditor General

Guidelines for Internal Auditing in a Computerized Information System (CIS) Environment

1. Introduction

Information Technology has become the most critical factor behind the success of an organization dominating other factors. IT system of an organization defines the system and control of the organization, document flow, information flow and internal auditing process. Hence, as an internal auditor should play a vital role to ensure Accountability and Transparency on the activities taking place in CIS environment. There is no significant change in fundamentals of auditing in a CIS environment but it has directly caused substantial changes in the method of evidence collection and evaluation them. Therefore, it is very essential to upgrade the IT knowledge on software and hardware by the internal auditor to face the rapidly changing CIS environment.

2. National Level IT Policy and Vision in the Country

"The young generation of Sri Lanka needs to be broadly empowered with modern information and communication geochronology. The future market for employment will depend entirely on these skills. For these reasons, our youth will be given more opportunities to improve their knowledge in these areas and information and communication technology will be introduced for accessing all services in the country" (*Mahinda Chinthana 2010,Page 45*)

"To adopt ICT in all its aspects to make government more efficient and effective, improve access to government services, and create a more citizen centric government"
(Vision as mentioned in "e-Governance Policy Document" dated 02.12.2009 developed by ICTA)

3. Legal Environment of Information Governance in Sri Lanka

The internal auditor should have awareness on the following existing legislations, laws, rules and regulations with regard to the information governance in Sri Lanka;

i. Evidence (Special Provision) Act No. 17/1995 – (www.documents.gov.lk)
ii. Information and Communication Technology Act No. 27/ 2003 – (www.documents.gov.lk)
iii. Electronic Transaction Act No. 19/2006 – (www.documents.gov.lk)
iv. Intellectual Property Act No. 36/2007 – (www.documents.gov.lk)
v. Computer Crime Act No. 24/2007 – (www.documents.gov.lk)
vi. Policy and Procedures for ICT Usage in Government (e-Government Policy) – document developed by ICTA in 2009 – (www.icta.lk)
vii. Circular Issued by the President Office on Policy and Procedure for ICT usage in Government (e-Government Policy) - Circular No. SP/SB/03/10 dated 31 May 2010 – (www.icta.lk)
viii. Circular Issued by the President's Office on Implementation of e-Government policy in the Government Organizations - Circular No. SP/SB/06/11 dated 24 June 2011 – (www.icta.lk)

4. Scope of Internal Audit in a CIS Environment

Outcome of computerization on audit approach needs consideration of following factors;

I. **High Speed** – Information can be generated quickly in a CIS environment. Computer system can provide information compiling into complex reports through various formats. This will cut down the time enabling the auditor to extend their analytical review under coverage with high speed of operation and internal auditor has an opportunity to expand his substantive procedure to collect more evidence to ensure his opinion.

II. **Low Clerical Error** – Information which provides by computerized system are all most free from clerical errors.

III. **Concentration of duties** – The internal auditor needs to employ individuals for carrying out the verification process in a manual environment but it can be saved considerable number of labour hours in CIS environment. The traditional audit approaches did not apply in many cases in a CIS environment. Therefore, the internal auditor can spend more time on concentration of duties personally.

Considering the above three main factors, the internal auditor should plan his audit works based on the following aspects;

- **System and Applications** – The main objective of this event is to assess and verify that the systems and applications are appropriate, efficient and such controls lead to ensure valid, reliable timely and secure input, processing and output at all levels of a system's activity
- **Information Processing Facilities** – An audit to assess and verify that the processing activities are controlled to ensure timely, accurate, and efficient processing of systems and applications under planned situation as well as potentially destructive position.
- **Management of Information Technology and institutional Architecture** – An audit to assess and verify that information system management has focused organizational structure and procedures to ensure a system controlled and efficient environment for proper information processing.
- **Systems Development** – An audit to assess and verify that all the system developments should be aligned with the vision and mission of the organization and such developments have to be done in accordance with generally accepted standards for system development.
- **Client/Server Telecommunications Intranets and Extranets**– An audit to assess and verify that the entire mechanism on network connections and servers are properly placed with high security levels.

5. The Internal Auditor should ensure the following attributes on Information as well as the Information system in a CIS environment

I. **Confidentiality**- Confidential information must only be accessed, used, copied, or disclosed by users who have been authorized and only when there is a genuine need. A confidentiality breach occurs when information or information system have been or may have been accessed, used copied, or disclosed by someone who was not authorized to have access to the information.

