APPENDIX I

GENERIC CRITICALITY ASSESSMENT CHECKLIST

Key to the checklist:

d. Weights have to be allocated to the Criteria question by the SAI. If required, the SAI may assign weights in consultation with the entity.If no weight have to be assigned, the SAI could give equal weight to all criteira questions, i.e., 1.
e. Figures in parenthesis are indicative scores for the responses.The scores indicated are between 1 to 5 with 1 indicating least risk area and 5 as high risk area. SAIs can adopt different scores as relevant to their scenario.
f. The criteria questions are not exhaustive. The SAIs can select criteria questions from the below table or develop criteria questions as per their requirement.
g. The information for the checklist should be collected for all organisations to be audited by the SAI. SAIs may endeavour to collect as much information as possible to make the scoring and comparisions relevant.
h. The SAI may decide to keep the scores and ranking confidential or share it with stakeholders as per their policy.

I. Name of IT System and Organisation:

	CRITERIA	WEIGHT	SCORE
	IT Governance		
1	**General state of computerisation in the entity. The entity has computerized**		
	All the business processes (5)		
	Most of the Business processes (4)		
	Only a few processes (3)		
	No business process (1)		
2	**The entity has an IT and related policies**		
	Yes (1)		
	Partially (3)		
	No (5)		
3	**The entity has**		
	Separate IT wing (2)		
	Has outsourced some IT functions (5)		
	Has outsourced IT facilities (5)		
4	**The entity has a**		
	Chief Information Officer (CIO) in charge of activities related to IT (1)		

	CRITERIA	WEIGHT	SCORE
	The entity has a sufficiently senior official in charge of activities related to IT in addition to his responsibilities (3)		
	Entity has a subordinate official in charge of activities related to IT (3)		
	The entity has no one designated to attend to activities related to IT (5)		
	Development, Acquisition and Outsourcing		
5	**The system was developed**		
	In-house with sufficient in house capacity (1)		
	In-house with insufficient in house capacity (5)		
	By a contractor/other Governmental agency (4)		
	A mix of in-house and outsource development (5)		
6	**The acquisition was made**		
	By the entity itself with sufficient capacity to make IT acquisitions (3)		
	By the entity itself with insufficient capacity to make IT acquisitions (5)		
	By utilising services of a consultant (4)		
7	**System documentation is**		
	Available (1)		
	Partially available (3)		
	Not available (5)		
8	**How often changes are made/warranted to the applications**		
	More than five times in a year (5)		
	Less than five times in a year and more than twice in a year (3)		
	Less than twice in a year (2)		
	Not even once in a year (1)		
	IT Operations and IS Security		
9	**Number of access points/ transaction locations/ users**		
	More than Y (5)		
	More than X, less than Y and more such levels, if required (3)		
	Less than X (1)		
	(Numbers X and Y to be decided by the SAI)		
10	**Network based system**		
	No network (1)		
	Local Area Network (LAN) (3)		
	Wide Area Network (WAN) (4)		
	Web based (5)		
11	**Number of locations** *(Threshold/Numbers for locations as X and Y to be decided by the SAI)*		
	Only one location (1)		
	More than one, less than X locations (3)		
	More than X locations (5)		
12	**Does the system make use of direct links to third parties e.g. EDI**		

	CRITERIA	WEIGHT	SCORE
	Yes (5)		
	No (1)		
13	**Number of end-users of the system** *(Threshold/Numbers for end-users X and Y to be decided by the SAI)*		
	Less than X (1)		
	More than X, less than Y and more such levels if required (3)		
	More than Y (5)		
14	**Does the entity maintain the data and application**		
	In house (1)		
	Partially in house and on outsourced facilities (3)		
	Hosted on outsourced facilities (5)		
15	**The system has been in operation for**		
	More than 10 years (1)		
	Between 5 and 10 years		
	Between 2 and 5 years		
	Less than 2 years (5)		
16	**Volume of data in the system is approximately (including offline data)**		
	More than 10 GB (5)		
	Between 2 GB and 10 GB		
	Less than 2 GB (1)		
	Financial Exposure		
17	**Investment made in the System** *(Threshold/Amounts $x and $Y levels to be decided by the SAI)*		
	Above $Y (5)		
	More than $X, Less than $Y (and more such levels, if required) (3)		
	Below $X (1)		
18	**Mode of financing of the system**		
	From internal resources (3)		
	From borrowings (4)		
	From loans from international organizations (5)		
19	**Recurring expenses on the system** *(Threshold/Amounts $x and $Y levels to be decided by the SAI)*		
	Above $Y (5)		
	More than $X, Less than $Y (and more such levels, if required) (3)		
	Below $X (1)		
	Functional Exposure / Usability of the System		
20	**The system is used for**		
	internal processes only (3)		
	external processes only (4)		
	Both internal and external processes (5)		
21	**Does the system provide citizen services?**		

	CRITERIA	WEIGHT	SCORE
	Yes (5)		
	No (3)		
	Internal control and Audit Assurances		
22	**Has a third party certification of the system been done**		
	Yes (1)		
	No (5)		
23	**Has the system been audited by IT Auditors of SAI**		
	3 years back (2)		
	5 years back (4)		
	Never (5)		
24	**Have other audit (financial/ compliance/ performance related) observations been made in previous audits**		
	Several recurring audit observations (5)		
	Few recurring audit observations (3)		
	No recurring audit observations (1)		
The list is not exhaustive. SAIs can identify their own such criterion over and above the list given above.			
	Total Score		

II. Ranking of IT Systems

Having completed the Criticality Assessment Checklist above, the IT Auditor can use the table below to summarize their assessment of the IT systems within the audit entity. This can be done by using the total scores generated from the checklist and deriving a category of risk (as per section III below) as well as a corresponding ranking.

Name of IT System	Total Score	Category of Risk	Rank

III. Category of Risk

Priority of IT System	Total Score Range*
A	L1-L2
B	>L2 and <L3
C	>L3 and <L4
D	> L4

*L1, L2, L3, L4 are score ranges to be decided by SAI to categorise the IT Systems

The above framework thus provides for categorising the IT systems and also ranking them for prioritising for audits. Category 'A' being the lowest risk, and category 'D' being the highest risk categories, respectively.

APPENDIX II

SUGGESTED MATRIX FOR AUDIT OF IT GOVERNANCE

Business Needs Identification, Direction & Monitoring	
Audit objective: Assess whether the organisation's leadership effectively directs, evaluates and monitors IT use in the organisation in order to fulfil the organisation's mission.	
AUDIT Issue 1: Defining IT requirements **How does the organisation identify and approve business and IT requirements?**	
Criteria: The organisation has a plan on how it identifies emerging business or IT needs and the Steering Committee approving requirements has sufficient information to make their decisions.	
Information Required	**Analysis Method(s)**
Requirements management process	Review of documents to ensure that new business requirements are identified and analysed according to the organisation's requirements management process.
Steering committee charter and operating principles including approval and rejection thresholds	Review of approved or rejected requirements to ensure that these are in accordance with accepted operating principles.
List of approved and rejected requirement	Interview management or others responsible for approving projects to ensure that they take into account the IT organisation's capabilities, skills, resources, and training, and the ability of the users to utilise the new tools and methods or procedures.
AUDIT Issue 2: Leadership **How does the leadership direct and monitor the performance of business and IT objectives on a periodic basis?**	
Criteria: Performance measures are established and the steering or equivalent high level committee conducts periodic reviews and meetings and takes appropriate action, or there is a reporting system to management that informs them of the status of key performance measures.	
Information Required	**Analysis Method(s)**
Performance measures for business and IT	Review sample management decision or memos to ensure that they are clear, well substantiated, and unaambiguous.
Periodic reports about project status	Review performance measures to ensure that they cover both business and IT systems.
Minutes from periodic reviews	Review project status reports (or other documentation that has the status of the project (meeting minutes, emails, etc.)) to ensure that it contains cost, schedule and performance indicators and variations from plan.
List of action items and their status etc	Review management actions items to ensure that they are assigned and tracked to closure and include lessons learned.
AUDIT Issue 3: IT Investments **How does the organisation manage IT investments?**	
Information Required	**Analysis Method(s)**
Investment management plan and procedures	Interview management to determine the organisation's investment management procedures.

Portfolio of IT projects Sample cost benefit analysis reports List of approved and rejected or deferred projects Project status reports for approved projects Sample post project evaluation reports	Review portfolio to assess whether projects have been prioritised according to approved criteria. Review status reports to see they provide cost and schedule tracking Review cost benefit analysis reports to assess that they are complete, reflect actual conditions and do not overstate the benefits or understate cost or schedule (utilise specialist services of economists or cost experts as needed). For projects in trouble, determine whether their methodology was suitable to the type of project and properly applied, and whether QA has been involved during the life cycle. Interview management to determine whether any projects have been terminated due to underachieving benefits or performance. Interview management to determine how the organisation makes decisions on building vs. acquiring (buying) solutions (for example, based on capability, skills, cost, risk, etc.).
Audit Conclusion: To be filled in by auditor	

IT Strategy

Audit objective: Confirm whether there is an IT strategy in place, including an IT plan and the processes for the strategy's development, approval, and implementation and maintenance which is aligned with the organisation's strategies and objectives. The risks and resources while accomplishing IT objectives are effectively managed.

AUDIT Issue 4: Quality of IT strategy

Does the organisation have an IT Strategy that serves to guide its IT functions?

Criteria:

An organisational-level IT strategic plan exists, it translates business objectives into IT goals and requirements, addresses the needed IT resources to support the business, and it is reviewed and updated periodically.

Information Required	Analysis Method(s)
IT Strategic Plan, or equivalent document Meeting minutes from IT and Organisation's Steering committee meetings.	Review of document. Interview business owners to determine if their needs are met by the IT organisation. Review periodic IT Committee and Organisational Steering Committee meeting minutes to ensure that business owners are represented and that strategic IT decisions are made at the Steering Committee level. Review the IT Strategy or interview management to determine resources' requirements and how they are determined and approved, who approves appropriate acquisition of tools and other resources (staff, contractors, skill via training, etc).

AUDIT Issue 5: Risk management

How does the organisation manage their risks?

Criteria

The organisation has a risk management policy and plan, and has assigned sufficient resources to identify and manage risks.

Information Required	Analysis Method(s)
Risk management plan List of risks (including IT) and mitigation strategies	Review risk management plan or other document to ensure that risk management responsibilities are clearly and unambiguously assigned. Review of documents to determine whether IT risks are part of the overall governance risk and compliance (GRC) framework.

Minutes of periodic risk assessment or other meeting if available.	Review meeting minutes to ensure that new risks are added and analysed as appropriate. Interview personnel responsible for risk management to determine whether the risks to be mitigated have appropriate cost estimates, and resources are allocated. Interview management or review minutes of meeting to determine that leadership is aware of both IT and other risks and monitors their status on a periodic basis.
Audit Conclusion: To be filled in by auditor	

Organisational Structures, Policy, & Procedures	
Audit objective: Ensure that there are organisational structures, policy, and procedures in place that enable the organisation to meet its mandate for business goals.	
AUDIT Issue 6: **Does the structure of the IT Organisation enable it to meet its IT Goals and business needs?**	
Criteria: The IT Organisation is positioned at a sufficiently high level within the organisation and its roles and responsibilities are clearly defined including those of the Chief Information Officer (CIO) or equivalent.	
Information Required	**Analysis Method(s)**
Overall organisation chart IT Organisational chart.	Review organisational charts to determine that the IT organisation is positioned at a strategic level (for example, there is a CIO who reports to or is a member of the Steering Committee). Review the IT organisation chart to determine that it is aligned to support the business (has a help desk, data base managers, maintenance personnel or contactors who help and facilitate IT operations).
AUDIT Issue 7: Policy and procedures **Has the organisation approved and is it using appropriate policies and procedures to guide its business and IT operations?**	
Criteria: The organisation documents, approves, and communicates appropriate policies and procedures to guide the business and IT operations in order to meet its mandate.	
Information Required	**Analysis Method(s)**
Organisational policies regarding: Human Resources including hiring and termination security, document retention, contracting and/or outsourcing, software development and/or acquisition, etc. Procedures for the selected policy areas Emails or other ways policy is communicated to appropriate users and stakeholders QA reports to management reporting on periodic policy and procedures compliance and other issues	Review policies to ensure they are approved and current. For example, review the Human Resources policy to determine that skill requirements are defined, and training is identified for new and other staff. Review initial and refresher training materials or other internal processes through which these policies and procedures are communicated within the organisation. Interview members of the quality assurance or other group that is responsible for enforcing policy's to see what they do to ensure compliance. Interview QA or compliance staff to determine how and when they report their results to senior management. Interview personnel responsible for compliance of policies and procedures to determine how often they report the results to senior management and how they solicit input on non-compliance anonymously or independently. Interview managers and users to understand their perception and attitude to the analysed policies and procedures. In case of frequent opinion: "Procedures are to complex" ask what and how they could be simplified. Review policy change control history to determine that policies are updated periodically or as needed.

