6. BPA RISKS & CONTROLS

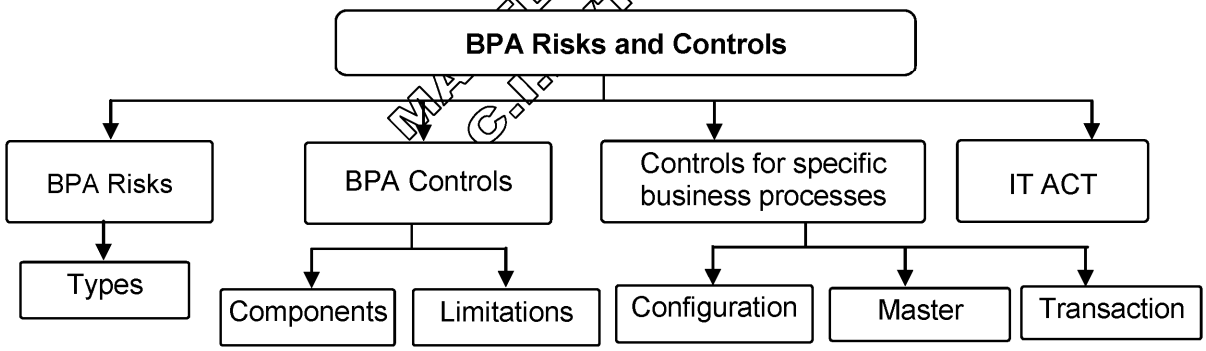
QUESTION WISE ANALYSIS OF PREVIOUS EXAMINATIONS

No.	M-14	N-14	M-15	N-15	M-16	N-16	M-17	N-17	M-18 (O)	M-18 (N)	N-18 (O)	N-18 (N)	M-19 (O)	M-19 (N)	N-19 (O)	N-19 (N)	N-20 (O)	N-20 (N)
THEORY QUESTIONS FOR CLASSROOM DISCUSSION																		
16.	-	-	-	-	-	-	-	-	-	-	-	-	-	5	-	-	-	-
20	-	-	-	-	-	-	-	-	-	5	-	-	-	-	-	-	-	-
22.	-	-	-	-	-	-	-	-	-	-	-	-	-	5	-	-	-	-
27.	-	-	-	-	-	-	-	-	-	5	-	-	-	-	-	-	-	-

CHAPTER OVERVIEW

SECTION	TOPIC	STARTING PAGE NO.
1.	THEORY FOR CLASSROOM DISCUSSION	6.1
2.	QUESTIONS FOR ACADEMIC INTEREST FOR STUDENTS SELF STUDY	6.18

SECTION 1: THEORY FOR CLASSROOM DISCUSSION



PART 1: RISKS IN BPA OF IS

Q.No.1. Define Risk. What are the sources and characteristics of risks? (C)

RISK: Risk is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence.

SOURCES OF RISKS: Some of the common sources of risk are Commercial and Legal Relationships, Economic Circumstances, Human Behavior, Natural Events, Political Circumstances, Technology and Technical Issues, Management Activities and Controls, and Individual Activities.

BROADLY, RISK HAS THE FOLLOWING CHARACTERISTICS:

1) Potential loss that exists as the result of threat/vulnerability process;
2) Uncertainty of loss expressed in terms of probability of such loss; and
3) The probability/likelihood that a threat agent increasing a specific attack against a particular system.

SIMILAR QUESTION:

1. **Risk is a part of all aspects of everyday life. Development of an informational system is a complex process, which makes it submissive to a great number of risks. Many projects do not achieve previously set goals; therefore risk management is not to be ignored in the development of informational systems. Then make a brief note on Risk, its sources and characteristics.**

A. **Refer above answer.**

Q.No.2. Write about the classification of risks. (C)

The risks broadly can be categorized as follows:

1) ***Business Risks:*** Businesses face all kinds of risks related from serious loss of profits to even bankruptcy
2) **Technology Risks:** The dependence on technology in BPA for most of the key business processes has led to various challenges. As Technology is taking new forms the enterprises should consider the new set of IT risks and challenges
3) ***Data related risks:*** These include Physical access of data and Electronic access of data.

SIMILAR QUESTION:

1. **Risk can be referred to like the chances of having an unexpected or negative outcome. Any action or activity that leads to loss of any type can be termed as risk. There are different types of risks that a firm might face and needs to overcome. Widely, risks can be classified into three types what are they?**

A. **Refer above answer**

Q.No.3. Businesses face all kinds of risks related from serious loss of profits to even bankruptcy then write about business risks? (B)

BUSINESS RISKS: Businesses face all kinds of risks related from serious loss of profits to even bankruptcy.

THE BUSINESS RISKS ARE DISCUSSED BELOW:

1) **Strategic Risk:** These are the risks that would prevent an organization from accomplishing its objectives. Examples include risks related to strategy, political, economic, regulatory, and global market conditions and reputation risk;
2) **Financial Risk:** These Risks could result in a negative financial impact to the organization Examples include risks from volatility in foreign currencies, interest rates etc.,
3) **Regulatory (Compliance) Risk:** These Risks could expose the organization to fines and penalties due to non-compliance with laws and regulations. Examples: environmental, employee health and safety etc.,
4) **Operational Risk:** These Risks could prevent the organization from operating in the most effective and efficient manner or they can be disruptive to other operations. Examples: risks related to the organization's human resources, business processes, technology, business continuity etc.,
5) **Hazard Risk:** These Risks are insurable, such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism etc.
6) **Residual Risk:** Any risk remaining even after the counter measures(=an action taken against an unwanted action or situation) are analyzed and implemented is called Residual Risk. Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level the risk can be managed.