II. **Integrity** – Integrity means data cannot be created, changed or deleted without proper authorization. It also means that data stored in one part of a database system is in agreement with other related data stored in other part of the database system (or another system). It even refers to the people involved in handling the information, are they acting with proper motivation and integrity.

III. **Availability**- Availability means that the information, the computing systems used to process the information and the security controls used to protect the information are all available and functioning correctly when the information is needed.

IV. **Authentication**- Authentication breach can occur when a user's ID and Password is used by un-authorized users to send un-authorized information.

V. **Non-repudiation**- Non-repudiation implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

VI. **Utility**- It means usefulness and usability of information as well as the information system.

6. Identification of Information Assets

An asset is something that organization values and therefore has to protect. Assets include all the information and supporting items that the organization requires to conduct its activities. Type of information assets are as follows;

I. **Information/Data**

Examples: Databases and data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and information

II. **Software**

Examples: Applications software, system software, development tools and utilities

III. **Hardware/ Physical equipment**

Examples: Processors, monitors, laptops, modems, routers, Fax machines, tapes, disks, power supplies, air conditioning units, furniture and accommodation

IV. **Services**

Examples: Computing and communications services, general utilities

V. **Printed documents**

Examples: Contracts, financial documents

VI. **People and their knowledge**

Examples: Administrators, data entry operators, system designers, users, employees and clients

VII. **Image and reputation**

Examples: Organization's image, brand image and credits

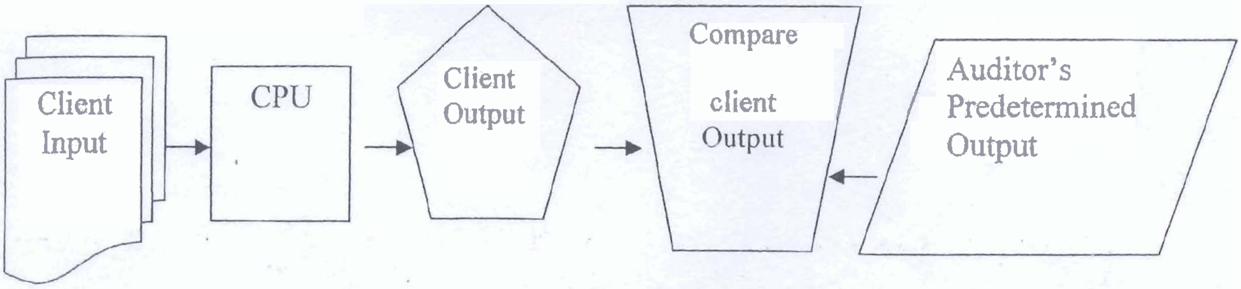
7. Audit Approaches in a CIS environment

There are two main audit approaches in CIS environment, based on the knowledge, skills and expertise of auditors in working with computerized data. Those approaches are as follows;

I. Auditing Around the Computer (Black Box Approach)

II. Auditing through the Computer (White Box Approach)

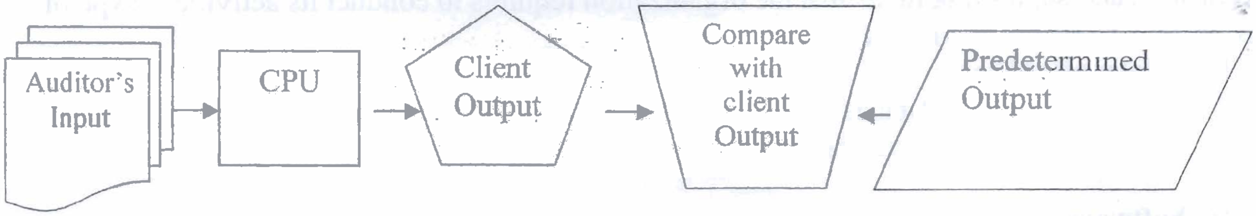
i. Auditing Around the Computer (Black Box Approach)



In this approach, the internal auditor should pay attention on input and output and ignores the specifics of how computer process the data or transactions. If input matches the output, the internal auditor assumes that the processing of transaction or data must have been correct. The comparison of inputs and outputs may be done manually with the assistance of the computer. The information provided by Government Pay-Roll System (GPS) or Computer Integrated