Request changes to policy and or periodic review and results.	Review QA reports to ensure that they contain any policy or procedure compliance issues as appropriate. Review emails or other mechanisms (physical mail, training, etc) to ensure that policies are distributed to appropriate users and stakeholders when updated or on an as-needed basis. Review policies to determine adequacy by looking for (as an example): • Scope of policy and mandate. • Definition of roles and responsibilities. • Required resources and tools. • Linkage to procedures. • Rules to deal with non-compliance.
Audit Conclusion: To be filled in by auditor	

People & Resources

Audit objective: To assess whether sufficiently qualified/trained personnel are employed and that they have access to suitable resources that enable the organisation to met its business goals.

AUDIT Issue 8: HR and logistics

How does the organisation deal with meeting current and future people and resource requirements?

Criteria:

The organisation should have a plan to meet its current and future requirements for meeting business needs.

Information Required	**Analysis Method(s)**
Organisational policies regarding: Human Resources & Training IT Strategy or Strategic Plan Hiring & Training Plans.	Review policies to ensure they are approved and current. Review policies to ensure they require various groups (IT, quality assurance (QA), Business Users) to identify their current and future needs for personnel and resources. Review hiring and training plans to ensure that they reflect identified needs. For example, review the Human Resources policy to determine that skill requirements are defined, and training is identified for new and other staff. Interview HR or business managers to assess how they ensure critical positions are staffed during contingencies or extended absences. Review initial and refresher training materials or other internal processes through which these policies and procedures are communicated within the organisation. Review the IT Strategic plan to ensure that it contains people and resource requirements for current and future needs.

Audit Conclusion:

To be filled in by auditor

Risk Assessment and Compliance mechanisms

AUDIT Issue 9: Mechanism

How does the organisation ensure that it has an adequate and working compliance mechanism to ensure all policies and procedures are being followed?

Criteria:

The organisation has a mechanism (via a QA group, internal audit, or spot check, etc.) to ensure that all policies and procedures are being followed.

Information Required	Analysis Method(s)
Organisational policies & procedures (Security, SDLC, Training, etc) Organisation Chart Quality Assurance Plan Reports from compliance teams or groups Steering Committee Minutes	Select a sample of policies and organisational procedures to assess compliance. Interview management to determine who is responsible for ensuring compliance to the (audit selected) policies and associated procedures. Interview team or group responsible for compliance of above to determine how they accomplish their duties. Review reports from various compliance groups to see what they found, what actions they have taken and reported to management. Review steering committee minutes to see if high level compliance issues are discussed at this or at other meetings. Interview author(s) to determine reason for update to existing policies or procedures. Review past non-compliance issues and resolutions. Review training or other dissemination mechanisms (email, memo, notice) to see if non-compliance issues were addressed.
Audit Conclusion: To be filled in by auditor	
See Appendix III and Appendix IV respectively for audit matrices on Development and Acquisition and IT Operations	

APPENDIX III

SUGGESTED MATRIX FOR AUDIT OF DEVELOPMENT & ACQUISITION

<table>
<tr><th colspan="2">Requirements Development & Management</th></tr>
<tr><td colspan="2">Audit objective: Assess how the organisation identifies, prioritises and manages their requirements for IT systems.</td></tr>
<tr><td colspan="2">AUDIT Issue 1:
How does the organisation identify user requirements for IT Systems?</td></tr>
<tr><td colspan="2">Criteria:
The organisation has a plan or procedures on how to collect, review, and catalog requirements for new or added functionality</td></tr>
<tr><td>Information Required</td><td>Analysis Method(s)</td></tr>
<tr><td>Requirements' management plan or procedure

Sample user submitted requirements

Sample initial review</td><td>Review the requirements' management plan or procedures to ensure users, stakeholders, or other relevant users are involved in identifying requirements.

In a major functionality enhancement development, user consultation and prototype development can be implemented in parallel. The information interchange between the business process owners and vendor/ IT organisation needs to be looked into.

Review sample requirements to ensure that there is an initial review, and that similar or duplicate requirements are grouped.</td></tr>
<tr><td colspan="2">AUDIT Issue 2:
How does the organisation analyse, prioritise, and manage user requirements?</td></tr>
<tr><td colspan="2">Criteria:
The organisation analyses, prioritises, and manages requirements to ensure that user needs are met in an optimum and cost effective manner</td></tr>
<tr><td>Information Required</td><td>Analysis Method(s)</td></tr>
<tr><td>List of requirements

Sample analysis of requirements

Requirements traceability matrix

Criteria for priority of requirements</td><td>Review requirements to determine that they include author, date, priority, cost, risk, and other elements.

Review analysis of requirements or comments on requirements by business owners or stakeholders to determine that all views are solicited and summarised for appropriate analysis (accept, defer, reject, etc.) taken.

Review traceability matrix to determine that approved requirements are assigned to either development or acquisition projects, and are tracked to closure when implemented.

Review criteria for requirements priority to assess whether they include elements such as cost, business need, emergency issues, and new mandates.</td></tr>
<tr><td colspan="2">Audit Conclusion:
To be filled in by auditor</td></tr>
</table>

Project Management & Control

Audit objective: Assess how the organisation manages and controls the development or acquisition of approved IT projects.

AUDIT Issue 3:
How does the organisation plan for the development or acquisition of IT projects?

Criteria:
The organisation has a project management plan or equivalent for each approved project that guides its execution

Information Required	Analysis Method(s)
Project management plan or equivalent	Review the requirements' management plan or equivalent to ensure that it contains the project description, scope, cost, schedule, risks, management structure and that it identifies stakeholders (internal or external). Review the plan to ensure that it has been approved by senior management and incorporates comments by stakeholder. Review the project's organisational chart to determine the roles of individuals who are responsible for quality assurance or testing, development, and installation of the system on organisations IT infrastructure, support group, etc. For acquisition projects, ensure that the plan or equivalent list of those who will be responsible for oversight of the contractor exists and review approvals given by responsible persons. Interview project managers to determine which SDLC method is being used for the development of the project.

AUDIT Issue 4:
How does the organisation control IT projects?

Criteria:
The organisation controls and tracks projects to ensure they meet their cost, schedule, and performance requirements.

Information Required	Analysis Method(s)
Project cost and schedule baselines	Compare project cost and schedule baselines with project status reports to assess deviations.
Project status reports Contractor status reports, SLA Results of reviews Action items	Interview project manager / review reports to determine whether appropriate corrective action was taken for major deviations. Interview project management team and review minutes of meetings with contractor to assess the frequency and effectiveness of monitoring the outsourced project activities. Review contractor SLA or contract to ensure that they are following the terms of the contract, for example, look for contractors conducting periodic reviews, providing status reports, tracking action items, conducting risk management activities in accordance to the contract. Interview contract officer at the organisation to determine how it manages the contractor if SLAs are not available.

Quality Assurance & Testing

Audit objective: Assess how the organisation ensures that IT projects under development or acquisition meet their quality goals.

AUDIT Issue 5:
Does the organisation have a quality assurance organisation and are their roles and responsibilities defined?

Criteria:
An established procedure for conducting quality assurance activities.

Information Required	Analysis Method(s)
Quality assurance policy or plan Quality assurance procedures Roles and responsibilities of the Quality Assurance group or individual(s) Quality assurance reports Project adopted SDLC	Review the quality assurance policy and/or plan to determine what group or individuals is responsible for conducting quality assurance activities for the project (for example, the Quality Assurance group should review documents to ensure they accurately reflect the requirements, review user manuals to ensure they are legible and do not contain missing elements or steps). Review the quality assurance procedures or interview quality assurance personnel to determine what activities they conduct (observe peer reviews, sit in on design or other reviews, etc.). Review reports from the quality assurance organisation to determine what they observed (whether the project team is following its project management plan, and the adopted SDLC and associated reviews etc.) to whom are issues reported.
AUDIT Issue 6: **How does the organisation plan for and conduct testing on IT systems?**	
Criteria: The organisation conducts test on IT systems and based on the results accepts or rejects the system.	
Information Required	**Analysis Method(s)**
Test plan Test schedule Test results Accept or reject criteria	Review test plans. Compare project cost and schedule baselines with project status reports to assess deviations, if any. Interview project manager / review reports to determine whether appropriate corrective action was taken for major deviations. Interview project management team and review minutes of meetings with contractor to assess the frequency and effectiveness of monitoring the outsourced project activities. Review contractor SLA or contract to ensure that they are following the terms of the contract, for example look for contractors conducting periodic reviews, providing status reports, tracking action items, conducting risk management activities in accordance to the contract. Interview contract officer at the organisation to determine how it manages the contractor if SLAs are not available.
Audit Conclusion: To be filled in by auditor.	

Solicitation
Audit objective: Assess how the organisation ensures that solicitation activities (set of tasks such as firming up the needs document, framing RFP, evaluating proposals, conducting pre-bid clarifications, designing and floating tender, evaluation, etc leading up to the award contract) are conducted in accordance with its adopted solicitation plan or procedure.
AUDIT Issue 7: **What is the plan or procedure for the conduct of solicitation activities?**
Criteria: Solicitation activities including vendor selection are conducted in accordance with the organisation's solicitation plan

Information Required	Analysis Method(s)
Solicitation plan or procedure Solicitation package User review of requirements User review of solicitation package Applicable laws that govern the conduct of solicitation.	Review the solicitation plan to ensure it covers areas such as user involvement, getting bids on a competitive basis, conducting market research prior to contract on areas as applicable, and that vendor selection is based on objective criteria. Interview key contracting personnel to assess how they ensure that the solicitation package is complete (for example, by getting users, stakeholders, experts as appropriate to review it). Interview users or business owners to ensure that they were consulted during the generation of requirements or approved the technical requirements of the solicitation and / or the final bid package. Interview contracting officer(s) to assess how they ensure that the solicitation process follows applicable laws and regulations.
AUDIT Issue 8: **What criteria does the organisation use in selecting a vendor?**	
Criteria: The organisation uses objective and published criteria for vendor selection for each.	
Information Required	**Analysis Method(s)**
Vendor selection criteria Vendors scoring matrix or equivalent.	Review the vendor selection criteria to ensure that it reflects the intent of the solicitation (for example, on a software contract, vendor selection should not include parameters not critical to the organisation). Interview key stakeholders to assess if they agree with the selection criteria. Review vendor scoring matrix or equivalent to confirm it is consistent with the selection criteria.
Audit Conclusion: To be filled in by auditor	

Configuration Management	
Audit objective: Assess how the organisation manages configurations of work products related to development and acquisition.	
AUDIT Issue 9: **What policy does the organisation use for configuration management?**	
Criteria: Configuration management activities are conducted according to the organisational policy or procedure.	
Information Required	**Analysis Method(s)**
Configuration management policy or procedures or equivalent.	Review the configuration management policy for adequacy by looking for (as an example): Scope of policy and mandate Definition of roles and responsibilities Required resources and tools Linkage to procedures Rules to deal with non-compliance. Interview personnel responsible for configuration management if there is no policy to assess how they ensure that their duties are uniformly carried out for the organisation.

