Effective data management seeks to achieve the following **objectives**:

(i) **Confidentiality** of data must be maintained. Data should be accessible to authorized users only.
(ii) Data **integrity** must be preserved.
(iii) **Data type and structure** should be appropriate so that required contents may be stored in the desired format.
(iv) Data should be backed up so that in case of data loss, it could be made **available** with minimum data loss.

Responsibilities of Data Administrator and Database Administrator regarding following data/database related functions.

Function	Data Administrator	Database Administrator
Defining data	(i) Strategic data planning (ii) Determine user needs (iii) Specify conceptual and external schema definitions	(i) Specify internal schema definitions / specifying the physical data definition (ii) Changing the physical Data definition to improve performance
Creating data	Advising users about criteria for: (i) data collection, (ii) data validation and (iii) data editing	(i) Answering programmer queries and educating programmers in DB structure (ii) Implementing DB access controls, DB update controls and concurrency controls; (iii) assist in populating database
Retiring data	Specify retirement policies	Implement retirement policies
Making database available to users	Determining end user requirements for: (i) DB tools, (ii) Testing and evaluation of end user tools	Determining programmer requirements for: (i) DB tools, (ii) Testing and evaluation of programmer and optimization tools
Maintaining database integrity	Developing organizational standards	Implementing database and application controls
Monitoring operations	Monitoring end users	(i) Monitoring DB usage (ii) Collecting performance statistics (iii) Tuning the database

Case Study: In a recent memo to the Chief Internal Auditor of YME Limited, the CEO has expressed his concern that review of IT function is being ignored by the Internal Audit Department. He advised that a strategy should be devised to measure the performance of IT department in ensuring continuous service, managing problems and ensuring systems security.

Possible reasons for ignoring the IT function by Internal Audit Department are as follows:
(i) Roles and responsibilities of the internal audit department may not be clearly defined.
(ii) Lack of adequate resources.
(iii) The personnel of internal audit may be lacking in knowledge and understanding of IT related controls.
(iv) Lack of coordination between internal audit and the IT department.

Key performance indicators which can be used to measure the performance of IT department in ensuring **continuous service** are as follows:
(i) Number of hours lost per user per month (due to unplanned outages).
(ii) Number of times the availability requirement of SLAs was not met.
(iii) Frequency of service interruption of critical systems.
(iv) Number of IT continuity training hours per year per relevant IT employee.

Key performance indicators which can be used to measure the performance of IT department in **managing problems** are as follows:
(i) Number of recurring problems with an impact on the business.
(ii) Number of business disruptions caused by operational problems.
(iii) Average and standard deviation of time lag between problem identification and resolution.
(iv) User's satisfaction (through survey forms).

Key performance indicators which can be used to measure the performance of IT department in ensuring **systems security** are as follows:
(i) Number of security incidents damaging the organisation's reputation.
(ii) Number of systems where security requirements are not met.
(iii) Average time to grant, change and remove access privileges.
(iv) Number and type of suspected and actual access violations.

Case study: XBL is a large multinational bank. It has recently received license to operate banking business in Heavenland, which is a resource rich country with lots of business opportunities. The Government of Heavenland has recently opened its banking sector to foreign banks and allowed seven other multinational banks to operate in the country. The management of XBL intends to launch its operations in all the major cities of Heavenland. XBL's operational feasibility team is in consultation with various firms for developing the infrastructure facilities and recruiting the work force. However, outsourcing option for IT support services is also under its consideration. In this respect, they have identified two highly reputed service providers which have a presence all over Heavenland.

IT Outsourcing:
IT outsourcing refers to outsourcing all or parts of IT functions to an external party. By this option, XBL may hire an outsourcing agent and use its well-trained, experienced and polite workforce for the fulfillment of the desired tasks.

XBL may derive following **advantages** by outsourcing its IT support services:
(i) XBL may start its full fledge operations within targeted time.
(ii) Experienced working team would be available to XBL from Day 1.
(iii) XBL would be free from substantial HR related overheads and issues as outsourcing agent would be responsible for hiring, firing, training and salary issues.
(iv) More services may be available to XBL at lower price, especially for 24/7/365 days requirement.

There are some **inherent risks associated with the outsourcing of IT services**; however, most of these risks could be mitigated if appropriate clauses have been included in the outsourcing agreement.

Risks	Suggested measures
High security risk, as system will be exposed to outsiders.	Confidentiality agreement with the outsource service provider.
Outsourced staff may be frequently changed by the outsourcing agent which may extend the learning curve and XBL may never be able to get the efficiency of a fully trained team.	Appropriate clauses shall be included in the agreement to bound the outsourcing agent to: □ deploy staff on long term basis. □ deploy dedicated resources at the critical areas.
There is a risk to business continuity of XBL on account of either any dispute with the outsourcing agent or if the outsourcing agent goes out of business.	□ Business continuity management would be part of the contract. □ Make arrangement with another outsourcing agent to handle the XBL's systems incase contract with outsourcing agent is terminated abruptly.
Outsourcing agent may fail to deliver the agreed level of services.	Define penalty clause in case of nonfulfillment of agreed service levels.