Government Accounting System (CIGAS) can be compared with the input such as monthly changes of salary bill, arrears of salaries, Loan details, vouchers, cash book, vote ledger, etc. In the black box approach, it is not necessary to have an in-depth knowledge and study on application programmes with the internal auditor.

ii. Auditing through the Computer (White Box Approach)



The processes and controls surrounding the subject are not only subject to audit but also the processing controls operating over this process are investigated. In order to help the internal auditor to gain access to these processes computer audit software may be used. In this approach, the internal auditor should have sufficient knowledge of computers to plan direct and review the work performed. The following aspects may typically contain in these packages;

I. Interactive enquiry facilities to interrogate files

II. Facilities to analyze computer security logs for unusual usage of the computer.

III. The ability to compare source and object (compiled) programme codes in order to detect dissimilates

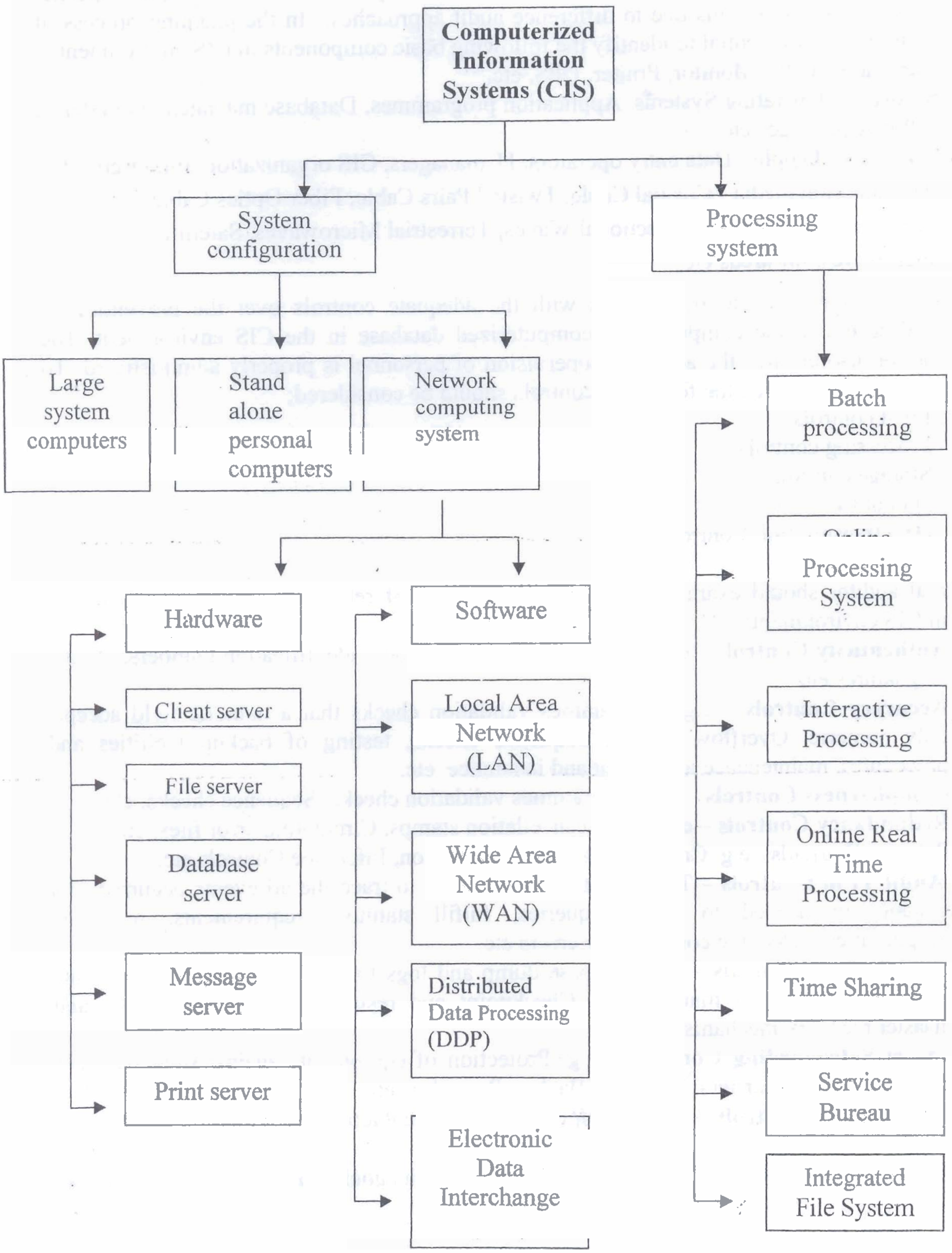
IV. The facility to exclude and observe the computer treatment of "live transaction" by moving through the processing as it occurs.