AUDIT Issue 10: **What group or individual(s) are responsible for authorising changes and for final installation into the production environment?**	
Criteria: Only authorised and approved changes should be introduced into the production environment.	
Information Required	**Analysis Method(s)**
Group or individual responsible for authorising changes	Ensure that a group exists that authorises changes to the work product(s). The group could be the change control board or equivalent that reviews and approves changes.
Process for approval and introducing approved and tested changes to the production environment.	Interview personnel responsible for authorising introducing new software to the production environment to ensure that software has been tested (including regression testing with other systems if needed) meets the acceptance criteria, has appropriate documentation, and includes user training (if appropriate) prior to being introduced for business. Interview personnel responsible for authorising changes to the production system to determine how they control and prevent unauthorised changes to the system (for example, by controlling access to the production system, separating the production and development environments, etc.).
Audit Conclusion: To be filled in by auditor	

APPENDIX IV

SUGGESTED MATRIX FOR AUDIT OF IT OPERATIONS

<table>
<tr><th colspan="2">Service Management</th></tr>
<tr><td colspan="2">Audit Objective: To assess whether the IT organisation is actively monitoring IT operations against agreed-to internal Service Level Agreement or contract.</td></tr>
<tr><td colspan="2">Audit issue 1: Key parameters
What baseline service metrics are covered by the internal SLA between the business and the IT organisation?</td></tr>
<tr><td colspan="2">Criteria:
SLA Best practices – allocation of responsibilities between the business process owners and the IT support group, documented network management business objectives, service offerings and metrics, definition for problem types, help desk responsibilities.</td></tr>
<tr><td>Information Required
Entity's internal SLA between business owners and IT organisation.
• Help desk responsibilities
• Service reports generated
• User/ application response time.</td><td>Analysis methods
Review the SLA to find whether it contains appropriate elements – detailed and measurable service level objectives, systems and services covered, quality of service (QoS), services not covered, application level support and troubleshooting, system availability, help desk hours, response and resolution time dependent on severity classification of a problem, throughput, maintenance schedules etc.
Check whether data back-up and recovery practices are consistent with the entity's BCP standards.
Check if the Business Process Owners have signed on the agreement.
Interview sample of users to understand the level of awareness.</td></tr>
<tr><td colspan="2">Audit issue 2: Compliance
What mechanisms are in place to ensure that the SLA is adhered to consistently?</td></tr>
<tr><td colspan="2">Criteria:
SLA implemented, monitored and amended where necessary.</td></tr>
<tr><td>Information Required
The SLA parameters
Reporting timelines
Charts or graphs that show the success or failure of how these agreements are met over time
Periodic meeting documents that reviews the analysis of the baseline and trends</td><td>Analysis methods
Review the reports that the IT Organisation generates daily or over any other time interval. Check if all the indicators agreed upon are being monitored through the reports/trend graphs etc.
Review reports to examine what metrics are measured and reported to the management periodically.
Review documents to check whether the helpdesk activity reports are considered by the management and compared to resolution requests, and critical issues are noted for buying decisions and for periodic review of the SLA itself.
Interview IT organisation personnel and examine the nature of supervision of help desk personnel, the monitoring tools used, the support task prioritisation, gathering of baseline for network and application, data on response time, frequency of back-ups, testing of backed up data to verify compliance with SLA requirements.</td></tr>
</table>

Operational parameters - defect rates, help desk requests, other communication trails, response time, Time to implement new functionality, change documentation, serviced locations andincentive and penalty clauses (especially important if IT support services are outsourced).	Check what actions are taken by the IT unit, or in the case of an outsourced IT support group – by the organisation's management – if operational parameters are not in agreement with SLA requirements.
Audit issue 3: Effectiveness Does the management of IT services ensure satisfaction of business users and help meet business objectives of the organisation?	
Criteria: achievement of performance metrics that are aligned to business needs and goals.	
Information Required	**Analysis methods**
Help desk reports minutes of meetings between business stakeholders and IT organisation Agenda items for SLA review cycles.	Interview a sample of business users (at various levels) or conduct a satisfaction survey about the quality of services by the help desk and IT support group. Review help desk reports to check whether a significant proportion of critical service issues were prevented before being reported by users. Check whether the resolution time for reported issues was less than the parameters set in the SLA. Check whether SLA parameters were being reviewed by management periodically and examine QoS issues.
Audit Conclusion: To be filled in by auditor	

Capacity Management

Audit Objective: Assess whether the IT organisation is ensuring that the system capacity and performance meets current and future business needs.	
Audit issue 4: Agreement on parameters Is there a documented agreement between the business and IT organisation that is used as the basis for selecting operational parameters for IT operations?	
Criteria: IT governance – track and monitor strategy implementation in terms of measurable metrics.	
Information Required	**Analysis methods**
Internal SLA, or other form of agreement IT operational parameters – processing resource availability, average system login time, % downtime, average system response time, etc.	Review the agreement or operating guidance that the IT group is using. Ensure that it is has been reviewed and signed by the relevant business users or senior executive management. Compare performance baseline parameters (viz. network resource availability, host response time) set by IT organisation with the Operating guidance set by Business process owners to verify that the IT organisation follows the operating guidance.

Audit issue 5: Monitoring Does the IT organisation collect and review system performance data on a real time/periodic basis for better alignment with business needs?	
Criteria: best practices by system/network administrators including performance base lining, collection of traffic and configuration information, system resource availability, observe traffic stats and trends, what-if analyses, and use of tools to pinpoint causes of performance deterioration.	
Information Required	**Analysis methods**
Reports, action items, help desk response time, and other metrics.	Use Compliance issue in SLA matrix. Pay special attention to all elements having impact on capacity, i.e. compare actual capacity metrics to the SLA requirements, etc.
Audit issue 6: Performance data analysis Is the performance data analysed and tuned for efficiency gains and avoidance of capacity constraints? If needed, has the IT organisation planned for and acquired additional resources to meet business needs? Does the IT organisation hire, train, or contract for staff as the business needs change?	
Criteria: parameters set in the agreement/operation guidebest practices in performance tuning (memory, optimisation of network response time, OS, I/O; efficient design of database schema, scheduling tasks according to priority and resource requirement, upgrade or tuning procedures set up to handle capacity issues on both a reactive and long-term basis).	
Information Required	**Analysis methods**
Reports, actions, status reports, performance metric graphs Minutes of meeting at the apex IT organisation level.	Review the reports that the IT Organisation generates daily or at other chosen time frame, look to see if it generates and analyses trend data, identifies bottlenecks to look for action items, and exception reporting for capacity issues. Compare to SLA requirements. Compare reports/trend patterns to verify procedural actions taken in response to the reports. Review minutes of meetings and find whether IT staffing issues, capacity problems and any additional resource needs are discussed and highlighted at the right time.
Audit Conclusion: To be filled in by auditor	

Problem & Incident Management	
Audit Objective: To evaluate the effectiveness of organisation's problem and incident management policies and procedures.	
Audit issue 7: Policy awareness Is there a documented incident response policy and are the business users aware of it?	
Criteria: Best practices in incident response.	
Information Required	**Analysis methods**
Entity's incident response policy Guidelines for communicating with outside parties regarding incidents.	Review the policy to find whether it contains appropriate stages – preparation, detection and analysis, containment and eradication, post-incident activity. Does type of activity depend on high incidence or level of incidents? Verify whether the policy assigns responsibility, scope and reporting requirements. Review the actual procedures by which the business users are made aware of the policy, and the nature of communication between the incidents response team and the business stakeholders. Interview a sample of business users across the organisation to get an assurance about the awareness of the incident response plan.

Audit issue 8: Skills set and resources Is there an adequately skilled incident response team with proper tools, resources and higher management support to handle incidents?	
Criteria: Incidents response best practices, NIST guidelines, as laid down in SLA	
Information required	**Analysis methods**
Incident response policy and plan Charter of the incident response team, composition and expertise SLA Incident response awareness training, upgrade strategy for skillsets of IRT staff List of logging tools and applications used for network monitoring and usage.	Look at whether the team has a charter to investigate incidents. Look for expertise in networks, operating systems, and security in the team members and how they conduct their work. Review the service desk procedures to check whether escalation procedures are laid down for incidents that cannot be resolved immediately in accordance to risk categories defined in the SLA. Review what actions have been taken in response to past incidents. Review case report(s) to check whether appropriate personnel were involved in investigating incidents. Check what incident management tools are being used – are they relevant for the organisation's needs? Verify whether the organisation has established logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.
Audit issue 9: Effectiveness of response Does the incidence response strategy result in effective response to incidents?	
Criteria: Incidents response best practices (COBIT 5 DSS domain, ITIL on Service support)	
Information required	**Analysis Methods**
Incident response action items, forms logs, etc. Periodic security awareness training Incident handling procedures – guidelines for prioritising incidents Case reports and action taken.	Check if an incident response/handling priority is assigned to each asset or service. Verify whether procedures provide for the capture and analysis of volatile[50] and static data in a timely manner. Verify whether the response team periodically makes users aware of policies and procedures regarding appropriate use of networks, systems, external media and applications. Review documents to find whether post-incident activities such as refresher training has been given to user groups to avoid costly recurrence of significant incidents. Look for whether source of incident was identified. Look for action taken. (Procedure change, reprimand, training, etc.). Check whether the incident response team records all resolved incidents in detail and review the information for possible update in the knowledge base.
Audit Conclusion: To be filled in by auditor	

[50] Volatile data are data that are overwritten or changed over time, where a snapshot cannot be obtained without capturing the information interactively, or by regularly scheduled data extracts.

Change Management

Audit Objective: Assess whether the entity has implemented a standardised procedure for controlling all changes to the core IT systems and applications.

Audit issue 10: Policy

Does the organisation have an approved Change management policy that contains the appropriate controls throughout the change cycle?

Criteria:

Best practices in change controls: Request for change- authentication- acceptance- prioritisation - change design -testing change- implementation- documentation

Information required	Analysis methods
Change management policy and procedures, process flow diagrams	Refer to general requirements for policy and procedures in IT Governance section.
Change control board charter	Review the change management policy document to verify whether procedures for initiation, review and approval of change are laid out along with mapping of responsibility for these tasks.
Timeline of policy review	Review the change control board charter to identify the allocation of responsibilities and responsibility levels.
Change documentation: Change request, Change control testing procedures, quality assurance plan, test plan & procedures	Interview personnel, observe actual practices and review documents to obtain assurance that change management procedures are followed: ask to see a change, trace change to operational environment, see that requisite procedures – e.g. management review and prioritisation – were followed, look for approvals and documentation.
Change Management software reports and logs	Look to see if internal QA has done an audit. Review if adequate review of logs and reports are done by the management where a change management software is used.
Minutes of meeting of the change control board	Ensure that the access to production source library (e.g. Source code, configurations) is limited to CM staff, and the IT organisation is preventing unauthorised changes to the operational environment.
Change management summary reports considered by the management.	Review documents, observe practices to ensure that business users are associated during testing of changes to ensure correctness.
	Ensure that program changes have appropriate sign-off by relevant business stakeholder before moving into production.

Audit issue 11: Fallback procedures

How does the IT organisation ensure that the organisation can revert back to a previous version if needed?

Criteria:

Change Management best practices – documentation on procedures and responsibilities for recovery of affected areas due to undesirable change impact.