SIMILAR QUESTION:

1. **Running a business comes with many different types of risk. Some of these potential hazards can destroy a business while others can cause serious damage that can be costly and time-consuming to repair. Despite the risks implicit in doing business, CEOs and risk management officers can anticipate and prepare for potential risks regardless of the size of the business. Then what kinds of business risks are faced by the organizations give a detailed note of them?**

A. **Refer above answer.**

2. **As an entrepreneur, your business may face all kinds of risks related from serious loss of profits to even bankruptcy. What could be the possible Business Risks?**

A. **Refer above answer.**

Q.No.4. As Technology is taking new forms and transforming as well, the business processes and standards adapted by enterprises should consider these new set of IT risks and challenges then Write about technology risk in BPA? (A)(RTP-M18)

TECHNOLOGY RISK: The dependence on technology in BPA for most of the key business processes has led to various challenges, as technology is taking new forms the enterprises should consider these new set of IT risks and challenges

1) **DOWNTIME DUE TO TECHNOLOGY FAILURE:** Information system facilities may become unavailable due to technical problems or equipment failure. A common example of this type failure is non-availability of system due to server failure.

2) **FREQUENT CHANGES OR OBSOLESCENCE OF TECHNOLOGY**: Technology is dynamic and becomes outdated very quickly. Hence, there is always a risk of obsolescence in technology investment.

3) **MULTIPLICITY AND COMPLEXITY OF SYSTEMS:** Personnel should have necessary technology skills because technology includes multiple digital platforms and is quite complex.

4) **DIFFERENT TYPES OF CONTROLS FOR DIFFERENT TYPES OF TECHNOLOGIES/ SYSTEMS:** using technology can pose new risks which need to be reduced by proper controls.

5) **PROPER ALIGNMENT WITH BUSINESS OBJECTIVES AND LEGAL / REGULATORY REQUIREMENTS:** Organizations must ensure that the systems implemented, cater to all the business objectives and needs, in addition to the legal/regulatory requirements envisaged(=to imagine or expect something in the future)

6) **VENDOR RELATED CONCENTRATION RISK:** For various services organizations can either depend on a single vendor or multiple vendors. For example, network, hardware, system software and appliation software services. Both these situations result in higher risks due to heavy dependence on vendors.

7) **SEGREGATION OF DUTIES (SOD):** The segregation (=separation) of duties should be clearly represented in the IS used by the organization. SoD conflicts are high-risk areas and can be a possible reason for fraudulent activities.

8) ***DEPENDENCE ON VENDORS DUE TO OUTSOURCING OF IT SERVICES****: IT implementation by the organization requires staff with specialized domain skills. Hence, these services could be outsourced to several vendors. Heavy dependence on vendors gives rise to vendor risks, which should be managed by proper contracts, controls and monitoring.*

9) ***EXTERNAL THREATS LEADING TO CYBER FRAUDS/ CRIME*** *Making the information available to outsiders is business imperative(=extremely important) but this is also fraught(=Serious and unpleasant) with risks of increased threats from hackers and others who could access the software to commit frauds/crime.*

10) ***HIGHER IMPACT DUE TO INTENTIONAL OR UNINTENTIONAL ACTS OF INTERNAL EMPLOYEES:*** *Employees in a technology environment are the weakest link(=least dependable) in an enterprise.*

11) ***NEW SOCIAL ENGINEERING TECHNIQUES EMPLOYED TO ACQUIRE CONFIDENTIAL CREDENTIALS:*** *Fraudsters use new social engineering techniques such as socializing with employees and extracting information which is used in an unauthorized way to commit frauds*

12) ***NEED FOR GOVERNANCE PROCESSES TO ADEQUATELY MANAGE TECHNOLOGY AND INFORMATION SECURITY:*** *As Technology, has become key enabler for business and is implemented across the organization, senior management should be involved in directing how technology is deployed(=used) in and approve appropriate policies.*

13) ***NEED TO ENSURE CONTINUITY OF BUSINESS PROCESSES IN THE EVENT OF MAJOR EXIGENCIES:*** ***A*** *documented business continuity plan with adequate technology and information systems should be planned, implemented and monitored.*

SIMILAR QUESTION:

1. **Technology is the enabler of business process automation (BPA), and it can automate workflows to the point where human intervention is unnecessary. Automation can save time and money, delight customers who no longer have to wait**

in line for a person to assist them with a transaction, and preclude human error. But automating business processes using technology has its fair share of risks which are to be focused, make a list of probable technology risks of BPA.

A. Refer above answer.

Q.NO.5. Define various terminologies relating to risk management. (B)

VARIOUS TERMINOLOGIES RELATING TO RISK MANAGEMENT ARE GIVEN AS FOLLOWS:

1) **RISK MANAGEMENT:** Risk Management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. It involves identifying, measuring, and minimizing uncertain events affecting resources.
2) **ASSET:** Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees.
3) **VULNERABILITY:** Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. Ex., *Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.*
4) **THREAT:** Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat.
5) **EXPOSURE:** An exposure is the extent of loss the enterprise has to face when a risk materializes. For example - loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources etc.
6) **LIKELIHOOD:** Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event.
7) **ATTACK:** An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.
8) **COUNTER MEASURE:** An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure.

Q.No.6. Effective risk management begins with a clear understanding of an enterprise's risk appetite and identifying high-level risk exposures. After defining risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Then write about risk management strategies? (B)(RTP-M20)

When risks are identified, and analyzed, it is not always appropriate to implement controls to counter them.

Some risks may be minor, and it may not be cost effective to implement expensive control processes for them.