V. The generation of test data

VI. The generation of aids showing the logs of application programmes. The actual controls and the higher level control will be evaluated and then subjected to compliance testing and, if necessary, substantive testing before an audit report is produced.

8. Types of Computerized Information Systems (CIS)

Based on the nature and size of CIS, it can be classified as follows;



9. Identification of Internal Control Systems in a CIS Environment

The internal auditor should obtain an understanding of internal control systems in the CIS environment to plan the audit and develop the audit procedures to carryout the internal audit functions efficiently and effectively. The internal control systems in CIS are quite specific comparing with manual systems due to difference audit approaches. In the planning process of internal audit, it is very essential to identify the following basic components in CIS environment;

- Hardware – CPU, Monitor, Printer, UPS, etc.
- Software – Operating Systems, Application programmes, Database management systems, software packages etc.
  Live ware / People - Data entry operators, IT managers, CIS organization, End users, etc.
- Transmission media - Coaxial Cable, Twisted Pairs Cable, Fiber Optics Cable, Directional waves, Omni directional Waves, Terrestrial Microwaves, Satellite microwaves, Infrareds etc.

The internal auditor needs to be satisfied with the adequate controls over the prevention of unauthorized access to the computer and computerized database in the CIS environment. The internal auditor also ensures the adequate supervision of personnel is properly administrated. To plan the internal audit works, the following controls should be considered;

i. Input controls
ii. Processing controls
iii. Storage controls
iv. Output Controls
v. Data transmission Controls

The internal auditor should examine and evaluate the level of reliability on following internal controls in CIS environment;

I. **Authenticity Controls** – e.g. Password controls, Personal identification numbers, Digital signatures etc.
II. **Accuracy Controls** – e.g. Programmes validation checks that a numeric field accepts only numeric, Overflow checks, Sequence checks, testing of backup facilities and procedures, maintenance agreement and insurance etc.
III. **Completeness Controls** – e.g. Programmes validation checks, Sequence checks, etc.
IV. **Redundancy Controls** – e.g. Batch cancellation stamps, Circulating error files, etc.
V. **Privacy Controls** - e.g. Cryptograph, Data compaction, Inference Controls etc.
VI. **Audit Trail Controls** – These controls which help to trace the all events occurred in a system are needed to answer queries, fulfill statutory requirements, minimize irregularities, detect the consequence errors etc.
VII. **Existence Controls** – e.g. Database dump and logs for recovery purposes duplicate hardware, Preventive maintenance, Checkpoint and restart controls, Emergency and disaster recovery mechanism etc.
VIII. **Asset Safeguarding Controls** – e.g. Protection of equipments against fire and other hazards, Physical barriers, Libraries, Backup Procedure etc.
IX. **Effectiveness Controls** – e.g. Monitoring of user satisfaction, Post audit, Periodic cost benefit analysis etc.
X. **Efficiency Controls** – These controls help to achieve its goals using minimum resources.

10. Matters to be considered to Audit in a CIS environment

The approach to auditing in a CIS environment provides for the following;

I. Skills, qualifications and competence

The internal auditor should have appropriate knowledge and competence of planning the audit works in computer based environment and implementation and evaluation of such audit programmes. Therefore, the internal auditor needs to develop IT knowledge and skills in his career path. Such knowledge and skills will help;

- To plan the internal audit activities in computerized information system properly.
- To design the internal audit tests and investigations and to implement them
- To assess and review the financial and internal controls in a computer base environment
- To identify the risk areas behind the systems, applications, hardware and controls of the CIS.
- To review the security measures of the CIS

If the internal auditor does not have sufficient knowledge and skills to conduct an audit in CIS environment, then necessary actions have to be taken to obtain the assistance from an expert or expert group approaching outsourcers.

II. Internal Audit Planning

In the audit planning process, the auditor should obtain an understanding of components such as the significance and complexity of the CIS activities, the availability of the data for use in the audit, accounting and internal control systems which help to determine the nature, time and extent of the audit procedures.