Information Required	Analysis methods
Change management procedures	Review documentation, interview business users to find if unintended impacts of functionality changes/ enhancements have been addressed on priority, in line with business interests.
Documentation on change tests and implementation	
Recovery documentation and configuration change logs	
Back-up and restore procedures	

Audit Issue 12: Emergency changes Are emergency changes controlled adequately when established change management procedures for defining, authorising, testing and documenting of changes cannot be followed?	
Information required	**Analysis Methods**
Emergency change control procedures Documentation of emergency changes that have been made during the audited period	Review the change management procedures to identify whether they contain a dedicated section and set of procedures to control emergency changes to the system. Ask for an example of an emergency change. Compare against documented procedure. Look for what testing was done prior to introduction into production environment. If documented procedure does not exist, ask how it knows what to do and who approves such changes. Examine whether emergency changes are approved by an appropriate member of the management before moving into production.
Audit Issue 13: Change closure and documentation Are there appropriate processes followed for the update of associated systems and user documentation after a change is implemented?	
Criteria: Change management best practices (e.g. COBIT 5-BAI domain, ITIL on Service support).	
Information required	**Analysis methods**
Process documentation of functionalities affected by change Established procedures for documentation.	Review documents to ensure comprehensiveness and consistency of changes implemented. Did operational procedures, configuration information, application documentation, help screens and training materials follow the same change management procedure, and were they considered to be an integral part of the change. Examine whether there is an appropriate retention period for change documentation and pre- and post-change system and user documentation. Examine what mechanisms exist to update business processes for changes in hardware or software to ensure that new or improved functionality is used.
Audit Conclusion: To be filled in by auditor	

APPENDIX V

SUGGESTED MATRIX FOR AUDIT OF OUTSOURCING

Outsourcing Policy	
Audit objective: To assess whether the agency has an adequate policy on outsourcing.	
AUDIT Issue 1: Key Elements of Outsourcing Policy Does the organisation have a policy on outsourcing?	
Criteria: Organisational policy on outsourcing	
Information Required	**Analysis Method(s)**
Policy Document Approval process for outsourcing of a function/ service List of outsourced functions/ services List of outsourced functions/ services with partial outsourcing Mode of service by the service provider Cost-benefit analysis on outsourcing of a function/ service List of outsourced service providers with locations Approval related documents for outsourced functions/ services Strategy to ensure continuity in case of takeover of the service provider by another organisation Information on any takeover of the service provider Monitoring documents/ reports.	Review policy to ensure it is approved. Review policy to check (for example) it contains information about organisation assets that can be outsourced or not, identifies the list of services/ functions that it may outsource. Review acquisition or outsourcing approval documents to ensure senior management are involved in the approval. Document review to assess that the organisation has identified the risks associated with respect to different modes of outsourcing and locations of outsourced service provider. Document review to verify whether the organisation is aware of risks associated with possibility of takeover of the service provider. Document review to verify whether the organisation has ensured that the business continuity, data rights, security, ownership and cost are embedded in the service agreement covering the case of takeover. Document review to assess that the policy includes identification of monitoring parameters for the outsourced functions and requires them to be included in the outsource agreement.
Audit Conclusion: To be filled in by auditor	

Solicitation
Audit objective: To assess whether the agency has a policy on how to manage solicitation.
AUDIT Issue2: Policy and Process of Solicitation • Does the organisation have a policy on acquisition? • Does the organisation have a definite process for identification and selection of the service provider? • Does the organisation have a process to ensure inclusion of user requirements into the Service Level Requirements/ contractual requirements? • Are the related decisions taken at appropriate levels?
Criteria: Provisions of organisation policy on Outsourcing and policy on IT services procurement dealing with solicitation and acquisition.

Information Required	Analysis Method(s)
Acquisition or equivalent Policy List of laws regulating the acquisition and outsourcing Selection process for identification and selection of a service provider List of outsourced functions/ services along with the service provider User requirements for the contracted or outsourced service Contract/ Service Level Agreement Approval related documents for selection of service provider.	Document review to assess that the organisation has a policy on solicitation or acquisition. Review policy to ensure it contains provisions for data requests from sub-contractors if the prime contractor has included sub-contractors as part of the proposal. Document review to assess that the policy on solicitation and acquisition complies to the laws on outsourcing and acquisition (review that it references to provides links to applicable laws and regulations) Review of selection process for compliance to the policy for each a sampling of contracts or outsourced service (review that the selection process is transparent, has objective criteria, the selection team is comprised of personnel who understand the requirements, is represented by contractual and legal personnel, and consult with users as appropriate for clarification). Ensure that the contractual requirements have been approved by users and relevant stakeholders. Meet with the contractual office to ensure that an appropriate level of management approved the solicitation and contract.
Audit Conclusion: To be filled in by auditor	

Vendor or Contractor Monitoring

Audit objective: To assess whether the organisation is managing the contractor or vendor and takes appropriate action when performance or quality deviates from established baselines.

AUDIT Issue3: Vendor Management

- Is there a contract with the service provider?
- Are Service Levels identified and agreed through a Service Level Agreement?
- Is there a monitoring arrangement (for services) with the service provider?
- Are the service levels ensured through this arrangement?
- Is appropriate action taken when service level agreement provisions are not met?

Criteria:

Provisions/ parameters defined in Service Level Agreement and the follow up actions by the organisation.

Information Required	Analysis Method(s)
Contract/ Service Level Agreement Approved schedules, baselines, cost and other technical parameters that define the product or service being acquired or outsourced Monitoring documents/ reports / meeting minutes of reviews conducted, action items, direction to vendor (task orders, statement of work, etc.) Impact assessment of deviations Action items or direction to vendor Action taken reports on deviations from service levels.	Document review to assess if a service level agreement has been established. Review of monitoring reports submitted by the contractor to ensure that they contain elements that are in the contract or SLA (cost, schedule, performance, risk, status, issues, and status of past action items or tasks). Review of monitoring reports to identify service deficiency/ deviation and assessment of impact due to the deficiencies/ deviations. Review of notices and action-taken reports for action taken to be commensurate with impact on business and contractual provisions.
Audit Conclusion: To be filled in by auditor	

Data Rights

Audit objective: To assess whether the organisation's data protection requirements are identified, and that they are part of the contractual requirements.

AUDIT Issue 4: Data protection and management of data

- Are the data protection and access rights built into the service contract?
- Is the data defined appropriately to cover the transaction data as well as the programs/ software supporting the data, as the case may be?
- Is there a mechanism to ensure that the data protection and security requirements as per the Service Level Agreement are being adopted and implemented by the service provider?

Criteria

Organisation's data protection and access rights requirements are levied on the contractor as appropriate.

Information Required	Analysis Method(s)
Organisation's Data Protection and access rights requirements	Document review on adequacy of data protection and access rights requirements/ definition of data.
Definition of data (for protection and access rights)	Document review of the contract with service provider to check for incorporation of Data Protection and access rights requirements.
Contract with the service provider	Document review of third party/ self audit reports.
List of data access records from the service provider	Document review of the monitoring reports, correspondence and incident handling reports to assess the follow-up activities by the organisation.
Reports of third party audits or self audits with recommendations and follow up on them	Review of the non-disclosure agreement to verify that all relevant information is covered.
Monitoring reports	Verify if the disclosure of information by outsourced agency is authorised.
Correspondence with the service provider on the subject	
Incident handling reports	
Non disclosure agreement with the outsourced agency	
List of information disclosed by the outsourced agency to third party / unrelated party(s).	

Audit Conclusion:

To be filled in by auditor

Overseas Service Provider

Audit objective: To determine if the organisation has strategy on contracting services to overseas vendors.

AUDIT Issue 5: Management of vendor who is overseas

Whether the organisation understands the issues involved in outsourcing to overseas agencies while outsourcing to overseas agencies?

Criteria:

Provisions of outsourcing policy related to outsourcing to overseas agencies.

Laws of land regulating business with overseas agencies.

Information Required	Analysis Method(s)
List of laws and regulations related to outsourcing services	Document Review to assess that the organisation has identified risks related to outsourcing to overseas service provider.
Information on any in-country presence of the service provider	Document review to assess the cost benefit analysis addressed the risks related to outsourcing to overseas service provider.
List of foreign offices of the organisation	Document review to assess that adequate background check on the service provider has been carried out.
List of laws and regulations regulating the service provider in their country	
Bilateral agreement between the country of organisation and the service provider facilitating outsourcing agreements	

Reports on vendor's past performance on delivery times and quality issues in Cost benefit analysis of indigenous and overseas service provider Outsourcing contract and Service Level Agreement Information on escrow amount/ financial guarantee related to performance List of deviations from the Service Level Agreement and outsourcing contract Monitoring and follow up reports on action taken on deviations by the service provider.	Document review to assess that a robust system is in place to ensure performance on Service Level Agreement and outsourcing contract. Document review to assess that any deviations from Service Level Agreement and the contract are followed up in a timely manner ensuring minimum downtime and loss to the organisation.
Audit Conclusion: To be filled in by auditor	

Retaining Business Knowledge/ Ownership of business process

Audit objective: To assess whether the agency retains business knowledge and ownership of business process(es).

AUDIT Issue 6: Policy on ownership of business knowledge and processes

- Is the business process ownership well delineated and documented?
- Is it ensured that the loss of business knowledge due to outsourcing does not occur?
- Is there capacity to conduct the outsourced services in house?
- Can business continuity be ensured if the vendor was unable to provide services at any point/ in future?

Criteria:

Organisations retain business knowledge and are able to continue operations in-house for mission critical function if contractors or vendors are unable to provide the service.

Retention of business process ownership.

Retention of business knowledge.

Performance vis a vis business continuity with respect to the service provider failing to provide service at any point.

Information Required	Analysis Method(s)
Identification of business processes, and critical skills that need to be retained in-house Documentation of business processes Detailed system design document of outsourced service with the organisation List of training of staff on the business processes, system design, data, application software Incident reports/ correspondence related to stoppage of service/ dispute with the service provider, including those related to ownership of system/ data Meeting minutes with contractor.	Document review to assess that the ownership of the process, data and application software is retained by the organisation through adequate provisions in the contract. Document review to assess that the business knowledge in terms of data, application software, system design are well documented and that the staff is updated with these periodically through training etc. Document review to assess that the organisation and its staff are involved in any system updates carried out by the outsourced agency and the detailed system update documentation is provided to the organisation. Document review to assess that there are no incidents or disputes with the service provider with respect to ownership of system and data. Review meeting minutes with the contractor to ensure that if there are any high level risks they are jointly managed and tracked to ensure continuity of operations.
Audit Conclusion: To be filled in by auditor	

Cost control and management

Audit objective: To assess whether the organisation has ensured most economical cost through the life cycle of the outsourced contract.

AUDIT Issue7: Cost benefit Assessment

- Have all the costs (including future costs) for outsourcing been identified?
- Has due cost-benefit analysis been carried out and best option been chosen?
- Are there specific responsibilities on the organisation in the outsourcing, and do they have critical cost elements/ impacts built in?
- Are additional costs or escalated costs being charged to the agency?

Criteria:

The cost benefit analysis is realistic and is the basis on which the programme is managed and controlled.

Information Required	Analysis Method(s)
Initial cost benefit analysis	Document review to assess that all costs have been identified by the organisation, reviewed and approved by relevant stakeholders.
Estimated cost of outsourced contract	Document review of the selection and approval process.
Selection process of the service provider vis a vis cost element	Document review to assess that all costs are reflected in the contract and that there are no hidden costs including any future costs.
Approval process documents related to selection	Review that all costs are subject to cost-benefit analysis before commitment by the organisation.
Instances of additional costs/ escalation of costs by the service provider	Review and comparison of estimated vs. actual expenditures on the contract.
Service Level Agreement and contract	Review of expenditure vis a vis the available budget.
Monitoring reports with respect to specific function/ activity for which escalation / addition of cost is being sought	Review of the performance of service provider on specific activity/ function for which change in cost is sought through monitoring reports and assess the need for such change.
Action documents on requests for additional costs/ escalation of costs by service provider.	Review of action by organisation on additional costs/ escalation of costs by service provider.