XBL should consider the following matters in making a choice between the two service providers:
(i) Prices offered by each vendor for its deliverables in comparison with other.
(ii) Financial soundness of the vendor – through its past annual reports and market feedbacks etc.
(iii) Available resources – manpower, machines, infrastructure etc.
(iv) Commitment to quality – through its existing clients and market feedback.
(v) Controls in place for disaster recovery and continuity of operations.
(vi) Comprehensive insurance and commitment to compensate the client's loss.
(vii) Technical competence – whether the vendor has relevant technical competence in the IT.
(viii) Proven track record – whether the vendor has successfully provided or providing such services to a similar organisation.
(ix) Access controls and security administration at the vendor's premises. etc.
(x) Location of vendor's business.

Case Study: Transpose Energy Limited (TEL) is a large importer and distributor of UPS, generators and solar panels. TEL has been using separate information systems for suppliers, customers, HR and Finance. These systems have been developed in-house but due to non-integration, several data items are required to be re-entered.
The CEO of TEL has recently received a proposal from Alternative Technologies (AT) for outsourcing TEL's IT function. AT proposes to implement a significantly improved and integrated information system in TEL. AT has offered to train the existing employees of TEL on the new system; however, the administrative rights of the system would remain with AT. AT's monthly billing would depend upon the number of man hours worked by their employees.

Business risks associated with AT's proposal are as follows:
(i) Cost of arrangement with AT may exceed TEL expectations.
(ii) TEL would become extremely dependent on AT on account of non-availability of source code and limited system administration rights.
(iii) TEL may lose internal IS expertise.
(iv) AT's management may not be as responsive to TEL's need as TEL's employees.
(v) AT may fail to deliver the agreed level of services.
(vi) There is a risk to business continuity of TEL on account of:
 Dispute with AT.
 AT going out of business.
(vii) AT may use pirated/copied software for which TEL may also be held responsible.
(viii) Confidentiality of TEL's data may be compromised.

Besides inclusion of appropriate clauses in the agreement, TEL may take following **other measures to mitigate the identified risks:**
(i) Appropriate communication with the employees and wherever necessary, their placement at other appropriate places in TEL.
(ii) Planning the course of action in case of dispute with AT, including:
 Sign a separate agreement for the use of alternate processing facility in case of emergency.
 Train key IT employees on IT tools and technologies relevant to TEL.
 Develop internally a program that may enable TEL to continue its operations in case AT ceases to provide services.
(iii) Entering into a short-term contract, at least initially.
(iv) Assessing viability of AT's business before accepting the proposal.

Case study: Flash Marketing Limited (FML) is a medium sized fast moving consumer goods distributor. Few months ago, FML got its website revamped by Web Experts Limited (WEL). The new website has interactive features with separate areas designated for different stakeholders. On expiry of the free service period, WEL has proposed FML to enter into a 3 years contract for website administration and maintenance. Under the proposed agreement, WEL would also be responsible to update website as instructed by FML. However, all changes in design would be billed separately.

FML may face the following **risks:**
(i) There may be hidden costs in the contract because of slight changes in the design of a web page WEL may demand substantial fee.
(ii) WEL may not perform timely maintenance which may result in non-availability of the website.
(iii) Service costs may not remain competitive over the period of entire contract.
(iv) FML may become entirely dependent on WEL.

(v) Confidentiality of information may be compromised.

FML could take the following **measures** to mitigate the above risks:
(i) Review the proposal thoroughly as regards the basis of billing for services related to change in design.
(ii) Specify clearly defined performance criteria to ensure quality of services.
(iii) Define penalty in case of non-fulfillment of agreed service levels.
(iv) Ensure that WEL has a sound BCP in place.
(v) Instead of three years contract enter into annual contract and before renewal of contract, make fresh survey of the market as regards the cost of services.
(vi) To reduce dependency on WEL, make back up arrangements. For example, contract with another vendor to handle the website incase contract with WEL is terminated abruptly or develop in-house resources.
(vii) Get Non-disclosure agreement signed from WEL.
(viii) Clearly specify data ownership.

Case study: King Limited (KL) has decided to engage Queen Limited (QL) for maintenance of its IT hardware, including printers, scanners, monitors, network related devices and cabling. Important clauses of the draft Service Level agreement between them are as follows:
(i) The agreement will commence on December 13, 2009 and will be terminated automatically if not formally extended, on December 12, 2010.
(ii) KL will ensure that the equipment will be in proper mechanical and electrical condition on the commencement date. Any work involved in putting the equipment into such condition will be charged separately.
(iii) Fifty visits per annum will be made by qualified technical personnel of QL.
(iv) Emergency visits will be provided as and when required. However, emergency visits made after office hours or on holidays will be charged separately, at the rates prevailing at that time.
(v) Routine maintenance services will be carried out during normal business hours, at regular intervals.
(vi) All faulty parts and consumables will be replaced at extra cost after the approval by KL.
(vii) This agreement does not cover any work necessitated by neglect, misuse, accident or voltage fluctuation.
(viii) QL reserves the right to discontinue services under this agreement whenever it finds that sub-standard or non-genuine supplies are being used thus hampering the proper fulfillment of their responsibilities.
(ix) Payment will be made in advance, on or before the commencement date.