RISK MANAGEMENT STRATEGY IS EXPLAINED AND ILLUSTRATED BELOW:

1) **TOLERATE/ACCEPT THE RISK:** In the case of Minor risks, consciously accepting the risk as a cost of doing business is appropriate. The risks should be reviewed periodically to ensure that their impact remains low.
2) **TERMINATE/ELIMINATE THE RISK:** Risks associated with the use of a technology, supplier, or vendor can be eliminated by replacing the technology with more robust(=Strong) technology products and by seeking more capable suppliers and vendors.
3) **TRANSFER/SHARE THE RISK:** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.
4) **TREAT/MITIGATE THE RISK:** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
5) **TURN BACK:** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

SIMILAR QUESTION:

1. A risk management strategy provides a structured and coherent approach to identifying, assessing and managing risk. It builds in a process for regularly updating and reviewing the assessment based on new developments or actions taken. A risk management strategy can be developed and implemented by even the smallest of groups or projects or built into a complex strategy for a multi-site international organization. What are the probable risk management strategies that can be adopted by the organizations?

A. Refer above answer.

Q.No.7. Define the term RISK? Explain different Risks of Business Process Automation? (A)(MTP-M19)

DEFINITION OF RISK: Risk is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence.

BPA gives significant benefits as well as some inherent risks to enterprises.

THE RISKS OF BPA ARE CLASSIFIED BELOW:

1) **Input & Access:** Always Input data may not be accurate, complete and authorized .
2) **File & Data Transmission:** Due to network errors, files and data transmitted may not be processed accurately and completely.
3) **Processing:** Although input data is valid it may not be processed accurately and completely due to program error or bugs.
4) **Output:** Output may not be complete and accurate due to program error or bugs and it may be distributed to unauthorized personnel due to weak access controls.
5) **Data:** Master data and transaction data may be changed by unauthorized personnel due to weak access controls.
6) **Infrastructure:** The business could stop if there is no proper backup in the event of a disaster so that all data & programs could be lost.

SIMILAR QUESTION:

1. Any business organization trying to adopt BPA should not only know the advantages but also the inherent risks involved in this context list out the risks of BPA.

A. Refer above Answer.

PART 2: CONTROLS IN BPA

Q.No.8. Define control. How controls are classified based on their mode of implementation? (C)

Control is defined as policies, procedures, practices and organization structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.

Based on the mode of implementation, controls can be

1) Manual,
2) Automated or
3) Semi- Automated (partially manual and partially automated).

The objective of a control is to mitigate the risk.

Q.No.9. Explain the Importance of IT Controls (B)

IT Control objectives is defined as: "A statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity".

THE IMPORTANCE OF IT CONTROLS IS AS FOLLOWS:

1) Implementing right type of controls is responsibility of management.
2) Controls provide a clear policy and good practice for directing and monitoring performance of IT to achieve enterprise objectives.

3) IT Controls perform dual role:
   a) They enable enterprise to achieve objectives; and
   b) They help in mitigating risks.
4) Many issues drive the need for implementing IT controls like the need to control costs and remain competitive to the need for compliance with internal and external governance.
5) IT controls promote reliability and efficiency and allow the organization to adapt to changing risk environments.
6) Resiliency is a result of a strong system of internal controls which enable a well-controlled organization-to manage challenges or disruptions seamlessly (=smoothly, faultlessly).

SIMILAR QUESTIONS:

1. **IT controls are essential to protect assets, customers, partners, and sensitive information; demonstrate safe, efficient, and ethical behavior; and preserve brand, reputation, and trust. In business and accounting, information technology controls (or IT controls) are specific activities performed by persons or systems designed to ensure that business objectives are met. Then how Controls are really important in IT?**

A. **Refer above answer.**

Q.No.10. Write about Information Technology General Controls (ITGC)? (B)

ITGC also known as Infrastructure Controls pervade (=spread through) across different layers of IT environment and information systems and apply to all systems, components, processes, and data for a given enterprise or systems environment.

GENERAL CONTROLS INCLUDE:

1) **Information Security Policy:** The security policy is approved by the senior management and encompasses all areas of operations and drives (=handles) access to information across the enterprise and other stakeholders.
2) **Administration, Access, and Authentication:** IT should be managed by clearly defining the levels of access to information and authentication of users.
3) **Separation of key IT functions:** Secure implementation of IT requires separate IT organization structure with key separation of duties to avoid SoD conflicts.
4) **Management of Systems Acquisition and Implementation:** Management should establish acquisition standards and the process of acquisition and implementation of systems should be properly controlled.
5) **Change Management:** Smooth changeover to new environments covering all key changes including hardware, software and business processes should be ensured.
6) **Backup, Recovery and Business Continuity:** Appropriate business continuity plan including backup, recovery and off-site data center should be ensured. Business continuity controls ensure that an organization can prevent interruptions (violations) and processing can be resumed in an acceptable period of time.
7) **Proper Development and Implementation of Application Software:** Application software drives the business processes .These solutions in case developed and implemented must be properly controlled by using standard software development process.
8) **Confidentiality, Integrity and Availability of Software and data files:** Security is implemented to ensure Confidentiality, Integrity and Availability of information. **Confidentiality** refers to protection of critical information .**Integrity** refers to ensuring authenticity of information at all stages of processing. **Availability** refers to ensuring availability of information to users when required.
9) ***Incident response and management:*** *At times of IT failure, the incidents need to be appropriately responded and managed as per pre-defined policies and procedures.*
10) ***Monitoring of Applications and supporting Servers:*** *The Servers and applications running on them are monitored to ensure that servers, network connections and application software along with the interfaces are working continuously.*

11) ***Value Add areas of Service Level Agreements (SLA):*** *SLA with vendors is regularly reviewed to ensure that the services are delivered as per specified performance parameters.*

12) ***User training and qualification of Operations personnel:*** *The personnel deployed have required competencies and skill-sets to operate and monitor the IT environment.*

SIMILAR QUESTIONS:

1. **General Controls are pervasive controls and apply to all the components of system, processes and data for a given enterprise or systems environment. As an IT consultant, discuss some of the controls covered under general controls which you would like to ensure for a given enterprise.**

A. **Refer above answer.**

2. **IT general controls are pervasive in today's organizations. They apply to all systems environments, components, processes, and data, and can be relevant to practically any audit engagement. The implementation of ITGC controls is a regulatory obligation for large companies. These controls are audited annually during the statutory auditors' audit of the financial statements. Then make a list of the components of ITGC policy of an organization.**

A. **Refer above answer.**

Q.No.11. Write about Application Controls and give some examples. (A)

1) Application Controls are controls which are implemented in an application to prevent or detect and correct errors. These controls are in-built in the application software to ensure accurate and reliable processing.