Audit Conclusion:

To be filled in by auditor:

Service Level Agreement

Audit Objective: To assess whether the agency has developed the Service Level Agreement detailing all its requirements and is actively monitoring the vendor against the agreement.

AUDIT Issue 8: Adequacy of Service Level Agreement

- Is a service level agreement agreed to between the organisation and the service provider?
- Is the service level agreement detailed enough to identify all roles and responsibilities between the organisation and the service provider?
- Is the service level agreement implemented diligently?
- Does the organisation have a mechanism to monitor the implementation of the service level agreement?
- Is there a mechanism available to address exceptions to the service level agreement?

Criteria:

The service level agreement is the basis for monitoring and controlling the contractor or vendor against technical and other requirements.

Information Required	Analysis Method(s)
Service level agreement or contract	Document review to assess that all user requirements are translated to service level requirements.
Technical and other requirements (list of services that will be performed by the vendor)	Document review to assess that the roles and responsibilities of the organisation and the service provider are clearly identified and delineated.

List of responsibilities of organisation and vendor Baselines for the services that will be measured, measurement period, duration, location, and reporting timelines (defect rates, response time, help desk staffing hours, etc.) Periodic vendor performance status reports.	Document review to assess that the parameters for performance levels are clearly identified and included in the service level agreement. Document review to assess that the service level monitoring mechanism is established and agreed to between the organisation and service provider. Review vendors status reports to assess that the parameters in the SLA are being reported on by the contractor and reviewed by appropriate personnel within the organisation. Assessment of compliance to SLA technical parameters and baselines. Verify the action taken by the organisation for deviations from service level agreement.
Audit Conclusion: To be filled in by auditor:	

Security

Audit objective: To assess whether the security requirements are addressed in outsourcing and being complied with.

AUDIT Issue 9: Response to security requirements

- Have the security requirements been identified by the organisation with respect to outsourcing?
- Is there a mechanism ensuring that the security requirements of the organisation are addressed by the service provider?
- Does the organisation have a mechanism to monitor compliance to security requirements by the service provider?

Criteria:

The organisation's pertinent security requirements are levied on the contractor as appropriate.

Information Required	Analysis Method(s)
Organisation security policy Outsourcing Contract Service Level Agreement Inventory of data, application software and hardware with the service provider Inventory of back up data files and application software with the service provider Access control logs of the data files, application software as well as hardware at the outsourced location Security plan for the back-up site and disaster recovery site Monitoring reports with respect to security issues Correspondence between organisation and service provider with respect to security issues.	Document review to assess that the security requirements have been identified by the organisation and built into the outsourcing contract or SLA. Verify if the organisation has the inventory of data files, application software. Verify that the organisation monitors/ is aware that status of data files, application software and hardware are preserved during the back up and data recovery process carried out by the outsourced agency. Verify if the organisation has assurance on authorisation of any change in data, application software and hardware by the outsourced agency. Verify if the organisation has an assurance on the access to the data, application software and hardware at the outsourced location through study of access logs (physical and logical). Verify if the organisation has assurance on security mechanisms put in place by the service provider. Verify if the organisation receives regular reports and acts on the information in the monitoring reports.
Audit Conclusion To be filled in by auditor:	

Back-up and disaster recovery for outsourced services	
Audit objective: To assess whether outsourced services adhere to business continuity and disaster recovery plans as required in the contract or service level agreement.	
AUDIT Issue 10: Backup and Recovery Procedures Is the vendor meeting the requirements of the contract or SLA for BCP and DRP?	
Criteria: Contractual or service level agreement for BCP and DRP at the vendor.	
Information Required	**Analysis Method(s)**
Contract or SLA Internal Audit or third party certification of BCP and DRP readiness of the vendor Periodic reports of BCP / DRP testing or updates.	Review contract or SLA to ensure that the vendor is required to ensure BCP and DRP on the outsourced data, applications and services. Review contract or SLA to ensure that the vendor is to provide independent or internal audit reports that confirm that BCP/DRP activities are in place and that the vendor tests their procedures periodically. Review submitted reports from the vendor to ensure that testing has been conducted in accordance with the conditions of the contract and /or SLA. Review periodic reports to ensure that the procedures have been updated if needed.
Audit Conclusion To be filled in by auditor:	

APPENDIX VI

SUGGESTED MATRIX FOR AUDIT OF BCP/DRP

Business Continuity Policy	
Audit objective: To assess whether there is an effective business continuity policy in the organisation.	
AUDIT Issue 1: Policy Does the organisation have a contingency plan and policy for business continuity?	
Criteria: The organisation has a published/ approved and adopted contingency plan and has a policy in place that comprehensively covers all areas of contingency operations and clearly identifies training requirements and testing schedules.	
Information Required	**Analysis Method(s)**
Business Continuity Policy Document	Document review for assessing that the policy is consistent with the organisation's overall IT policies.
IT Policy Document Approval process for adoption of business policy objectives	Document review to assess that the policy addresses requirements of business continuity by defining organisation's contingency objectives, organisational framework and responsibilities for contingency planning. Review or interview personnel to determine how often the policy is updated if conditions change.
Correspondence and minutes of meetings related to business continuity	Review policy to determine who approved it and when was it last distributed / interview a sample of business users to assess if the policy has been sufficiently communicated within the organisation.
Audit Conclusion: To be filled in by auditor	

Organisation of Business Continuity Function	
Audit objective: To assess whether an adequate business continuity team is in place.	
AUDIT Issue 2: Business Continuity Function Is there a business continuity team or equivalent function in place?	
Criteria: Coverage of all critical areas of the organisation in the team. Roles and responsibility requirements for the team members.	
Information Required	**Analysis Method(s)**
Organisation chart of organisation	Document review / Interview relevant staff to assess that all critical areas of organisation are represented in the business continuity team or equivalent
Organisation chart of business continuity team Role/ responsibility description of the business continuity team members	Document review to assess that there is adequate ownership and assignment of business continuity responsibility on the senior management. For example, has the management identified the level and urgency of recovery, and is this reflected in the policy? Document review to assess that all critical departments have assigned team members for disaster recovery and their roles are clearly laid out.
Correspondence / meeting minutes on issues of business continuity Business continuity plan	Interview a sample staff in business continuity team / equivalent to assess that they are aware of their roles for business continuity for each critical business unit/ department.

Audit Conclusion: To be filled in by auditor

Business Impact Assessment

Audit objective: To assess whether the business impact assessment and risk assessment have been completed and a risk management system is in place.

AUDIT Issue 3: Risk Assessment

Have business impact analysis and risk assessments been carried out and critical data, application software, operations and resources been identified and prioritised?

Criteria:

Enterprise Risk Management framework or equivalent

Business Continuity Policy or equivlent

Completion of the Business Impact Assessment and identification of critical data, application software, operations and resources.

Information Required	Analysis Method(s)
Risk Assessment report(s) Business impact assessment report(s) List of critical data, application software, operations and resources for each function List of residual risks List of related stakeholders Review report(s) on risk and business impact assessment Enterprise risk assessment policy/ framework Minutes of meetings on risk assessment and business impact assessment.	Document review to assess that the risk assessment was carried out, probable threats and their impacts are identified. Document review to assess that all functional areas were considered in the risk assessment and impact assessment. Document review to assess that the impact analysis evaluated the impact of any disruption in relation to time and other related resources and systems. Document review to assess that the decision on residual risks were taken at appropriate level. Document review to assess that the organisation has determined RTOs (Recovery Time Objectives) and RPOs (Recovery Point Objectives) for each critical application. Document review to assess that the RTOs and RPOs are practical and reasonable for each application and line of business or function. Document review to assess that the senior management involvement/ approval. Document review to assess that relevant stakeholders were involved in risk identification and impact assessment.

Audit Conclusion:

To be filled in by auditor

AUDIT Issue 4: Risk Management

Is a risk management process (including mitigation and tracking, etc.) in place and have emergency processing priorities been established?

Criteria:

Coverage of the risk management process vis a vis risk assessment and business impact assessment.

Risks and emergencies are promptly addressed as per organisation's agreed parameters.

Information Required	Analysis Method(s)
Risk Management process document Risk Assessment and Business Impact Assessment Report(s) List of all relevant personnel, members of the BCP team with roles and responsibilities List of prioritized items for emergency process	Document review to assess that the risk management process addresses all high priority items. Interview and document review to assess that all relevant personnel, including senior management are aware of their role and responsibilities and carry them out. Document review to assess that the residual risks do not have material impact on the organisation.

List of residual risks identified List of instances of emergency process being invoked Emergency process/ response reports.	Document review and observation to assess that the emergency instances are adequately handled. Document review to assess impact of the emergency. Review meeting minutes or list of risks to determine that risks have been assigned, mitigation activities defined, and that risks are tracked periodically and status updated.
Audit Conclusion: To be filled in by auditor	

Disaster Recovery Plan

Audit objective: To assess whether the Business Continuity Plan includes back-up and recovery plans for hardware, data, application software and data centre (recovery) and has been suitably implemented?

AUDIT Issue 5: Back-up Procedures

Have the data and program back-up procedures been devised and implemented effectively?

Criteria:

Established criticality of applications and functions as per Organisation's Business Impact Assessment.

Determined periodicity of back-ups.

Documented back-up and recovery plans.

Information Required	Analysis Method(s)
Back up plans and procedures for the hardware, data, application software Back-up logs/ Version logs Roles and responsibilities for back-up List of storage locations and periodicity Retention schedule Security arrangement for back-up site Disaster logs Roles and responsibilities for recovery activities Training records of responsible personnel Impact assessment of disasters Report on disaster recovery activities.	Document review to assess that the back-up plan includes all critical hardware, data, application software. Document review to assess that detailed back-up procedures have been devised. Document review to assess that the back-up plan is adequately implemented. Analysis of logs to assess the back-up is taken at determined timelines and are retained for the specified time period. Verify that the right version of back up is available. Document review to assess the adequacy of back-up location and the mode of transport of back up files etc to the back-up location. Verify that the security, logical or physical is adequate for the back-up site. Verify that the back-up files can be used for recovery. Document review to assess that back-up procedures are implemented minimising loss of time and resources. Document review to assess that detailed recovery procedure has been devised and includes resetting of system parameters, installation of patches, establishing the configuration settings, availability of the system documentation and operating procedures, reinstallation of application and system software, availability of most recent backup, and testing of system. Document review to assess that recovery procedures are implemented minimising loss of time and resources. Document review/ Interview staff to assess that the relevant staff have been trained on the back-up and recovery procedures.
Audit Conclusion: To be filled in by auditor	

Environment Control

Audit objective: To assess whether the organisation has suitable environment control at back-up sites.

AUDIT Issue 6: Control Mechanisms

Has an environment control mechanism been devised and put in place at the back-up site.

Criteria:

Environment control parameters in the environment control mechanism.

Information Required	Analysis Method(s)
Environment Control programme List of probable environment hazards identified during risk assessment with locations (risk assessment document) List of environment mitigating steps undertaken.	Document Review , observation, walk through of procedues to assess that: • Un-interrupted power supply is available. • Adequate fire protection system is put in place. • Humidity, temperature and voltage are controlled within limits. • Adequate flood protection system is put in place. • Environment controls are as per the regulations. • Environment control measures are conveyed to and adhered to by all concerned staff.

Audit Conclusion:

To be filled in by auditor

Documentation

Audit objective: The business continuity plan is adequately documented to conduct effective interim business activities and recovery procedures after a business interruption.

AUDIT Issue 7: Documented plans for back up and recovery procedures, roles and responsibilities

Does the organisation have a documented disaster recovery plan that is readily available for back-up and recovery?

Criteria:

Availability and currency of the business continuity and disaster recovery plan

Information Required	Analysis Method(s)
Business continuity plan	Document review to assess the currency of the business continuity plan.
Disaster recovery plan	Document review to assess the currency of the disaster recovery plan
Version/ currency of business continuity and disaster recovery plan	Verify if the latest version of business continuity plan and the disaster recovery plan are communicated to all concerned.
Distribution list of business continuity and disaster recovery plans to all concerned.	Determine if the business continuity and disaster recovery plan documents are available at off-site to be available in case of a disaster.
	Verify that roles and responsibilites of back-up and disaster recovery team/ related staff are clearly listed out.
	Interview a sample of staff to assess whether disaster recovery procedures are known and understood.