Following **weaknesses** are observed in the SLA of KL with QL:
(i) Performance criteria are not specifically defined. / Service level is not defined.
(ii) Exit root for QL is defined but for KL it is not defined.
(iii) It is not clear that if QL terminated the contract before end date what percentage of payment will be refunded to KL.
(iv) Full payment has been made in advance; in case of poor performance KL can neither easily recover the payment nor be able to deduct any penalty from QL's charges.
(v) Rates for after office hours/holidays emergency visits left unresolved.
(vi) Absence of appropriate penalty clause against non-fulfillment of commitment.
(vii) Interval between routine maintenance of equipment is not defined.
(viii) Number of visits expectation is unrealistic. It is a question of debate as to what the technical persons of QL will do during their 4-5 visits per month.
(ix) Neglect and misuse are open ended terms and should be clearly defined / described.
(x) Maintenance should be performed during off peak hours or after office hours to avoid disruption in normal office activities.

Case Study: ZZ and Company (ZZC) has purchased major shareholding in YYC group which consists of seven manufacturing units, each of which produces different type of products. Each unit has its own IT department. Two units charge out their IT costs on market based method while rest of the units include IT costs as an administrative overhead.
Management of ZZC is planning to make a major re-structuring in all units. In this regard it has planned to establish a centralised IT department and follow a single method for charging out IT costs.

ZZC may gain following **advantages** by establishing a **centralized IT department**:
(i) Uniform security standards can be enforced, and it gives better security/control over the data and files.
(ii) Standardization of IT equipment and IT processes in all units.

(iii) Economies of scale would be available in purchasing computer equipment and supplies.
(iv) IT staff and resources are available at a single location, and more expert staff can be employed. Career paths for IT staff also become available.

ZZC may face following **disadvantages** due to a centralized IT department:
(i) Local offices might have to wait for IS/IT services and assistance.
(ii) A system fault at head office will impact across the organization.
(iii) IT staff redundancy may occur.
(iv) Existing IT staff of branch offices may be demoralized as they may not find future growth prospectus.

Comparative advantages and disadvantages of charging out IT costs as an administrative overhead or on market based methods are as follows:

Administrative overhead	Market based
It is simple and cheap to administer, as there is no charge out system to operate.	It can be difficult to decide on the charge out rate, particularly if there is no comparable service provider outside the organization.
May encourage innovations and experimentation as user-departments are more likely to demand better quality systems if they will not bear any cost.	Unnecessary use of IT resources would be reduced. / Users would avail the IT services when they actually need it.
The relationship between IS staff and user departments is not subject to conflict over costs.	If users feel that rates are excessive, they may reduce their usage to below optimal levels, and relationships between the IS/IT department and user departments may become strained.
Any inefficiencies within the IS/IT department are less likely to be exposed –as user departments will not be monitoring cost levels.	The efficiency of the IT department has to improve otherwise the user departments have the right to demand external standards of service.
User departments may accept sub-standard service, as it is 'free'.	In case of sub-standard services, user departments have the right to demand external standards of service.
It encourages the view that information systems and technology are a drain on resources rather than tools in the quest for competitive advantage.	It encourages as entrepreneurial attitude as IT Manager is in-charge of a profit making department.
A true picture of user department's financial performance is not obtained, as significant costs attributable to that department are held in a central pool.	A true picture of user departments financial performance is obtained – as the IS/IT costs charged to each department are based on market-rates.

The two methods of charging IT costs are as follows:

(i) Market-based charge out method
Under market-based methods, the IT department acts as a profit center. It sets its own prices and charges for its services with the aim of making a profit.

Advantages of the market-based charge out method include:
The efficiency of the IT department has to improve otherwise the user departments have the right to demand external standards of service.
It encourages an entrepreneurial attitude. IT managers are in charge of a department that could make a profit – this helps to motivate them.
A true picture of user department's financial performance is obtained – as the IT costs charged to each department are based on market-rates.

Disadvantages of the market-based charge out method include:
It can be difficult to decide on the charge out rate, particularly if there is no comparable service provider outside the organization.
If user feel rates are excessive, they may reduce their usage to below optimal levels, and relationships between the IS/IT department and user departments may become strained.
Even if the service provided is poor, it may not be in the organization's interest for user departments to buy from outsiders because the IT function's fixed costs still have to be covered.

(ii) Inclusion as an administrative overhead
Under this system IT costs are treated as a general administrative expense, and are not allocated to user departments.

Advantages of this approach are:
- It is simple and cheap to administer, as there is no charge out system to operate.
- May encourage innovations and experimentation as user-departments are more likely to demand better quality systems if they will not bear any cost.
- The relationship between IS staff and user departments is not subject to conflict over costs.

Disadvantages of this approach are:
- User departments may make unreasonable and economically unjustifiable demands.
- Any inefficiencies within the IT department are less likely to be exposed – as user departments will not be monitoring cost levels.
- A true picture of user department's financial performance is not obtained, as significant costs attributable to that department are held in a central pool.

Benefits of Bulk IT procurement process
(i) Standardization of IT equipment.
(ii) Higher discounts.
(iii) Better terms related to support and maintenance.