This understanding would include matters such as;

- Infrastructure of the CIS – Hardware, software, live ware and Transmission media
- The significance and complexity of computer processing in each significant accounting application. Significance relates to materiality of the financial statement assertions affected by the computer processing.
- The organizational structure of the client's CIS activities and the extent of concentration or distribution of computer processing throughout the entity, particularly as they may affect segregation of duties.
- The internal auditor needs to determine extent of availability of data by reference to source documents, computer files and other matters with regard to evidence. Most of time the CIS provides reports which might be useful in performing substantive tests.

III. Risk Involved in a CIS

It is very essential to assess whether it may influence the assessment of inherent and control risks when the CIS is significant.

The nature of the risks and the internal control systems in CIS environment include the following;

- **Lack of Transaction Trails** - Some CIS are designed so that a complete transaction trail that is useful for audit purposes might exist for only a short period of time or only in computer-readable form. Where a complex application system performs a large number of processing steps, there may not be a complete trail. Accordingly, errors embedded in an application's program logic may be difficult to detect on a timely basis by manual (user) procedures.

- **Uniform Processing of Transactions** – Computer programmes processing transactions uniformly, virtually eliminating the occurrence of clerical errors. Nevertheless, all transactions will be processed incorrectly due to such programming errors.
- **Lack of Segregation of Functions** – Many controls become concentrated in a CIS environment allowing data processing of incompatible functions.
- **Potential for errors and irregularities** – The potential for human error in the development, maintenance and execution of CIS may be greater than in manual systems, because of the level of detail inherent in these activities.
- **Initiation or Execution of Transaction** – In a CIS process certain types of transactions are initiated by the system, the authorization for which may not be documented as in manual system. In such cases, management; authorization of these transactions may be implicit.
- **Dependence of Other Controls over Computer Processing** – Certain manual control procedures are dependent on computer generated reports and outputs for their effectiveness. Therefore, the effectiveness and consistency of transaction processing controls are dependent on the effectiveness of general CIS controls.
- **Increased Management Supervision** – Information provided by CIS can offer management different type of analytical tools which can enhance the effectiveness of the entire internal control structure.
- **Use of Computer-Assisted Audit Techniques (CAAT)** – The internal auditor can apply general or specialized computer audit techniques and tools in the execution of audit tests.

IV. Risk Assessment

The internal auditor should make an assessment of inherent and control risks for material financial statement assertions.

Risk can be generated from deficiencies in;

- Programme development and maintenance
- System software support
- Operations
- Physical CIS security
- Control over access to specialized utility programmes

As new CIS technologies are emerging for data processing and clients are adopting the same for building complex computer systems, these may increase risk which needs further consideration.

V. Documentation

The internal auditor should prepare the annual internal audit plan according to the DMA circular No. 2009/01 and 2009/03 considering the nature, timing and extent of audit procedures performed and the conclusions drawn from the evidence obtained. Most of internal audit evidence in CIS environment is in electronic form. The internal auditor should satisfy himself that such evidence is sufficiently and safely stored and is retrievable in its entirely as and when required.

11. Internal Auditors Involvement in the Clients System Development and Documentation Control

Internal Auditor should be consulted while designing appropriate controls over the development of computerized system within an institution. Such collaborative association may help the internal auditors in suggesting preventive and corrective actions for the betterment of the system and also internal functions.

Examples: The internal auditor of the Ministry or Department may involve in the event such as;

a. System modification and application of new version of CIGAS Programme
b. System modification and application of new version of GPS Programme
c. Designing and developing a specific (Client based) CIS for the organization as a project

The major functions may be described as analysis of the system involves identification understanding and critically examining the system and its inter-related sub systems. For the purpose of achieving the goals and objectives set for the CIS in macro level, through modification, changed inter-relationship of components, deleting or merging or separating or break-up of component. They may also involve upgrading the system as a whole. In this event, the internal auditor should request to create system generated audit files for the internal audit purposes from the system designers.

Therefore, the internal auditor should play a significant role in the process of designing, developing and implementing a new CIS for the organization involving into the various stages of such project.