Audit Conclusion:

To be filled in by auditor

Testing the BCP/DRP

Audit objective: To assess whether the business continuity disaster recovery procedures have been tested.

AUDIT Issue 8: Trials

Has the organisation tested its BC and DR procedures, and what changes (if any) have been made as a result of the test?

Criteria:

The organisation should test its documented BCP and DRP procedures via drills or mock-ups to ensure that they work in actual conditions. Personnel involved in ensuring continuity should be aware of their roles.

Information Required	Analysis Method(s)
BC and DR procedures & Test procedures List of items for which business continuity/ disaster recovery plan has to be tested Frequency of testing of business continuity plan and disaster recovery plan List of tests conducted List of test criteria like RTOs and RPOs etc List of testing methods employed Test results & actions taken or test recommendations Follow up action on test results.	Document review to assess whether all relevant items are covered for testing. Document review to assess whether the tests are conducted are right intervals, in time. Document review to assess that the tests were conducted against identified criteria. Document review to assess that the tests were conducted using appropriate testing methods. Document review to assess that the recommendations are conveyed to appropriate authorities for follow-up. Document review to assess that the test recommendations are adequately followed up and the business continuity plan or the disaster recovery plan are adequately updated.
Audit Conclusion: To be filled in by auditor	

Security

Audit objective: To assess whether business continuity plan and disaster recovery plan ensure security of data, application software, hardware and data center.

AUDIT Issue 9: Efficiency of Security Indicators

To determine whether the data, application software, hardware and data centre are secured appropriately during the back-up disaster recovery procedures?

Criteria:

Security baselines for the organisation like procedures laid down in the IT security policy and disaster recovery plans

Information Required	Analysis Method(s)
Inventory of data, application software and hardware Inventory of back-up data files and application software Access control logs of the data files, application software as well as hardware Security plan for the back-up site and disaster recovery site.	Verify if the number and status of data files, application software and hardware are preserved during the back-up and data recovery process. Verify if the data, application software and hardware have undergone any change during the process of back-up or disaster recovery through study of control totals on number of records and size of files related to data and application software. Verify if there has been any breach of security through examination of access control logs (physical and logical).
Audit Conclusion To be filled in by auditor:	

Back-up and disaster recovery for outsourced services

Audit objective: To assess whether outsourced services adhere to business continuity and disaster recovery plans.

AUDIT Issue 10: To determine whether the outsourced service provider ensures adoption of the organisation's business continuity plan and disaster recovery plan.

Criteria:

Security baselines for the organisation like procedures laid down in the IT security policy and disaster recovery plans.

Information Required	Analysis Method(s)
Inventory of data, application software and hardware of the organisation with the outsourced agency Inventory of back-up data files and application software of the organisation with the outsourced agency Access control logs of the data files, application software as well as hardware with the outsourced agency Test results of back-up plan and disaster recovery plan at the outsourced agency Security plan for the back-up site and disaster recovery site at the outsourced agency site Strategy to ensure continuity in case of takeover of the service provider by another organisation Information on any takeover of the service provider.	Verify if the organisation verifies if the number and status of data files, application software and hardware are preserved during the back-up and data recovery process at the outsourced agency. Verify if the organisation verifies if the data, application software and hardware have undergone any change during the process of back-up or disaster recovery through study of control totals on number of records and size of files related to data and application software at the outsourced agency. Verify if the organisation verifies if there has been any breach of security through examination of access control logs (physical and logical). Verify if the organisation verifies that the testing of back-up and disaster recovery is ensured at the outsourced agency. Verify whether the organisation is aware of the risks associated with possibility of takeover of the service provider. Verify whether the organisation has ensured that the Business Continuity is embedded in the service agreement.
Audit Conclusion To be filled in by auditor:	

APPENDIX VII

SUGGESTED MATRIX FOR AUDIT OF INFORMATION SECURITY

Risk Assessment	
Audit Objective: To ensure that all risks associated with information security have been identified and an appropriate risk mitigation strategy is put in place.	
Audit Issue 1: Assessment Mechanism Does the organisation has an effective and well-documented information security risk assessment mechanism?	
Criteria: Internal policy, procedures or regulations reflect organisation's preparedness to manage critical risks	
Information Required IS Security Policy Formal procedures of risks management System configuration documentation.	**Analysis Method(s)** Analyse risk management policy, risk assessment documents and interview top management and operational level to: • understand the real role of the organisation in risk assessment procedures. • identify who are involved in assessing risks. • find out the mechanism's operational costs. • verify whether risk assessment is performed and documented on a regular basis, or whenever the conditions change. • check if the current system configuration is documented, including links to other systems. • check if the documentation contain descriptions of key risks for the organisation's system, business, and infrastructure? In the case of lack of the formal procedures and documents on risk assessment, do not underestimate controls that are embedded within the operation procedures of the organisation – verify if the compensatory control mechanism embedded within operations is effective. This can be seen by walk through of a sample of operations etc.
Audit Issue 2: Coverage Does the risk assessment cover all important internal and external risks? Are possible effects and impact of Information Security breaches assessed?	
Criteria: All the significant risks are identified and assessed properly (best practices in risk assessment[51]).	
Information Required Documented Risk Assessments Risk register Incident handling reports.	**Analysis Method(s)** Review documents to check if the risk assessment performed by the audited organisation was based on sufficiently comprehensive information. Check whether data and reports were obtained from the organisation's incident management system. (Support your analysis with results of Analysis Methods of IT Operations focused on Incident Management system, esp. if the information security incident handling forms a system separated from a general incident management system.) ***Validation Test 1:*** Security audit trails: Determine if security audit trails capture user identification (ID), type of event, data and time, success or failure indication, origination of event, and the identity or the name of the affected object

[51] ISO 27005 information security risk management, ISACA RiskIT Framework, COSO Enterprise Risk Management Framework.

	Interview relevant personnel to verify whether there is a standard re-assessment of risk whenever the organisation plans to roll out new information systems, upgrades, and new versions. Check the risk assessment design for completeness, relevancy, timeliness and measurability. Check if consequences of infrastructure inoperability is considered while assigning risk categories. Verify documents to see if a business impact analysis is done for the consequences of critical information becoming unavailable, corrupted, inappropriately compromised or lost. Review incidence response reports and earlier risk documents/ registers to examine whether the risk assessment methodology has been effective in the past.
Audit Issue 3: Mitigation Are significant risks mitigated in effective and efficient way?	
Criteria: Adequate risk mitigation practices are in place.	
Information Required Problem/incident handling reports Periodic activity reports.	**Analysis Method(s)** Review incident handling reports and check whether appropriate procedures were in place to prevent, detect and control security risks identified in the risk assessment document. In organisations that do not follow a well-defined risk assessment mechanism, determine what compensatory control exist. Analyse if any serious security incidents occurred in relation to risks that might have been mitigated better with a properly working risk assessment mechanism, vis-à-vis existing compensatory controls. Take into account that problem/incident reports may be incomplete in some cases. Nevertheless, important events may be reflected directly or indirectly in other documents, as e.g. annual activity reports or other periodic reports.
Audit Conclusion: To be filled by the auditor	

Information Security Policy	
Audit Objective: To assess whether there is adequate strategic direction and support for information security in terms of a security policy, its coverage, organisation-wide awareness and compliance.	
Audit Issue 4: Information Security Policy Does the organisation possess an Information Security Policy? Is it properly implemented and documented? Does it form a consistent and robust IT security plan?	
Criteria: The organisation's information security policy covers all operational risks and is able to reasonably protect all business critical information assets from loss, damage or abuse.[52]	
Information Required IT Strategy Legal acts defining information security requirements Formal and written information security policy	**Analysis Method(s)** Check the document to examine whether IT Strategy adequately highlights the critical role of Information Security. Also refer and use the *IT Governance* matrix for *IT Strategy*. In the absence of a written IT strategy, interview top management, middle level management and staff to see what is their understanding of the strategic role of Information security. Assess compliance of the organisation's *IT Strategy and Information Security Policy* external compliance requirements

[52] See ISO 27000 series Information Security Management System and other internal policy, procedures or applicable regulations.

Organisation structure and its job description Contractual arrangements with external parties IT Security Plan.	Compare policy goals and security procedures to determine the effectiveness of integration of information security requirements into the IT security plan (charter, framework, manual etc.). Verify whether it is regularly reviewed at appropriate management levels. Examine coverage of the IT security plan and check whether it considers IT tactical plans, data classification, technology standards, security and control policies and risk management. Check if the IT security plan identifies: Roles and responsibilities (board, executive management, line management, staff members and all users of the enterprise IT infrastructure), Staffing requirements, Security awareness and training; Enforcement practices; and the need for investments in required security resources. Review and analyse the charter to verify that it refers to the organisational risk appetite relative to information security, and that the charter clearly includes scope and objectives of the security management function. Check security incident reports and follow-up documents to find what actions the organisation takes when individuals violate the security policy. Check the incident reports to identify the number of Information Security breaches by employees or external parties in given period to assess effectiveness of the policy.
Audit Issue 5: Confidentiality Has the organisation confidentiality requirements or non-disclosure agreements that appropriately reflect the need for protecting information? Do the policies secure information in the organisation's relation with external parties?	
Criteria: The organisation's information security policy is able to protect all confidential information related to internal stakeholders and third parties	
Information Required	**Analysis Method(s)**
External and internal regulations concerning confidential and classified information. Eg, Non-disclosure clauses for employees. Contractual arrangements with external parties Information security policy IT Security Plan.	Check procedural measures taken by the organisation to comply with the confidentiality requirements. Where access to confidentiality breach cases are restricted to special law procedures and specialised agencies only, base your opinion on their reports and recommendations to the organisation's management – if available. Review contractual arrangements with external parties or contractors. Do they involve granting and invoking access, processing, communicating or managing organisational information assets? Check whether the contractual terms and obligations define the security restrictions and obligations that control how contractors will use organisation's assets and access information systems and services. Check whether any information security breaches were committed by contractors. Check management action on such breaches.
Audit Conclusion	

Organization of IT Security

Audit objective: To ensure the secure operation of IT processing facilities.

Audit Issue 6: Structure

Does the auditee have clear organisation of IT security? Are security roles and responsibilities defined with regard to information security policy?

Criteria:

Documented and clear IT roles and responsibilities relating to Information Security Policy[53]

Information Required	Analysis Method(s)
IT Organisation structure	Determine if the responsibility for IT security is formally and clearly stated.
Internal regulations related to IS security	Check whether a process exists to prioritise proposed security initiatives, including required levels of policies, standards and procedures.
Job descriptions	Check how senior management maintains an appropriate level of interest in information security within the organisation.
Minutes of relevant bodies' meetings.	

Audit Issue 7: Coordination

How does the organisation coordinate information security activities from different parts of organisation?

Criteria:

No responsibility conflicts, disharmony nor "no-man's land" in Information Security activities[54]

Information Required	Analysis Method(s)
Legal requirements concerning classified information	Check documents, observe practices and interview personnel to verify whether there are inherent conflicts/ overlaps/ gaps between security procedures followed by employees in different departments/ units.
Organisation structure	Check operational workflow procedures to identify if some information is transmitted to external parties out of control of responsible units/employees.
Internal regulations related to IS security	Check if higher level managers are aware of coordination problems and whether they supervise inspections and coordinating activities.
Minutes of meeting of IT security committee	Review processes to check whether there is any established procedure for management to authorize new information processing facilities.
Failure reports.	

Audit Conclusion

To be filled by auditor

Communications & Operations Management

Audit objective: To ensure that internal and external communication is secure.