Drawbacks of Bulk IT procurement process
Purchasing IT equipment for the entire year in one go may not always be advisable, because:
(i)of higher cost of capital (financing).
(ii)warranty of equipment start from the date of delivery, irrespective of the fact whether they are used six or seven months later.
(iii)the equipment may become relatively obsolete by the time it is actually used.

Case Study: As an audit senior of a firm of chartered accountants, you are assigned to conduct an audit of Creative Insurance Company Limited (CICL). CICL places considerable reliance on its computer–based information systems for generation of operational and financial data. CICL has formed a quality assurance (QA) department during the current year to review and monitor its information systems. In the course of your discussions with the QA Manager, you have been told that:
(i) Due to time and resource constraints, QA plans were developed only for those information systems where:
the system is of material significance to the company as a whole;
all the stakeholders agree on the quality goals identified for that information system.
(ii) QA plans will be developed for all the remaining information systems as soon as adequate resources are available and QA department has achieved necessary competencies.
Your review of the project documentation shows that presently 12 out of a total of 20 information systems meet the above criteria. The remaining 8 information systems include 5 financial information systems.

Following **concerns may restrict** my decision to place **reliance on QA function** of CICL:
- The given situation indicates that QA function is not fully equipped with the required resources and has not attained a trusted level of competency.
- The stakeholders' inability to agree on QA goals indicates that information systems objectives have not been clearly set, which may restrict the reliance being placed on them.
- If data produced by a system which has not passed through the QA function is transferred to a system which is QA compliant, we may not be able to place as much reliance on the QA compliant system also.
- Since this is the first year of application of QA function, the auditor has very little experience on which he can assess the reliability of the QA function.
- Since 40% of the systems have not passed through QA test, placing reliance on QA function for the rest may give rise to inconsistent audit approach.

For material information systems where QA plans have been developed but which import data from information systems that do not meet the QA function's criteria, I would:
- test the QA controls of information system which is receiving data;
- test controls of those information systems from whom data is being imported.

If the result of above tests is satisfactory, I would place the reliance on these controls and reduce the extent of substantive testing. Otherwise, I would go for detailed substantive testing.

Case Study: While conducting IS audit of Wonder Bank Limited you have observed the following roles/duties assigned to various users:
(a) Tape Librarian records scheduled backups.
(b) Application Programmers perform changes in test programs.
(c) Operational support staff executes changes in batch schedules.
(d) One of the Application Programmer is also responsible for Security Administration.
(e) Database Administrator performs data entry tasks during peak load period.

Required: Analyze each of the above observations and discuss the risk of fraud/weakness, if any, in each case.

(a)The librarian is required to record, issue, receive and safeguard all programs and data files that are maintained on computer tapes/disks in an Information Processing Facility. Check and balance on currency and completeness of backups stored in the library would be weakened in case if the scheduled backups are recorded by the librarian.
(b) Test programs are used only in development and do not directly impact live processing. Hence there is no risk in this case.
(c) The implementation of changes to batch schedules by operation staff will affect the scheduling of the batches only. It does not impact the live data. Hence there is no risk in this case.
(d) The functions of Application Programmer and Security Administrator are incompatible. The level of security administration access rights could allow changes to go undetected.
(e) The Database Administrator (DA) has the tools to establish controls over the database and the ability to override these controls He has also the capability of gaining access to all data including production data. If data entry is performed by the DA it would contradict separation of duties principle and could compromise confidentiality of data as well.

Case study: You are a member of the team which is conducting the IS audit of Awesome Textiles Limited (ATL). ATL has a well-established IS Department and a dedicated in-house Systems Development team. The key members in the team are System Development Manager, Project Manager, System Analyst and Quality Assurance Manager.
Your team leader has assigned you to evaluate the following risk:
"*New programs or the changes made in existing programs are NOT authorized, tested and documented and may NOT operate as planned*".

Expected controls to mitigate the above risk	**Responsible person**
Development and change requests are documented and approved at an appropriate level.	System Development Manager
Procedure exists for implementing new and amended programs.	
The names/designations of persons authorized to approve amendments in programs is documented.	
The names/designations of persons authorized to make amendments in programs is also documented.	
Procedure exists for transferring copy of source code from production to test environment and vice versa.	
Procedure exists for assigning priorities and monitoring the status of outstanding requests.	Project Manager
Procedure exists for documenting requirement definition for new programs.	System Analyst
Procedure exists for getting system design approval from appropriate level.	
Procedure exists for testing the development and changes in programs.	Quality Assurance Manager
Test results are documented.	
Procedure exists for reviewing new and amended programs before implementation.	
User acceptance testing is documented.	
Procedure exists for reviewing new and amended programs after implementation.	
Appropriate naming convention exists for test and live production programs.	
Log of all changes made to a program during a given time is available.	

Segregation of duties means that important responsibilities are distributed between two or more individuals. As a result check and balances are created as work of one person is checked by the other.
If adequate segregation of duties does not exist, the following could occur:
- Misappropriation of assets OR Chances to fraud increases.
- Inaccurate information (i.e. errors or irregularities remain undetected).
- Modification of data could go undetected.