12. Type of Internal Audits in CIS environment

Based on the purpose and objectives of the assignment, internal audits in CIS environment can be categorized as follows;

i. Operational Computer System/ Network Audits
ii. IT Installation Audits
iii. System Development Audits
iv. IT Management Audits
v. IT Process Audit
vi. Change Management Audits
vii. IT Legal Compliance Audits
viii. IT Strategy Audit
ix. Special Investigations under CIS environment
x. Information Security and Control Audits

13. Internal Audit Procedures in CIS Environment

The internal auditor should design the internal audit procedures in order to reduce the audit risk to an acceptably low level considering the "Risk Assessment and Internal Controls" in CIS environment as mentioned in the above.

The auditor's specific audit objectives do not change whether accounting data is processed manually or by computer. However, the methods of applying audit procedures to gather evidence may be influenced by the methods of computer processing. The auditor can use either manual audit procedures, computer-assisted audit techniques (CAAT), or a combination of both to obtain sufficient evidential matter. However, in some CIS that use a computer for processing significant applications, it may be difficult or impossible for the auditor to obtain certain data for inspection, inquiry, or confirmation without computer assistance.

Examples;

(a) ASYCUDA system in Sri Lanka Customs
(b) Postal Money Transfer System in Postal Department
(c) Computerized Travel Document Model in Department of Immigration and Emigration
(d) Treasury Operation Manager (TOM) in the Department of Treasury Operations
(e) Treasury Consolidated Accounting System in Department of State Accounts

Internal Audit Questionnaire to Assess the CIS of the Organization and its Effectiveness and Efficiency

(This is a specimen questionnaire form. Therefore, this should be customized according to your organizational requirements)

1. Legal Background, Policies and Practices

No.	Question	yes	No	Not Applicable	Responsible Officer	Remarks
1.1	Is there a specific IT policy for the organization and is it updated based on the current requirements?					
1.2	Has the above IT policy been developed according to the Govt. IT policy at the national level? (As mentioned in above Para. 02)					
1.3	Is the IT policy of the organization documented?					
1.4	Has the management responsibility been linked with the IT policy of the organization?					
1.5	Have an annual ICT plan for the organization?					
1.6	Has the strategic plan/corporate plan /action plan been prepared according to the IT policy of the organization?					
1.7	Have the performance indicators been developed to measure the progress of IT developments of the organization?					
1.8	Has Individual performance been linked with the objectives of IT development?					

2. CIS of the Organization

No.	Question	yes	No	Not Applicable	Responsible Officer	Remarks
2.1	Has the relevant legal authority been granted for the CIS of the organization?					
2.2	Does the internal auditor satisfy with "Value For Money" (VFM) of the CIS?					
2.3	Is the CIS a configuration system?					
2.3.1	Is the CIS a large computer system?					
2.3.2	Is the CIS a personal computer system?					
2.3.3	Is the CIS a network computing system?					

2.3.3.1	Is the CIS a LAN system?					
2.3.3.2	Is the CIS a WAN system?					
2.3.3.3	Is the CIS a DDP system?					
2.3.3.4	Is the CIS an EDI system?					
2.3.3.5	Is the CIS a mix system with above?					
2.4	Is the CIS a processing system?					
2.4.1	Is the CIS an online processing system?					
2.4.2	Is the CIS a batch processing system?					
2.4.3	Is the CIS an interactive processing system?					
2.4.4	Is the CIS an online real time processing system?					
2.4.5	Is the CIS a time sharing processing system?					
2.4.6	Is the CIS a service bureau processing system?					
2.4.7	Is the CIS an integrated file system?					
2.5	Is a specific operating manual available for the CIS?					
2.6	Does the internal auditor satisfy with the internal controls in the CIS?					
2.7	Does the internal auditor satisfy with the authenticity controls such as security levels/password levels, digital signatures of the CIS?					
2.8	Does the internal auditor satisfy with the management responsibility on the CIS?					
2.9	Does the internal auditor satisfy with the security measures on the CIS? (Virus guards, Information hacking, unauthorized access to the system, Information/data distortion)					
2.10	Are there any facilities to upgrade the system according to the future developments and changes?					
2.11	Are audit files auto generated through the system?					
2.12	Does the internal auditor regularly review the audit files generated through the CIS?					
2.13	Does the internal auditor satisfy with the user-friendliness of the CIS					