Audit Issue 8: Policy and procedures

Are policy and procedures adequate for safe and efficient internal and external communication?

Criteria:

The policy and procedures form stable management environment for internal and external communication[55]

Information Required	Analysis Method(s)
Formal and written policy for communications and IT operations	Check whether the policies and procedures of the organisation embrace communication with citizens, mass media, and external organisations.
Documentations of operational procedures.	Verify how the organisation documents its operating procedures and makes them available to all users. Interview a sample set of users at different levels to examine whether the procedures for data handling are well known by employees.
	Check how often the communication and data handling procedures are reviewed and updated.

[53] See ISO 27000 series

[54] See ISO 27000 series Information Security Management System

[55] See following standards: : ISO-27002, S15-IT Control (ISACA Standard), COBIT

Audit Issue 9: Network control How does the organisation manage and control information in the network?	
Criteria: Network operations are managed and performed in safe and effective way[56]	
Information Required	**Analysis Method(s)**
Information restriction policy Network Admin Logs/ Registers Results of the logs analysis User Acceptance Test Report Service Level Agreement(s) Information available to the public or found in the web pages.	Check what tools are used for network monitoring and analysis. verify whether users and IT systems of the audited organisation are protected against spam. Check whether Intrusion Detection System configurations and logs are analysed by appropriate personnel to ensure security of information from hacking attacks and malware intrusions. Verify whether the attacks (failed and effective ones) are analyzed and reported. Check the statistics of spam, hacking and malware attacks. Inquire how the organisation provides secure transmission of transactions passing over public networks. Eg. Circulating/ notifying operating procedures to users for e-commerce/ online transactions. Review policies to verify whether data transmission outside the organisation requires an encrypted format prior to transmission. Inquire whether information security policies have been implemented in accordance to the sensitivity classification of organisation's data (e.g., confidential, sensitive). Through enquiry determine whether the client utilises cryptography for sensitive information processing. If so, conduct a validation testing. **Control Validation Testing Procedures** ***Validation Test 1:*** Operating effectiveness of cryptographic controls: Determine: • the existence of processes for the key management life cycle. • key destruction. • segregation of duties for the authorised key custodians.
Audit Issue 10: Configuration Management Are the IT resource settings/ applications under appropriate configuration control?	
Criteria: Clear and well-managed configuration system that supports Information Security in communication and operations.	
Information Required	**Analysis Method(s)**
Policy and procedures referring to configuration matters in operations area Configuration lists/ library.	Review role matrices to determine who is responsible for administering the configuration, and what the scope of the configuration control in operations is. Check how it is registered, controlled and updated. Verify if any problems occurred in the past because of configuration discrepancies. If so, interview managers to check what procedures have been implemented to configuration changes
Audit Conclusion To be filled in by the auditor	

[56] *ibid*

Assets Management	
Audit objective: To encourage appropriate protection of IT assets.	
Audit Issue 11: Assets Management Does organisation have an appropriate asset management system that supports its Information Security?	
Criteria: Ensuring appropriate protection of information assets (Ref: ISO 2700 series Information Security Management System, COBIT, and other internal policy, procedures or regulations applied).	
Information Required	**Analysis Method(s)**
Asset management policy Asset Classification Information classification Asset disposal procedures Financial audit reports (if they refer to assets and inventories).	Review policy to check if there is an acceptable use policy for IT hardware and software (Example, laptops may be used for personal use if it does not interfere with official business). Check whether the asset database is up-to-date. Check inventory records to verify whether assets are categorised in terms of value, sensitivity, or other categories. Review procedures for assets disposal and the level of supervision mandated. Check the authorisation requirement for any disposal or re-use of equipment. Inquire persons and check provisions that ensure data is erased prior to disposal or re-use of equipment.
Audit Conclusion	

Human Resources Security	
Audit objective: To ensure that all employees (including contractors and any user of sensitive data) are qualified for data handling and understand their roles and responsibilities, and that access is removed once employment/ contract is terminated.	
Audit Issue 12: Staff Awareness and Responsibility Are employees aware of their roles and responsibilities with respect to their duties and security responsibilities?	
Criteria: Professionlly trained staff in guarding information security	
Information Required • HR Policy and recruitment procedures • Information Security policy and procedures • Competency Standard for IT Personnel • Individual assessment reports • Security incident reports (including violation of code of ethics or code of conduct) • Security Awareness Campaign • User Management Roles and Responsibilities.	**Analysis Method(s)**[57] Inspect hiring documentation for a representative sample of IT staff members to evaluate whether background checks have been completed and evaluated. Inspect selection criteria for performance of security clearance background checks. The role of each position must be clear. Supervision activities should be run to check adherence to management policies and procedures, the code of ethics, and professional practices. Check if roles thay are critical for Information Security are clearly defined and documented. Employees and third parties assigned such roles should know their responsibilities with respect to protecting the organisational information assets, including electronic data, IS infrastructures, and documents. Review for appropriate definition of critical roles, for which security clearance checks are required. This should apply to employees, contractors and vendors. Check for appropriate Segregation of Duties between IT security management and Operations. Check if the policy of IT personnel placement, transfer and rotation, as well as employee termination is clear to reduce dependence on the individual. Verify what knowledge transfer mechanisms are followed.

[57] Human resources *vis-à-vis* Information Security is one of key topics in other sections including *IT Governance*, and portions of this Audit Matrix such as *Information Security Policy* (awareness, responsibility, top-down information flow, sanctions) and/or *Access Control* (individual user rights).]

Audit Issue 13: Training Is training in Ind\formation Security procedures effective in enhancing staff's professional skills in guarding the same ?	
Criteria: Conduct, Scope and Periodicity of Orgnisational Training for Information Security.	
Information Required	**Analysis Method(s)**
Training schedule Results of ending tests Evaluation of training effectiveness.	Assess the training effectiveness measurement process, if any, to confirm that the critical IT security training and awareness requirements are included. Inspect IT security training programme content for completeness and appropriateness. Inspect delivery mechanisms to determine whether the information is delivered to all users of IT resources, including consultants, contractors, and temporary staff members and, where applicable, customers and suppliers. Inspect training programme content to determine if all internal control frameworks and security requirements are included based on the organisation's security policies and internal controls (e.g., impact of non-adherence to security requirements, appropriate use of company resources and facilities, incident handling, employee responsibility for information security). Inquire whether and confirm that training materials and programmes have been reviewed regularly for adequacy. Inspect the policy for determining training requirements. Confirm that the training policy ensures that the organisation's critical requirements are reflected in training and awareness programmes. Interview staff to asess whether they have undergone the organisational training and whether responsibilites in maintaining information security and condfidentiality are clearly understood by them.
Audit Conclusion	

Physical Security	
Audit objective: To prevent theft or damage of IT hardware, unauthorized access, and copying or viewing of sensitive information.	
Audit Issue 14: Premises safety Are the buildings and grounds of the organisation secured against physical and environmental risks?	
Criteria: Ensure that physical and environmental security stays in compliance with the safety requirements and sensitivity classification of IT assets.	
Information Required	**Analysis Method(s)**
Network diagram Site Security Plan Periodical physical testing report Reports by relevant services (eg. Fire dept).	Analyse what the audited organisation's primary physical security controls are. Check if they match the up-to-date risk analysis. Review location and physical precautionary measures for key elements of IT infrastructure. Check what environmental controls are in place (fire extinguisher, alarm, power systems, etc). Verify if recommendations by relevant services (esp. firemen, housing inspection, disaster prevention) been implemented. (For security plans relating to disasters, refer to BCP and DRP section of this Handbook).

Audit Issue 15: Physical access How the organisation ensures that only authorised personnel access the facility?	
Criteria: Security measures are put in place by the organisation to ensure no unauthorised physical access to critical IT facilites (server rooms, data storage etc)	
Information Required	**Analysis Method(s)**
Layout of IT hardware installation Site Security Plan Devices configuration Periodical physical testing report Incident reports.	Review security instructions, network diagram and related documents and check how the organisation controls access to sensitive areas of its premises. Review and observe the in/out traffic and how the physical security system works. Determine what means are used. Obtain policies and procedures as they relate to facility security (gates, badges, turnstiles, guards, barriers, key and card reader access etc.) and determine if those procedures account for proper identification and authentication. Check who maintains and controls the allocations of access control to the sensitive locations. Find if the level of management is sufficient for Information Security. Find if access to secure areas /secure rooms/ server locations is restricted. Select a sample of users/employees and determine if their access to facilities is appropriate, based upon their job responsibilities. Verify if incidents are reported to an incidents/problems management system. Find if they are analysed and lessons learnt.
Audit Issue 16: Intrusion defense. Whether the organisation has a policy on intrusion detection and follows it	
Criteria: Procedure to comabt intrusions as laid down in Organisation's Internal Security Policy	
Information Required	**Analysis Method(s)**
Site Security Plan Devices configuration Incident reports.	Inquire how the organisation's security unit knows that an intrusion has occurred to secure locations. Check instructions to find out the Process for handling an intrusion to a secure space or building. Check incident reports to identify whether intrusion was detected early. Check if the organisation have a clear desk or clean screen policy to prevent unauthorised access.
Audit Conclusion.	

Access Control	
Audit objective: To ensure that only authorised users have access to relevant information	
Audit Issue 17: Access policy Does the organisation have clear and efficient policy on access control?	
Criteria: The Access Policy gives sound basis for control of relevant information distribution.	
Information Required	**Analysis Method(s)**
Access Policy and procedures List of users Access control list/ matrix.	Analyse Access Policy and procedures to ensure that employee duties and areas of responsibility are separated in order to reduce opportunities for unauthorised access and privilege approval. ***Validation Test:*** Operating effectiveness of authorisation of user access to the LAN (not separate testing of user access to applications should be done in conjunction with application reviews).

	Select a sample of user and system accounts to determine existence (access control software maybe used) of the following: • clearly defined requested role and/or privileges mapped to job functions. • business justification for access. • data owner and management authorisation (i.e. signatures/ written approvals). • Business/risk justification and management approval for non-standard requests. • Access requested is commensurate with job function/role and required segregation of duties.
Audit Issue 18: Privileges management. Is process for granting and revoking access control to employees and contractors safe and effective?	
Criteria: The Information Security function monitors user account management operations on a timely basis and reports the operating efficiency and effectiveness.	
Information Required Access control procedures Sample of employees' transfers and terminations.	**Analysis Method(s)** Check procedures to determine how often the various accesses and privileges that employees or users have in the organisation are reviewed. **Check how the privileges that are granted to an employee are confirmed (Examples include asking the supervisor, area manager, group, etc.)** Interview sample of users and check instructions to verify how the users are informed about their responsibility for protecting sensitive information or assets when the access is granted to them. Determine whether the organisation's security practices require users and system processes to be uniquely identifiable and systems to be configured to enforce authentication before access is granted, and that such control mechanisms are utilised for controlling logical access across all users, system processes and IT resources. Analyse other than password privileges, e.g. how it is checked that a user does indeed have sufficient access and privileges to the requested resource? (Examples include access from secure location, hardware tokens or fingerprint readers, etc.) ***Validation Test 1:*** Operating effectiveness of transfers and terminations: Obtain from HR a sample of employee transfers and terminations and, through review of system account profiles and/or CAATs (e.g. ACL, IDEA) determine if access has been appropriately altered and/or revoked in a timely manner. ***Validation Test 2:*** Password management: Verify that the quality requirements for passwords are defined and enforced by the network management system and/or operating systems based on local requirements/ organisation policy or best practice.
Audit Conclusion	