2) These are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing.

3) For example: In banking, application software ensures that only transactions of the day are accepted by the system. Withdrawals are not allowed beyond limits, etc.

SOME EXAMPLES OF APPLICATION CONTROLS ARE AS FOLLOWS:

1) Data edits (editing of data is allowed only for permissible fields);

2) Separation of business functions (e.g., transaction initiation versus authorization);

3) Balancing of processing totals (debit and credit of all transactions are tallied);

4) Transaction logging (all transactions are identified with unique id and logged);

5) Error reporting (errors in processing are reported); and

6) Exception Reporting (all exceptions are reported).

SIMILAR QUESTIONS:

1. **An example of an application control is the validity check, which reviews the data entered into a data entry screen to ensure that it meets a set of predetermined range criteria. Or, a completeness check will examine a data entry screen to see if all fields have an entry. An authorization control ensures that only** authorized **users are gaining access to the database. Application controls, which may be manual or programmed, are designed to ensure the completeness and accuracy of the accounting records and the validity of the entries made. In this context, write about application controls citing some examples.**

A. **Refer above answer.**

Q.No.12. What are the Key indicators of effective IT controls? (B)

KEY INDICATORS OF EFFECTIVE IT CONTROLS:

1) The ability to execute and plan new work such as IT infrastructure upgrades required to support new products and services.

2) Development projects that are delivered on time and within budget, resulting in cost-effective and better product and service offerings compared to competitors.

3) Ability to allocate resources predictably.

4) Consistent availability and reliability of information and IT services across the organization and for customers, business partners, and other external interfaces.

5) Clear communication to management of key indicators of effective controls.

6) The ability to protect against new vulnerabilities and threats and to recover from any disruption of IT services quickly and efficiently.

7) The efficient use of a customer support center or help desk.

8) Heightened security awareness on the part of the users and a security conscious culture.

SIMILAR QUESTIONS

1. **Presence of controls in a computerized system is significant from the audit point of view as these systems may allow duplication of input or processing, conceal or make invisible some of the processes, and in some of the audited organizations where the computer systems are operated by third party service providers employing their own standards and controls, making these systems vulnerable to remote and unauthorized access. Then what are the key indicators of effective IT controls in organizations?**

A. **Refer above answer.**

Q.No.13. Explain Framework of Internal Control as per Standards on Auditing. (C)

SA 315 defines the system of Internal Control as

1) *"The process designed, implemented and maintained by those*

2) *charged with governance, management and other personnel*

3) *to provide reasonable assurance*

4) *about the achievement of an entity's objectives*

5) *regarding reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws and regulations."*

AN INTERNAL CONTROL SYSTEM -

1) Facilitates the effectiveness and efficiency of operations.

2) Helps ensure the reliability of internal and external financial reporting.

3) Assists compliance with applicable laws and regulations.

4) Helps safeguarding the assets of the entity.

Q.No.14. Discuss the five components of any internal control as they relate to a financial statement audit, as per SA315? (B)

As per SA315, the five components of any internal control as they relate to a financial statement audit are explained below

1) **CONTROL ENVIRONMENT:**

   a) The Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.

   b) The control environment comprises of integrity, ethical values, parameters of governance and rigor around performance measures etc. to drive accountability for performance.

2) **RISK ASSESSMENT:** Risk assessment is the basis for risk management and involves a dynamic and iterative$^{(=\text{repetitive})}$ process for identifying and assessing risks to the achievement of objectives.

3) **CONTROL ACTIVITIES:**

   a) **Control Activities** are the actions to ensure that management's directives to mitigate risks for achievement of objectives are carried out.

   b) Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment.

   c) They may be preventive or detective in nature and may encompass a range of manual and automated activities.

   d) Broadly, the control activities include the elements that operate to ensure transactions are

authorized, duties are segregated, adequate documents and records are maintained etc.

e) Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

4) INFORMATION & COMMUNICATION:

a) Management obtains or generates and uses relevant and **quality information** from both internal and external sources to support the functioning of other components of internal control.

b) **Communication** is the continual, iterative process of providing, sharing, and obtaining necessary information.

5) MONITORING OF CONTROLS:

a) **Monitoring controls** is an ongoing, cyclical process.

b) Ongoing evaluations, separate evaluations, or combination of the two are used to ascertain whether controls are present and functioning.

c) *Deficiencies are communicated to management and the board of directors as appropriate.*

SIMILAR QUESTION:

1. **Efficient and effective internal controls require certain components to be in place otherwise the controls proves to be inefficient. Comment.**

A. **Refer the above answer.**

2. **Elaborate the control activities performed by any business organization to mitigate the risks related to financial statement audit. (MTP – MAY 2020)**

A. **Refer point 3 control activities in the above answer**

3. **SA315 provides the definition of Internal Control that are required to facilitate the effectiveness and efficiency of business operations in an organization. Explain all components of Internal Control as per SA315.**

A. **Refer above answer.**

Q.No.15. Explain the Limitations of Internal Control System? (C)(MTP-M18)

Internal control systems are subject to certain inherent limitations, such as:

a) Management's consideration that the cost of an internal control does not exceed the expected benefits to be derived.

b) Most internal controls cannot manage transactions of unusual nature.Ex: carelessness, distraction, mistakes of judgment and misunderstanding of instructions by the human users.

c) The possibility of avoidance of internal controls through collusion with employees or with parties outside the entity.

d) The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.

e) Manipulations by management with respect to transactions or estimates and judgements required in the preparation of financial statements.