Separation of Duties Matrix

	System Analyst	SW Developer	Tape Librarian	DB Admin	Security Admin	Network Admin	Help Desk Officer	Data Entry Operator
System Analyst	OK	X	OK	X	OK	X	OK	
SW Developer	OK	X	X	X	X	X	X	
Tape Librarian	X	X	OK	X	X	X	OK	
DB Admin	OK	X	OK	OK	X	X	X	
Security Admin	X	X	X	OK	OK	OK	X	
Network Admin	OK	X	X	X	OK	X	X	
Help Desk Officer	X	X	X	X	OK	X	X	
Data Entry Operator	OK	X	OK	X	X	X	X	

Legend:

OK = Compatible function X = Incompatible function

If the role of Software Developer (SD) is to be combined with the role of Database Administrator (DBA), following compensating **controls** could be implemented to mitigate the associated risks:
(i) Authorization: Mandatory written authorization from supervisory level for every change or amendment in the application program/database structure/database permissions.
(ii) User Logs/Audit Trails: Generating complete un-editable log of DBA's activities. Such logs should not be accessible to DBA and SD and should be reviewed periodically by a supervisory authority.
(iii) Exception reporting: Configure exception reports or alerts for activities other than normal, like overriding database default controls, mismatch application program version etc. These reports should be handled at the supervisory level on priority basis and should require evidence, such as initials on a report, noting that the exception has been handled properly.
(iv) Supervisory reviews: Besides reviewing various logs, other supervisory reviews may also be performed through observation, inquiry and test checks etc.
(v) Independent reviews: Independent reviews may be carried out by internal or external auditor etc.

Suggested **best practices** for **preventing and detecting frauds** that may be committed by key information systems personnel are as follows:
(i) **Carry out periodic enterprise-wide risk assessments**
Periodic risk assessment procedure helps to identify risks which may result in loss to the organization.
(ii) **Clearly document insider threat controls.**
Clear documentation helps to ensure fewer gaps for attack and better understanding by employees.
(iii) **Carry out periodic security awareness training for all employees**
If the employees are trained and understand security policies and procedures, and why they exist, they will be encouraged and able to avert security lapses.

(iv) **Implement strict password and account management policies and practices**
Password controls and account management policies are often not followed to avoid inconvenience. Without strict implementation such controls are of no use.
(v) **Log, monitor, and audit online actions of the employees**
Periodic logging, monitoring and auditing discourages and discovers inappropriate actions.
(vi) **Use extra caution with system administrators and privileged users**
Typically, logging and monitoring is performed by a combination of system administrators and privileged users. Therefore, additional vigilance must be devoted to those users.
(vii) **Monitor and respond to suspicious or disruptive behavior**
Policies and procedures should be in place for all employees to report such behavior, with required follow-up by management.
(viii) **Physical controls**
Close circuit cameras, biometrics and digital door locks etc. serve a good physical control against insiders' threat.
(ix) **Deactivate computer access immediately after termination**
Immediate deactivation policy will discourage losses due to lapses and slackness.
(x) **Job rotation**
Periodical rotation of responsibilities enhances the check and balance environment. It helps in detecting errors and irregularities which otherwise remain undetected.
(xi) **Forced leave policy**
Mandatory leave policy helps in successful succession planning. It also tests the organization's preparedness in case its key IT personnel left.
(xii) **Restricted use of removable media**
This practice helps in minimizing the chances of virus and worms in the system. It also mitigates the chances of theft of sensitive data.
(xiii) **Access to sensitive data/ information on need to have basis**
This practice enhances the security and confidentiality of data. Since access to data is allowed on proper authorization, track of any modification to it can be detected easily.

List of documents along with their significance that an IS Auditor should review while auditing information processing facility is as follows:

Documents	Significance for IS Auditor
IT strategy, IT plans and IT budgets	These documents provide evidence of planning and management's control of the IS environment. They help to assess the alignment of IT strategy with the business strategy.
Security policy	It identifies the security standards followed by the organisation. It helps to assess the position of the organisation with regard to security risks. It identifies the implemented controls and actions to be taken in case of security violation/breach.
Organisation/functional chart	It provides an understanding of the reporting line within IT department or organisation. It illustrates a division of responsibility and gives an indication of the degree of segregation of duties.
Job descriptions	They help to understand the functions and responsibilities of positions throughout the organisation. They help to verify that the level of reporting relationships are based on sound business concepts and do not compromise the segregation of duties.
Steering committee reports	They provide information regarding on-going and new system projects. They provide information about major acquisitions of IT assets. They give an idea about overall IS performance.
System development, and program change procedures	They identify the framework within which system development or program changes are

	undertaken. □ Assess the adequacy of change management controls.
Human resource manuals	□ They provide the rules and regulations determined by an organisation for how it expects its employees to conduct themselves. □ Assess the degree of alignment between IT objectives and HR rules and regulations.
Risk management/disaster recovery/business continuity management procedures/manuals	□ They help in quick assessment of identified risks and implemented controls. □ They help in assessment of adequacy of implemented controls. □ They help in assessing organisation's resilience against identified threats.