IT Systems Acquisition, Development and Maintenance is in Appendix III

Business Continuity Management is in Appendix VI

APPENDIX VIII

SUGGESTED MATRIX FOR AUDIT OF APPLICATIONS CONTROLS

Input	
Audit objective: To assess whether valid data is being entered into the application by authorised personnel.	
AUDIT Issue 1: Validation of inputs Does the application have adequate input validation controls?	
Criteria: Several good practices provide basis for criteria of good inout validation controls, e.g. validation rules are comprehensive ,documented and implemented into the application entry interfaces; different methods and interfaces for data entry are documented; invalid data is properly rejected by the application; the validation criteria is updated in a timely, appropriate and authorised manner; there are compensating controls such as logs and authorisation rules in case of the possibility of overriding input controls; and there are proper controls and documentation for the application interfaces.	
Information Required	**Analysis Method(s)**
Business requirements and rules Data input types Legal and external compliance requirements Structure of data interfaces with other applications System flow diagrams User manuals Validation rules	Analyse business rules, requirements, application documentation and inquire business process owners to determine which validation rules should be assured in the business process being assessed. Check if these validation rules were proper designed and documented. Verify whether the validation controls for data input are being enforced: observing application users into real action; running the application in a testing environment and testing different interfaces for data entry; and analysing data records stored in the database through the use of CAATs. Obtain functional description for each class of input and design information on transaction data entry. Inspect the functionality and design for the presence of timely and complete checks and error messages. If possible, observe transaction data entry. Assess whether validation criteria and parameters on input data match business rules and enforce rejection of unmatched input types. In case of online processing systems, verify that invalid data is rejected or edited on entry and test the logic checks/calculation checks performed. Database operatives (such as *, =, or, select) should be disallowed as valid input, as they can be used to disrupt or retrieve information from the database. Inquire managers about whether validation criteria and parameters on input data are periodically reviewed, confirmed and updated in a timely, appropriate and authorised manner. Assurance could be obtained through documentation review, code analysis or interviews. Inquire and check documentation in order to verify the possibility of overriding input data control validations and controls. Verify if the override actions are being properly logged and reviewed for appropriateness. Check whether authority to override is restricted to only supervisory staff and to a limited number of situations. Inspect error corrections, entry overrides and other documents to verify that the procedures are followed. Determine which interfaces exist with the application. These interfaces could be in the form of real-time data transmission or periodic transmission of data files via batch processes. Review system flow diagrams and system code, and interview the application developers or administrator to obtain information on interfaces and controls over them. E.g.: Control totals from interface transmissions. E.g., Hash[58].

AUDIT Issue 2: Is management of source documents, data collection and entry adequate?	
Criteria: Data preparation procedures are documented and understood by users; there is appropriate logging and records of the source documents received until their disposal; there is assignment of unique and sequential numbers to each transaction and original source documents are retained for the time required by legal standards or policies.	
Information Required	**Analysis Method(s)**
Classes of source documents Entity's criteria for timeliness, completeness and accuracy of source documents Data preparation procedures Data interfaces with other applications Document retention policies System flow diagrams	Inspect and observe creation and documentation of data preparation procedures, and inquire whether and confirm that procedures are understood and the correct source media are used. Assess whether the Data Processing group (DP) or equivalent group maintains a log of all the user departments' source documents received and their final disposal. Verify the existence of a system of reconciliation of record counts with user department groups. Verify that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management. Inspect whether critical source documents are pre-numbered and how out-of-sequence numbers are identified and taken into account. Identify and review out-of-sequence numbers, gaps and duplicates using automated tools (CAATs). Verify if there is assignment of unique and sequential numbers to each transaction preventing duplication. Enquire responsible personnel about retention policies. Verify how these policies are ensured. A sample of system records might be checked against its source documents.
AUDIT Issue 3: Does the application have adequate procedures for error handling?	
Criteria: There is a system of clear and compact error messages communicating the problems so that immediate corrective action can be taken for each type of error. Errors are corrected or appropriately overridden before processing transactions. Logs are reviewed periodically and necessary corrective action is taken.	
Information Required	**Analysis Method(s)**
Error types and messages Log review procedures Policies and procedures for dealing with rejected data Suspense file review procedures	Discuss the application's error and exception handling with the developer and/or administrator. Inquire whether and confirm that policies and procedures exist for handling transactions that fail edit and validation checks. Verify whether the system provides error messages for every type of error (field level or transaction level) not meeting the edit validation. Verify how the application behaves if data is rejected by the input controls. Check whether the data items are recorded or if they are automatically written in a suspense file. Check if the automated suspense file includes codes indicating error types, date and time of entry and identify the person entering data. Evaluate if there are procedures for reviewing and correcting data in the suspense file before processing it again. Assess whether an escalation procedure is in place when error rates are too high and corrective action is taken. Ask managers about the existence of procedures for periodically reviewing the log. Verify whether the procedures include the initiation of corrective measures. Obtain evidence – either documental or digital – that the log is being periodically reviewed.

[58] PC Magazine Encyclopaedia, from http://www.pcmag.com/encyclopedia/term/44130/hash-total:
A method for ensuring the accuracy of processed data. It is a total of several fields of data in a file, including fields not normally used in calculations, such as account number. At various stages in the processing, the hash total is recalculated and compared with the original. If any data has been lost or changed, a mismatch signals an error

AUDIT Issue 4: How data entry authorisation into the application is being managed?	
Criteria: Authorisation levels for transactions were established and are enforced by proper controls; there is proper segregate of duties for data entry; and there are compensating controls in place for those cases in which segregation of duties is not possible.	
Information Required	**Analysis Method(s)**
Legal and external compliance requirements Business requirements and rules User manuals	Inquire whether and confirm that the design of the system provides for the use of preapproved authorisation lists. Verify, through inspection of authorisation lists, that authorisation levels are properly defined for each group of transactions. Assess whether authorisation rules for data input, editing, acceptance, rejection and override for major classes of transactions are well designed and documented. Observe that authorisation levels are properly applied running the application in a testing environment. Verify, through the use of CAATs or embedded audit modules, that the authorisation records present in the database are compliant to the authorisation rules defined. Determine if a separation of duties (SOD) table exists, and review for adequate separation of key duties/ job functions and permitted transactions, then, look into list of users and user-specific access privileges. Assess whether segregation of duties ensures that the person keying the data is not also responsible for verification of document. Verify the adoption of compensating controls in cases which SOD was not feasible.

Processing	
Audit objective: To assess whether the application ensures data integrity, validity and reliability throughout the transaction processing cycle.	
AUDIT Issue 5: Are the business processes rules and requirements properly mapped into the application?	
Criteria: Application transactions run accordingly to the expected behaviour.	
Information Required	**Analysis Method(s)**
Application documentation Business rules and requirements Data flow chart Highly critical transactions list Source code	Identify the executable programs in the application from a study of the data flow chart and match them with defined and established business process rules. Review the application documentation to verify that it is applicable and suitable for the task. Where appropriate for critical transactions, review the code to confirm that controls in the tools and applications operate as designed. Reprocess a representative sample to verify that automated tools operate as intended. For highly critical transactions, set up a test system that operates like the live system. Process transactions in the test system to ensure that valid transactions are processed appropriately and in a timely fashion.
AUDIT Issue 6: Do the application controls ensure the integrity and completeness of its transactions?	
Criteria: The application does correctly identify transactional errors. Data integrity is maintained even during unexpected interruptions to transaction processing. There is an adequate mechanism for handling processing errors, review of suspense files and clearance.	

Information Required	Analysis Method(s)
Application design documentation Business rules and requirements Out-of-balance reports Reconciliations Report review procedures Suspense files	Assess whether the application has adequate validity checks in place to ensure processing integrity. Inspect the functionality and design for the presence of sequence and duplication errors, referential integrity checks, control, and hash totals[59]. Inspect reconciliations and other documents to verify whether input counts are coherent with output counts to ensure completeness of data processing. Trace transactions through the process to verify that reconciliations effectively determine whether file totals match or the out-of-balance condition is reported. Inquire whether control files are used to record transaction counts and monetary values, and that the values are compared after posting. Verify that reports are generated identifying out-of-balance conditions and that the reports are reviewed, approved and distributed to the appropriate personnel. Take a sample of data input transactions. Use appropriate automated analysis and search tools to identify cases where errors were identified erroneously and cases where errors were not detected. Inquire whether and confirm that utilities are used, where possible, to automatically maintain the integrity of data during unexpected interruptions in data processing. Inspect the audit trail and other documents, plans, policies and procedures to verify that system capabilities are effectively designed to automatically maintain data integrity. Inspect the functional description and design information on transaction data entry to verify whether transactions failing validation routines are posted to suspense files. Verify that suspense files are correctly and consistently produced and that users are informed of transactions posted to suspense accounts. For a sample of transaction systems, verify that suspense accounts and suspense files for transactions failing validation routines contain only recent errors. Confirm that older failing transactions have been appropriately remediated.

Output

Audit objective: Assess whether application assures that output information is complete and accurate before further use and that it is properly protected.

AUDIT Issue 7:
Does the application have controls to ensure completeness and accuracy of its output?

Criteria:
Procedures have been designed to ensure that the completeness and accuracy of application output are validated prior to the output being used for subsequent processing, including use in end-user processing; tracking of application output is properly enabled; output is reviewed for reasonableness and accuracy; and completeness and accuracy controls are effective.

Information Required	Analysis Method(s)
Completeness and accuracy controls Methods for balancing and reconciliation List of electronic outputs / reports Sample of electronic output	Obtain a list of all electronic outputs that are reused in end-user applications. Verify that the electronic output is tested for completeness and accuracy before the output is reused and reprocessed. Examine the balancing and reconciliation of output as established by documented methods. Select a representative sample of electronic output, and trace selected documents through the process to ensure that completeness and accuracy are verified before other operations are performed. Re-perform completeness and accuracy tests to validate that they are effective. Examine if each output product contains processing program name or number; title or description; processing period covered; user name and location; date and time prepared; and security classification. Select a representative sample of output reports, and test the reasonableness and accuracy of the output. Verify that potential errors are reported and centrally logged.

[59] F/N: *ibid*

AUDIT Issue 8: Is the output data properly protected?	
Criteria: Output is handled in line with the applicable confidentiality classification; distribution of outputs/ reports are appropriately controlled.	
Information Required	**Analysis Method(s)**
Output handling and retention procedures Information classification policies	Review output handling and retention procedures for privacy and security. Assess whether procedures have been defined that require the logging of potential errors and their resolution prior to distribution of the reports. Examine the system of reconciliation of output batch control totals with input batch control totals before release of reports establishing data integrity. Check if there are documented procedures for labeling sensitive application output and, where required, sending sensitive output to special access-controlled output devices. Review the distribution methods of sensitive information and verify that the mechanisms correctly enforce pre-established access rights.

Application Security

Audit objective: Assess whether application's information is properly secured against misuse.

AUDIT Issue 9: Do the traceability mechanisms of the application are sufficient for its purpose?	
Criteria: There are audit trails that capture edits, overrides, and authorisation logs to critical transactions; the audit trails are periodically reviewed to monitor unusual activity; the audit trail is adequately maintained and protected; and unique and sequential numbers or identifiers are assigned to every transaction.	
Information Required	**Analysis Method(s)**
Audit trail structure and documentation Override policies Review procedures System flowcharts	Obtain documentation and assess the design, implementation, access and review of audit trails. Inspect the audit trail structure and other documents to verify that the audit trail is designed effectively. Inquire who can disable or delete the audit trails. Inspect the audit trail, other documents, plans, policies and procedures to verify that adjustments, overrides and high-value transactions are designed effectively to be promptly reviewed in detail. Inspect the audit trail, transactions (or batches), reviews and other documents; trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to verify that periodic review and maintenance of the audit trail effectively detects unusual activity and supervisor reviews are effective. Inquire how the access to the audit trail is restricted. Examine access rights and access logs to the audit trail files. Verify whether only restrict and authorised personnel have access to the audit trail. Assess if the audit trail is protected against privileged modifications. Verify, where possible, using automated evidence collection, if unique identifiers are being assigned to each transaction.
AUDIT Issue 10: Is the application data properly protected?	
For physical and logical access control refer to Appendix VII on Information Security. For disaster recovery planning refer to Appendix VI on BCP/DRP	