SIMILAR QUESTIONS:

1. **Framing of controls is not panacea for all problems in an organisation unless the control environment is properly understood and many other elements are required. Comment**

A. **Refer the above answer.**

2. **A system of controls does not provide absolute assurance that the control objectives of an organization will be met. Instead, there are several inherent limitations in any system that reduces the level of assurance. Then write some instances that can act as limitation to internal control system.**

A. **Refer above answer**

3. **Internal control, no matter how effective, can provide an entity with only reasonable assurance and not absolute assurance about achieving the entity's operational, financial reporting and compliance objectives. Explain the inherent limitations of internal control systems.**

A. **Refer above answer.**

PART 3: RISKS AND CONTROLS FOR SPECIFIC BUSINESS PROCESSES

Q.No.16. How CONTROLS for specific business processes could be implemented? (B)(M19)

BUSINESS PROCESSES - CONTROLS:

1) Suitable controls should be implemented such as manual, automated or semi-automated provided the risk is mitigated.
2) Based on the scenario, the controls can be **Preventive**, **Detective** or **Corrective**.
3) In computer systems, controls should be checked at three levels, namely Configuration, Master & Transaction level.

1) **CONFIGURATION:** Configuration refers to the way a software system is set up.

   When any software is installed, values for various parameters should be set up (configured) as per policies and business process work flow and rules of the enterprise.

   Configuration will define how software will function and what menu options are displayed.

   Some examples are given below:

   a) Mapping of accounts to front end transactions like purchase and sales
   b) Control on parameters: Creation of Customer Type, Vendor Type and year-end process.
   c) User activation and deactivation, user Access & privileges - Configuration & its management, Password Management.

2) **MASTERS: Masters** refer to the way various parameters are set up for all modules of software, like Purchase, Sales, Inventory and Finance etc.

   The masters are set up first time during installation and are changed whenever the business process rules or parameters are changed.

   Some examples are given here:

   a) **Vendor Master:** Credit period, vendor bank account details, etc.
   b) **Customer Master:** Credit limit, Bill to address, Ship to address, etc.

3) **TRANSACTIONS:** Transactions refer to the actual transactions entered through menus and functions in the application software, through which all transactions for specific modules are initiated, authorized or approved.

   For example:

   a) Sales transactions b) Purchase transactions c) Stock transfer transactions

SIMILAR QUESTION:

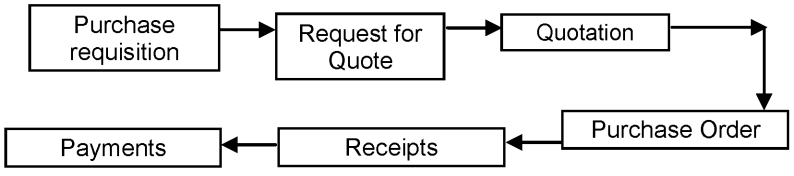
1. **Different controls at different points need to be implemented to have a successful BPA implementation in an enterprise. List out different controls.**

A. **Refer the above answer.**

Q.No.17. Discuss Procure to Pay (P2P) life cycle in detail? How Risks and Controls are implemented for P2P Transactions? (B)(MTP-N18)

1) **PROCURE TO PAY (PURCHASE TO PAY OR P2P)** Is the process of obtaining and managing the raw materials needed for manufacturing a product or providing a service.

   PROCURE TO PAY (P2P) LIFE CYCLE:



PROCURE TO PAY (P2P) - RISKS AND CONTROLS:

MASTERS:

Risks and Control Objectives (Masters - P2P)

RISK	CONTROL OBJECTIVE
Unauthorized changes to supplier master file.	Only valid changes are made to the supplier master file.
All valid changes to the supplier master file are not input and processed.	All valid changes to the supplier master file are input and processed.
Changes to the supplier master file are not correct.	Changes to the supplier master file are accurate.
Changes to the supplier master file are delayed and not processed in a timely manner.	Changes to the supplier master file are processed in a timely manner.

TRANSACTIONS:

Risks and Control Objectives (Transactions - P2P)

RISK	CONTROL OBJECTIVE
Unauthorized purchase requisitions are ordered.	Purchase orders are placed only for approved requisitions.
Purchase orders are not entered correctly in the system.	Purchase orders are accurately entered.
Amounts are posted in accounts payable for goods or services not received.	Amounts posted to accounts payable represent goods or services received.
Amounts posted to accounts payable are not properly calculated and recorded.	Accounts payable amounts are accurately calculated and recorded.
Credit notes and other adjustments are not accurately calculated and recorded.	Credit notes and other adjustments are accurately calculated and recorded.

SIMILAR QUESTION:

1. **The procure-to-pay process is the coordinated and integrated action taken to fulfill a requirement for goods or services in a timely manner at a reasonable price. It involves a number of sequential stages, ranging from need identification to invoice approval and vendor payment. Steps in a procure-to-pay cycle need to be executed in a strict order. Then what may be the risks and control areas that are to be considered in Procure to Pay (P2P) life cycle?**

A. **Refer above answer.**

Q.No.18. Discuss Order to Cash (O2C) life cycle in detail? What are the Risks and how Controls are implemented for O2C Transactions? (B) (RTP-N18)(MTP-M18)

1) **Order to Cash (OTC or O2C) is a set of business processes that involve receiving and** fulfilling customer requests for goods or services.

2) It is a set of business processes that involve receiving and fulfilling customer requests for goods or services.