3. **Safeguarding of Assets in the CIS**

No.	Question	yes	No	Not Applicable	Responsible Officer	Remarks
3.1	Is a separate fixed assets register maintained for IT devices by the organization? (According to the Treasury circular No. IAI -2002-02 dated 28.11.2002)					
3.2	Are the all computer devices and supporting accessories such as UPS, power cables, pen drives, speakers included in the fixed assets register?					
3.3	Have a specific fixed asset coding system to identify the hardware of the system in the organization?					
3.4	Is the custody of the hardware of the system assigned to the responsible officers?					
3.5	Is the fixed assets register maintained to separately identify the assets purchased by various funding agencies (Source of Financing)?					
3.6	Does the internal auditor satisfy with the existing physical security controls on computer hardware of the organization?					
3.7	Have maintenance agreements been signed for the all important computer devices?					
3.8	Are the facilities provided during the warranty period of the computer hardware enjoyed properly?					
3.9	Does the internal auditor satisfy with the activities of board of survey regarding computer devices?					
3.10	Are there enough controls on assets such as Laptops, Pen-drives etc. which are allocated for officers' personally use? (Easy identification of assets and location and proper handing-over of the such assets when they leave from the organization)					
3.11	Does the internal auditor satisfy with internal controls on assets relating to wireless technologies such as WAP, GPRS, BLUETOOTH, WIFI, CDMA, WIMAX, and HSPA?					

4. Safeguarding and Security Controls on Software in the CIS

No.	Question	yes	No	Not Applicable	Responsible Officer	Remarks
4.1	Are readymade software such as operating systems (Windows, Apple), application packages (MS office, Open office), security packages (Virus guards) and other software used in the organization?					
4.1.1	Are they licensed software?					
4.1.2	Are they auto updated online?					
4.1.3	Are they compatible with the organizational software (client based)?					
4.1.4	Is there a facility for future IT developments?					
4.1.5	Are there sufficient internal controls with regard to the safeguard of software CDs, pen drives, diskettes, tapes and soft and hard copy of user guides and system changes manuals?					
4.2	Are the specific organizational software (client based software) used for the organization?					
4.2.1	Have a proper authenticity for such software?					
4.2.2	Are there user manuals for such software?					
4.2.3	Are there specific system flowcharts for such software?					
4.2.4	Are they compatible with the commonly used operating systems and application packages?					
4.2.5	Is the ownership of the source codes of the system belonged to the organization?					
4.2.6	Is the ownership of the source codes of the system kept under the custody of third party?					
4.2.7	Does the internal auditor satisfy with the arrangements on event of system breakdown and interruptions?					
4.2.8	Is there a specific system maintenance agreement with the relevant party?					

4.2.9	Does the internal auditor satisfy with the authenticity controls such as security levels/password levels, digital signatures of the CIS?					
4.2.10	Does the system provide the reports and applications in three official languages in the event of using the information and the system by general public?					
4.3	Have the all software (readymade and client based) properly included in the fixed assets register?					

5. General Matters

No.	Question	yes	No	Not Applicable	Responsible Officer	Remarks
5.1	Is there a separate IT unit for the organization?					
5.2	Is there a separate IT organizational structure for the organization?					
5.3	Are the operating manuals and system development manuals available in the organization?					
5.4	Does the internal auditor satisfy that all programme changes are adequately tested and documented?					
5.5	Does the internal auditor satisfy with the delegation of authority considering the internal controls in the IT division?					
5.6	Does the internal auditor involve in the event of development of a CIS?					
5.7	Does the internal auditor satisfy with the involvement of other interested parties such as system analysts, programmers, external auditors, user departments and other responsible officers in the stage of developing a new CIS?					
5.8	Does the internal auditor satisfy with the Transparency and Accountability of the CIS?					
5.9	Does the internal auditor satisfy with the reliability and accuracy of data and information provided by the CIS?					
5.10	Is there a trend to use the					

	UNICODES introduced by the government?					
5.11	Doest the internal auditor satisfy with result of input/output ratio of IT projects under the concept of Value For Money (VFM) audit?					
5.12	Does the internal auditor satisfy with the adequacy of training facilities provided to the IT staff to perform their duties effectively and efficiently?					
5.13	Does the internal auditor clearly identify the risk areas in the CIS?					
5.14	Is there a disaster recovery plan for CIS?					
5.15	Does the internal auditor satisfy with the existing disaster recovery plan?					
5.16	Does the management update the disaster recovery plan time to time?					