Document	**Target Information**	**Purpose for which the information would be used by IS Auditor**
IT strategies and plans	• Details of management strategies and plans like: o IT objectives /targets o Long term/short term plans o Required resources	• Weather IT strategy is aligned with business strategy. • Assessing effectiveness of long term planning. • Assessing adequacy of requirement analysis. • Assessing effectiveness of capacity management.
IT budgets	• Allocated funds / Comparison of actual fund utilised last year with allocated funds • Details of cost of procurement, and other recurring costs.	• Assessing the adequacy of budget. • Instances of budget overruns. • Assessing effectiveness of resource utilisation.
Security policy	• Details of security plans and standards introduced by the management.	• Assess whether the security policy is comprehensive enough to cater to all current and anticipated risks (adequacy of controls). • Assessing whether regular updation and documentation of key policies is being carried out.
Business Continuity Plan	• Evidence of the process of risk assessment. • Disaster recovery procedures and plan • Evidence of testing and updation. • List of key persons.	• Assess effectiveness and adequacy of plan. • Assess adequacy of procedures. • Assess the level of awareness among the staff regarding their roles and responsibilities.
Organizational structure of IT department	• Management reporting lines • Structure of segregation of duties	• Identify persons responsible for the safeguarding of IT assets • Identify possible conflicting duties • Identify possible reliance on one or two key personnel or lack of succession plans.

IT Steering Committee membership should include the following:
(i) Representative from senior management such as COO, CEO, MD etc.
(ii) Representative from user management such as Production Manager, Sales Manager etc.
(iii) Key advisors from IT, Audit, Finance and Legal departments
Although not a common practice, a member of the board of directors may be included as chair of this committee. However, it is highly desirable that he/she should understand the risks and issues related to information technology.

Common responsibilities of an IT Steering Committee are as follows:
(i) Review the long and short range plans of the IT department to ensure that they are in accordance with the corporate objectives.
(ii) Review and approve major acquisitions of hardware and software within the limits approved by the board of directors.
(iii) Approve standards and procedures
(iv) Approve and monitor major projects and the status of IT plans and budgets.
(v) Review and approve sourcing strategies including insourcing or outsourcing and the globalisation or offshoring of functions.
(vi) Review adequacy and allocation of resources in terms of time, personnel and equipment.
(vii) Make decisions regarding centralisation vs. decentralisation.
(viii) Support development and implementation of an enterprise-wide information security management program.
(ix) Monitor overall IT performance.
(x) Report to the board of directors on IT activities.

IT Governance covers following **domains**:
(i) **Strategic Alignment**, focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.
(ii) **Value Delivery**, is about executing the value proposition throughout the delivery cycle, ensuring that IT is delivering the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
(iii) **Risk Management**, requires awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.
(iv) **Resource Management**, is about the optional investment in, and the proper management of, critical IT resources i.e. applications, information infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.
(v) **Performance Measurement**, tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting..

	Responsibilities of IT Head	***Co-operation from Management and Other Departments***
Strategic Alignment	Assist the IT strategy Committee in formulating the overall IT Strategy.	Give due weightage to IT head's recommendations.
Value Delivery	Ensuring timely completion of the project and fulfilling the users need with utmost cost effectiveness.	Management taking due interest and prompt feedback by the users.
Risk Management	Playing a key role in the formulation of a Business Continuity Plan. Clearly communicating the IT related risks. Identifying weaknesses promptly.	Management's active participation in ensuring that non-compliance to controls is strongly discouraged.
Resource Management	Updating the knowledge of IT Department. Proper capacity planning. Preventive maintenance.	Comply with the suggested procedures and controls. Provide resources for training of staff.
Performance measurement	Defining key performance indicators for IT functions and personnel.	Giving due weightage to IT head's recommendations when deciding upon the issue of compensation packages of IT related personnel.

Help Desk:
Following **functions** are usually supported through help desk:
(i) Installation of hardware and software upgrades.

(ii) Assisting end users in resolving issues related to hardware and software.
(iii) Informing end users about problems with hardware and software that may be foreseen in view of any specific situation.
(iv) Monitoring technological developments and informing end users of developments that might be pertinent to them.

The **critical requirements** for **efficient and effective working** of the help desk function are as follows:
(i) Support staff must be knowledgeable about the diverse range of systems used throughout the organization.
(ii) They must have a high level of interpersonal skills in order to interact effectively with users.
(iii) They must show empathy, for example, when users encounter problems.
(iv) The system should maintain a log of all difficulties reported and how they were resolved.
(v) The procedures for assignment of tasks should be well defined.
(vi) Time schedule of staff duties should be well defined.
(vii) If a response is not provided within the designated time period, the system should alert the manager of the help desk area.
(viii) Management's commitment to support Help Desk function.

The information required to evaluate the Help Desk function can be gathered through the following:
(i) **Interviews**
End users can be interviewed to determine their level of satisfaction with the service provided by the help desk.
(ii) **Observations**
Help Desk personnel may be observed to see how they respond to user queries.
(iii) **Review of documentation**
Logs maintained by the help desk reporting system may be reviewed to determine whether accurate, complete and timely responses are being provided.