An order to cash cycle consists of multiple sub-processes including

a) **Customer Order:** Customer order received is documented;

b) **Order fulfillment:** Order is fulfilled or service is scheduled;

c) **Delivery Note:** Order is shipped to customer or service is performed;

d) **Invoicing:** Invoice is created and sent to customer;

e) **Collections:** Customer sends payment /Collection; and

f) **Accounting:** Payment is recorded in general ledger.

Order to Cash (O2C) - Risks and Controls:

Masters:

Risks and Control Objectives (Masters-O2C)

RISK	CONTROL OBJECTIVE
The customer master file is not maintained properly and the information is not accurate.	The customer master file is maintained properly and the information is accurate.
Invalid changes are made to the customer master file.	Only valid changes are made to the customer master file.
All valid changes to the customer master file are not input and processed.	All valid changes to the customer master file are input and processed.
Changes to the customer master file are not accurate.	Changes to the customer master file are accurate.
System access to maintain customer masters has not been restricted to the authorized users.	System access to maintain customer masters has been restricted to the authorized users.

Transactions:

Risks and Control Objectives (Transactions-O2C)

RISK	CONTROL OBJECTIVE
Orders are processed exceeding customer credit limits without approvals.	Orders are processed only within approved customer credit limits.
Orders are not approved by management as to prices and terms of sale.	Orders are approved by management as to prices and terms of sale.
Orders and cancellations of orders are not input accurately.	Orders and cancellations of orders are input accurately.
Order entry data are not transferred completely and accurately to the shipping and invoicing activities.	Order entry data are transferred completely and accurately to the shipping and invoicing activities.
Credit notes issued are not recorded in the System	All credit notes issued are recorded.

SIMILAR QUESTION:

1. **The order-to-cash, also known as the O2C or OTC, process, refers to a company's business process for the entire order processing system. This is a set of business processes to manage from sales order right through to customer payments. It helps define your success as a company and your relationships with customers. Optimizing this process eliminates inefficiencies and can produce benefits seen throughout the entire business. Then what may be the risks and control areas that are to be considered in Order to Cash (O2C) life cycle?**

A. **Refer above answer.**

Q.No.19. Discuss Inventory Cycle in detail? How Risks and Controls are implemented? (C) (For student self-study)(MTP-N18)

The **Inventory Cycle** is a process of accurately tracking the on-hand inventory levels for an enterprise. An inventory system should maintain accurate record of all stock movements to calculate the correct balance of inventory.

PHASES OF THE INVENTORY CYCLE FOR MANUFACTURERS:

1) **Ordering phase:** The amount of time it takes to order and receive raw materials.

2) **Production phase:** The work in progress phase relates to time it takes to convert the raw material to finished goods ready for use by customer.

3) **Finished goods and delivery phase:** The finished goods that remain in stock and the delivery time to the customer. The inventory cycle is measured in number of days.

INVENTORY CYCLE - RISKS AND CONTROLS:

Masters:

Risks and Control Objectives (Masters-Inventory)

RISK	CONTROL OBJECTIVE
Invalid changes are made to the inventory management master file.	Only valid changes are made to the inventory management master file.
Invalid changes to the inventory management master file are input and processed.	All valid changes to the inventory management master file are input and processed.
Changes to the inventory management master file are not accurate.	Changes to the inventory management master file are accurate.
Changes to the inventory management master file are not promptly processed.	Changes to the inventory management master file are promptly processed.
System access to maintain inventory masters has not been restricted to the authorized users.	System access to maintain inventory masters has been restricted to the authorized users.

Transactions:

Risks and Control Objectives (Transactions-Inventory)

RISK	CONTROL OBJECTIVE
Adjustments to inventory prices or quantities are not recorded accurately.	Adjustments to inventory prices or quantities are recorded accurately.
Raw materials are received and accepted without valid purchase orders.	Raw materials are received and accepted only if they have valid purchase orders.
Receipts of raw materials are not recorded promptly and not in the appropriate period.	Receipts of raw materials are recorded promptly and in the appropriate period.
Defective raw materials are not returned promptly to suppliers.	Defective raw materials are returned promptly to suppliers.
Inventory is reduced when goods are not shipped and made based on unapproved customer orders.	Inventory is reduced only when goods are shipped with approved customer orders.

SIMILAR QUESTION:

1. **What are the three phases involved in Inventory cycle for manufacturers**

A. Refer "PHASES OF THE INVENTORY CYCLE FOR MANUFACTURERS" side heading above.

Q.No.20. Discuss Human Resources cycle in detail? How Risks and Controls are implemented? (B)(RTP-N19,M20)(M18)(MTP-N18)

The **Human Resources** life cycle refers to human resources management and covers all the stages of an employee's tenure within a specific enterprise.

TYPICAL STAGE OF HR CYCLE INCLUDES:

1) **Recruiting and on-boarding:** Recruiting is the process of hiring a new employee. This might include placing the job ads, selecting candidates, conducting employment interviews and administering assessments such as personality profiles to choose the best applicant for the position.

   On boarding is the process of getting the successful applicant set up in the system as a new employee.

2) **Orientation and Career Planning:** Orientation is the process by which the employee becomes a member of the company's work force through learning her new job duties, establishing relationships with co-workers and supervisors and developing a niche. Career planning is the stage at which the employee and her supervisors work out her long-term career goals with the company.

3) **Career Development:** After an employee, has established himself at the company and determined his long-term career objectives, the human resources department should try to help him meet his goals, if they're realistic.

4) **Termination or Transition:** Some employees will leave a company through retirement after a long and successful career. Others will choose to move on to other opportunities or be laid off. The role of HR in this process is to manage the transition by ensuring that all policies and procedures are followed.

HUMAN RESOURCES - RISKS AND CONTROLS:

Configuration:

Risks and Control Objectives (Configuration-Human Resources)

RISK	CONTROL OBJECTIVE
Employees who have left the company continue to have system access.	System access to be immediately removed when employees leave the company.
Employees have system access in excess of their job requirements.	Employees should be given system access based on a "need to know" basis and to perform their job function.

Masters:

Risks and Control Objectives (Masters-Human Resources)

RISK	CONTROL OBJECTIVE
Additions to the payroll master files do not represent valid employees.	Additions to the payroll master files represent valid employees.
New employees are not added to the payroll master files.	All new employees are added to the payroll master files.
Terminated employees are not removed from the payroll master files.	Terminated employees are removed from the payroll master files.
Employees are terminated without following statutory requirements.	Employees are terminated only within statutory requirements.
Deletions from the payroll master files do not represent valid terminations.	Deletions from the payroll master files represent valid terminations.

SIMILAR QUESTION:

1. **Give some examples of the Risks and Control Objectives for Human Resource Process at configuration level.**

A. **Refer Configuration Risks and Control Objectives table in the above question.**

PART 4- REGULATORY AND COMPLIANCE REQUIREMENTS

Q.No.21. What is the Auditors responsibility as per ICAI's "Guidance Note on Audit of Internal Financial Controls over Financial Reporting"? (B)

AUDITORS' RESPONSIBILITY:

1) The auditor's objective in an audit of internal financial controls over financial reporting is to express an opinion on the effectiveness of the company's internal financial controls over financial reporting and the procedures in respect thereof are carried out along with an audit of the financial statements.

2) Because a company's internal controls cannot be considered effective if one or more material weakness exists, to form a basis for expressing an opinion, the auditor should plan and perform the audit to obtain sufficient appropriate evidence to obtain reasonable assurance about whether material weakness exists as of the date specified in management's assessment.

3) A material weakness in internal financial controls may exist even when the financial statements are not materially misstated.

Q.No.22. What is Corporate Governance? Explain? (B) (M19 - 5M)

1) Corporate Governance is the framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in a company's relationship with its all stakeholders (financiers, customers, management, employees, government, and the community).

2) Good corporate governance requires establishment of sound internal control practices, risk management, and compliance with relevant laws and standards such as corporate disclosure requirements.

3) Good management practices are one of the important elements of corporate governance.

THE CORPORATE GOVERNANCE FRAMEWORK CONSISTS OF:

1) Explicit and implicit contracts between the company and the stakeholders for distribution of responsibilities, rights, and rewards

2) Procedures for reconciling the sometimes-conflicting interests of stakeholders in accordance with their duties, privileges, and roles, and

3) Procedures for proper supervision, control, and information-flows to serve as a system of checks-and-balances.

SIMILAR QUESTIONS:

1. **Corporate Governance is defined as the framework of rules and practices by which Board of Directors ensures accountability, fairness and transparency in a company's relationship with all its stakeholders. List the rules and procedures that constitute corporate governance framework.**

A. **Refer above answer.**

PART 5: IT ACT 2000

Q.No.23. Discuss the Advantages of Cyber Laws? (B)

ADVANTAGES OF CYBER LAWS: The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber-crimes. We need such laws so that people can perform purchase transactions over the internet without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects which are as follows:

1) The suggestion that email would now be a valid and legal form of communication in India that can be duly produced and approved in a court of law.

2) Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

3) Digital signatures have been given legal validity and sanction in the Act.

4) The Act open the doors for the corporate companies in the business of issuing Digital Signatures Certificates.

5) The Act now allows Government to issue notification on the web indicating e-governance.

6) The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form.

7) The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.

8) The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

SIMILAR QUESTION:

1. **Explain the positive aspects contained in the IT Act, 2000 and its provisions from the perspective of E-commerce in India. (M18 - 4M)**

A. **Same as above**

2. **In view of the growth in transactions and communications carried out through electronic records, the IT Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature. In this context write some positive aspects of IT act 2000 with respect to ecommerce transactions in India.**

A. **Refer above answer.**

Q.No.24. Discuss the key terms regarding IT Act, 2000 (as amended in 2008)? (B)

The IT Act, 2000 defines the terms access in section 2(a), computer in section 2(i), computer network in section 2 (j), data in section 2(o) and information in section 2(v). These are all the necessary ingredients that are useful to technically understand the concept of Cyber Crime.

DEFINITIONS:

1) 2(a)"**Access**" with its grammatical variations and cognate(=Similar) expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

2) 2(i)"**Computer**" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

3) **2(j)"Computer Network**" means the interconnection of one or more Computers or Computer **systems** or Communication device through-

   a) The use of satellite, microwave, terrestrial line, wire, wireless or other communication media;

   b) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

4) 2(o)"**Data**" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network.

   It may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

5) 2(v)"**Information**" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

Q.No.25. Write some of the key provisions of IT act? (B)

The IT Act recognizes risks of information technology deployment in India, various types of computer-related offences and provides a legal framework for prosecution for these offences.

Some of key provisions of IT related offences as impacting the banks are given here:

1) Section 43 provides for Penalty and compensation for damage to computer, Computer System, etc.
2) Section 43-A Compensation for failure to protect data
3) Section 65: Tampering with Computer Source Documents
4) Section 66: Computer Related Offences
5) Section 66-B:Punishment for dishonestly receiving stolen computer resource or communication device
6) Section 66-C: Punishment for identity theft
7) Section 66-D: Punishment for cheating by personation by using computer Resource
8) Section 66-E: Punishment for violation of privacy
9) Section 66-F Punishment for cyber terrorism
10) Section 67 Punishment for publishing or transmitting obscene material in electronic form
11) Section 67-A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
12) Section 67-B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Q.No.26. Give some examples of Common Cyber-crime scenarios that can be prosecuted under the IT Act 2000 (amended via 2008)?Or Computer Related Offences (A)

EXAMPLES OF COMMON CYBER-CRIME SCENARIOS:

1) **Harassment via fake public profile on social networking site:** A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labeled as person of 'loose character'. This leads to harassment of the victim.