Major steps for a **'security incident handling and response' mechanism** in an organization are:
Planning and preparation – Preparing a plan and strategy for possible security incidents that the organization's IT assets may face.
Prevention – Devising controls and processes to prevent security incidents.
Detection – Devising mechanism for detection of security incidents.
Initiation/Reporting – Devising process / mechanism by which a security incident could be reported.
Evaluation – Devising a mechanism for evaluating the reported security incident (its nature, criticality, possible consequences, etc.).
Containment – Devising a mechanism to contain the negative effects of security incidents.
Recovery – Devising the process of going back to normal operations.
Post-incident review – Devising the mechanism to assess things like why it happened? What should be done to avoid that? Was our response correct?
Lessons Learned – Developing a mechanism of documenting the overall incident for reference at a later stage.

Identification of two major **responsibilities** related to risk management
Board of Directors
- Establishing the policy of risk management in all activities.
- Ensuring regulatory compliance.

Steering Committee
- Identifying emerging risks.
- Identify compliance issues.

Executive Management
- Ensuring that all roles and responsibilities of the organization include risk management.
- Promoting business unit security policies.

Chief Information Security Officer
- Implementing the risk management policies.
- Advising concerned personnel on risk management issues. / Users training.

<u>Bespoke/Customized software:</u>
The option to appoint an Application Service Provider may prove to be more feasible for TDL on account of the following:

(i) ASP may prove economical, since software costs for the application are spread over a number of clients.
(ii) ASP's software is developed by experts who have considerably more application development experience than in house staff.
(iii) There is a strong possibility that system testing / implementation time will be reduced considerably since most of the ASP's software programs are tested and running at other clients' locations.
(iv) Systems will be kept up to date.
(v) A certain level of service can be ensured through Service Level Agreement.
(vi) Immediate problem resolution and better technical support.
(vii) ASP may keep TDL updated on latest technology and available products.
(viii) Internal IT costs shall be reduced to a predictable monthly fee.
(ix) IT staff and tools may be redeployed to focus on core issues.

TDL should pay special attention to the following factors while finalizing arrangements with an ASP:
(i) The cost and benefit analysis should be carefully planned.
(ii) Consider the viability of the ASP i.e. its financial position, experience, customers' response.
(iii) How will the sales and inventory system designed by the ASP, integrated with other systems?
(iv) How easy/costly would it be, to revise the software, whenever required?
(v) How the security of data be ensured?
(vi) Ensure the inclusion of an appropriate clause in the SLA relating to maintenance of confidentially.
(vii) Who will own the data which will be generated during the operation of the software?
(viii) The degree of assurance provided by the ASP as regards the uninterrupted availability of services.
(ix) What back-up support will the ASP provide in case of failure of the application?
(x) What other supports (training, troubleshooting, consulting) will the ASP provide?
(xi) The impact of a situation in which the ASP may intentionally hold its services.
(xii) Mechanism to resolve mutual disputes.
(xiii) What compensation will be provided in case TDL suffers loss on account of malfunctioning of the software?
(xiv) Terms and conditions related to termination of agreement.
(xv) Ensure the inclusion of an appropriate clause for having rights to audit the data and the software.
(xvi) If the ASP goes out of business or is unable to provide services to TDL during the contract period, TDL should have right to access the source code.
(xvii) Get the SLA scrutinized by a legal consultant.

Drawbacks of ASPs include:
(i) ASP may not provide a customized solution for such a small project and TDL might be required to accept the application as provided.
(ii) Increased reliance on an ASP specially in case of critical business functions like sales and inventory management may not be advisable.
(iii) Changes in the ASP market may result in changes in the type or level of service available to clients.
(iv) TDL may face problems when it may want to integrate its non-ASP based systems with the systems being run by the ASP.

Case Study: Black Steel Limited (BSL) is a manufacturer of industrial and domestic steel products. It has a network of 225 computers and relies heavily on its IT system for production, sales and recovery. Due to emerging requirements, the management is considering to replace its existing application program (information system) which was developed inhouse 15 years ago using ABC Pro 6.0 development toolkit. The system had been updated from time to time as per users' requirements. However, it is still based on ABC Pro 6.0 despite the fact that now ABC Pro 9.5 is available.

BSL may face following **problems** if it continues with its existing application program:
(i) When a new version of a development tool is introduced, various efficiencies are introduced. Hence BSL may not be utilizing the available potential.
(ii) The legacy system may not be able to integrate any new system acquired by BSL.
(iii) Since the system has not been upgraded to the latest version of the development tool, it may not be able to counter emerging security threats.
(iv) The system has been developed in-house fifteen years ago and apparently requires specialised knowledge to maintain it in a condition suitable for operation. This may leave BSL exposed should certain staff leave for example, the IT head or the programmer who was part of the development team.

BSL may face following **issues** if it decides to **replace** its existing application program:
(i) It may face resistance from administrative and support users, as they have expert knowledge of existing system and would need to learn the new system from scratch.
(ii) Cost of replacement would be high as significant time and effort would be involved in introducing the new system.
(iii) Ensuring integrity, accuracy and completeness of data migrated to new system would be challenging. For example, automated file conversion procedures may not be applicable due to system compatibility and data issues.
(iv) Some of the staff may become redundant with the replacement of legacy system.

Following **controls** should be considered while **hiring an IT personnel**:
(i) Reference checks.
(ii) Confidentiality agreement.
(iii) Employee bonding to protect against losses due to theft, mistakes and neglect.
(iv) Conflict of interest assessment.
(v) Undertaking to abstain from carrying on any other job/business, including any other activity which may be in conflict of interest of the organization.

Following control procedures should be followed when the **IT staff leaves**:
(i) Return of all keys, ID card and badges.
(ii) Deletion of assigned logon IDs and Passwords.
(iii) Notification to appropriate staff and security personnel.
(iv) Arrangement of the final pay routines.
(v) Exit interview.
(vi) Return of all company property.
(vii) Handing and taking over of responsibilities and assignments.

Case Study: Information related to BSL's IT department is as follows:
The department is headed by a seasoned IT professional for the past 17 years. He is due to retire after three months and management is looking for his replacement.
One of the programmers who developed the application program is still in the company and performs the functions of database administrator besides maintenance of application program.
Network administrator is responsible for backup of data and maintenance of network besides planning, implementing and maintaining BSL's telecommunication infrastructure.
Record of end user support provided by IT department is not kept.

Based on the given information, following **issues** are evident in the IT department of BSL:
(i) IT has been headed by the same person for past 17 years but his successor has not been developed. This shows lack of succession planning.
(ii) It appears that management is inclined to appoint the IT head from outside BSL, this may lead to resistance or non-cooperation from senior staff of IT department.
(iii) The functions performed by the programmer are incompatible and in violation of segregation of duties.
(iv) In the absence of support record it would be difficult to:
- identify the most problem hit area and avoid the recurrence of problems
- measure the efficiency/performance of IT support personnel

Q. You have recently assumed the responsibility of HR Head of Tarseel Couriers and found that most of the IT staff is not satisfied with their appraisal. You noticed that job descriptions and annual objectives/key goals do exist for each employee but the staff appraisal system is quite judgmental.
Required:
(a) Write a memo to the Chief Executive Officer briefly explaining the need to define Key Performance Indicators (KPIs) and their main characteristics. (05)
(b) Identify any two KPIs for each of the following goals/objectives set for the IT head:
(i) Effectively manage ongoing and upcoming IT projects.
(ii) Effective knowledge transfer for smooth system operations and use.
(iii) Improve IT's cost efficiency and its contribution to business profitability.
(iv) Ensure the confidentiality of critical information. (08)

(a) To: The Chief Executive Officer

From: HR Head
Subject: Need to define Key Performance Indicators
Date: December 8, 2015
On reviewing the appraisal system of our company, I am pleased to note that job description and annual goals/objectives of all employees are in place. However, evaluation of staff performance is judgmental. To avoid a judgmental evaluation we may define Key Performance Indicators (KPIs) which are measurable and comparable and improve the appraisal system.
Effective KPIs have the following characteristics:
(i) Have a high insight-to-effort ratio (i.e., insight into performance and the achievement of goals as compared to effort to capture them)
(ii) Are comparable internally (e.g., percent against a base over time).
(iii) Are comparable externally irrespective of enterprise size or industry.
(iv) Are easy to measure and are not confused with targets.
(v) Are either based on time or based on quantity.

Regards

(b)	Goals	KPIs
(i)	Effectively manage ongoing and upcoming IT projects	□ Percentage of IT projects completed on time □ Percentage of IT projects completed within budget
(ii)	Effective knowledge transfer for smooth system operations and use	□ Percentage of IT applications with adequate user and operational support training □ Number of incidents caused by deficient user and operational documentation and training
(iii)	Improve IT's cost efficiency and its contribution to business profitability	□ Percentage of reduction (increase) of the unit cost of the delivered IT services □ Percentage of IT expenditure expressed in business value drivers (e.g., service increase due to increased connectivity)
(iv)	Ensure the confidentiality of critical information	□ Number of instances where confidential information was compromised □ Number of adverse comments by Internal/external auditor over sufficiency/insufficiency of controls for maintaining confidentiality

Q. Brilliant Bank Limited is a large commercial bank. It has a progressive management which seeks pride in offering innovative services to its clients. New applications are developed on a regular basis with the objective of achieving high degree of customer satisfaction. On the recommendation of the newly appointed HR Director, the management wants to develop Key Performance Indicators (KPIs) in all critical areas.
Required:
List any three KPIs in respect of each of the following areas:
(a) IT projects performance
(b) IT operational support
(c) IT infrastructure availability
(d) IT security environment

(a) **Project performance**
(i) Ratio of projects completed on time.
(ii) Ratio of projects completed within budget.
(iii) Ratio of projects meeting functionality requirements. / Users' satisfaction rating.

(b) **IT operational support**

(i) Average time taken to respond to customers' complaints.
(ii) Ratio of number of problem reported and resolved/unresolved.
(iii) Percentage of customers' satisfaction over support services. (through survey form)

(c) **IT infrastructure availability**
(i) Number of system downtime (per unit time i.e. per hour, per day, per week etc.)
(ii) Mean time between failures.
(iii) Number of customers' complaints about non-availability of online facilities.

(d) **IT security environment**
(i) Percent increase/decrease in security breaches/incidents reported.
(ii) Mean time to resolve critical security issues.
(iii) Level of customers' awareness of risks and controls. (through survey form).