   Section 67 of the IT Act, 2000 is applicable here.

2) **Email Account Hacking:** If victim's email account is hacked and obscene emails are sent to people in victim's address book. Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act, 2000 are applicable in this case.

3) **Credit Card Fraud:** Unsuspecting victims would use infected computers to make online transactions. Sections 43, 66, 66C, 66D of IT Act, 2000 are applicable in this case.

4) **Web Defacement:** The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days. Sections 43 and 66 of IT Act and Sections 66F and 67 of IT Act, 2000 also apply in some cases.

5) **Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs:** All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information. Sections 43 and 66 of IT Act, 2000 are applicable in this case.

6) **Cyber Terrorism:** Many terrorists use virtual (Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business. Sections 43, 66, 66A of IT Act, 2000 are applicable in this case.

7) **Online sale of illegal Articles:** Where sale of narcotics, drugs weapons and wildlife is facilitated by the Internet.

8) **Phishing and Email Scams:** Phishing involves fraudulently acquiring sensitive information through masquerading oneself as a trusted entity (e.g. Passwords, credit card information). Sections 66, 66C and 66D of IT Act, 2000 are applicable in this case.

9) **Theft of Confidential Information:** Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.Sections 43, 66 and 66B of IT Act, 2000 are applicable in this case.

10) **Source Code Theft:** A Source code generally is the most coveted and important "crown jewel" asset of a company. Sections 43, 65, 66 and 66B of IT Act, 2000 are applicable in this case.

11) **Cyber Pornography:** Among the largest businesses on Internet, pornography may not be illegal in many countries, but child pornography is. Sections 67, 67A and 67B of the IT Act, 2000 are applicable in this case.

Q.No.27. What are the main principles on data protection and privacy enumerated under the IT Act, 2000 ? (A)(M18)

THE MAIN PRINCIPLES ON DATA PROTECTION AND PRIVACY ENUMERATED UNDER THE IT ACT, 2000 ARE:

1) Defining 'data', 'computer database', 'information', 'electronic form', 'originator', 'addressee' etc.
2) Creating civil liability if any person accesses or secures access to computer, computer system or computer network
3) Creating criminal liability if any person accesses or secures access to computer, computer system or computer network
4) Declaring any computer, computer system or computer network as a protected system
5) Imposing penalty for breach of confidentiality and privacy
6) Setting up of hierarchy of regulatory authorities, namely adjudicating officers, the Cyber Regulations Appellate Tribunal etc.

SIMILAR QUESTION:

1. **As a cyber-expert, you have been invited in a seminar to share your thoughts on data protection and privacy in today's electronic era. In your PowerPoint presentation on the same, you wish to incorporate the main principles on data protection and privacy enumerated under the IT Act, 2000. Identify them.**

A **Refer above answer.**

Q.No.28. Discuss the term Sensitive Personal Data Information regarding IT Act, 2000? (B)

1) **SENSITIVE PERSONAL DATA INFORMATION (SPDI):** Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 formed under section 43A of the Information Technology Act 2000 define a data protection framework for the processing of digital data by Body Corporate.

2) **SCOPE OF RULES:** Currently the Rules apply to Body Corporate and digital data. As per the IT Act, Body Corporate is defined as "Any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities."

3) **DEFINITION OF PERSONAL AND SENSITIVE PERSONAL DATA:** Rule 2(i) defines personal information as "information that relates to a natural person which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person."

   Rule 3 defines sensitive personal information as:

   a) *Passwords*

   b) *Financial information*

   c) *Physical/physiological/mental health condition*

   d) *Sexual orientation*

   e) *Medical records and history; and*

   f) *Biometric information*

4) **CONSENT TO COLLECT:** Rule 5(1) requires that Body Corporate should, prior to collection, obtain consent in writing through letter or fax or email from the provider of sensitive personal data regarding the use of that data.

5) **CONSENT TO DISCLOSURE:** Rule 6 provides that Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information.

SECTION 2: QUESTIONS FOR ACADEMIC INTEREST FOR STUDENT SELF STUDY

Q.No.1.Write about the fixed asset process its steps, risk and control objectives. (C)

Fixed Assets process ensures that all the fixed assets of the enterprise are tracked for the purposes of financial accounting, preventive maintenance.

Fixed assets process ensures that all fixed assets are tracked and fixed asset records are maintained properly.

Typical steps of fixed assets process are as follows:

1) **PROCURING AN ASSET:** An asset is most often entered into the accounting system; when the invoice for the asset is entered; into the accounts payable; or purchasing module of the system.

2) **REGISTERING OR ADDING AN ASSET:** Information entered at this stage could include; acquisition date, placed-in-service date, description, asset type, cost basis, depreciable basis etc.

3) **ADJUSTING THE ASSETS:** Adjustments to existing asset information is often needed to be made. **Events** may occur that can change the depreciable basis of an asset.

4) **TRANSFERRING THE ASSETS:** A fixed asset maybe sold or transferred to another subsidiary, reporting **entity**, or department within the company. These intercompany and intra-company transfers may result in changes that impact the asset's depreciable basis, depreciation, or other asset data.

5) **DEPRECIATING THE ASSETS**

6) **DISPOSING THE ASSETS**

Risks and Control Objectives (Masters-Fixed Assets)

RISK	CONTROL OBJECTIVE
Invalid changes are made to the fixed asset register and/or master file.	Only valid changes are made to the fixed asset register and/or master file.
Valid changes to the fixed asset register and/ or master file are not input and processed.	All valid changes to the fixed asset register and/or master file are input and processed.
Changes to the fixed asset register and/or master file are not accurate.	Changes to the fixed asset register and/or master file are accurate.
Changes to the fixed asset register and/or master file are not promptly processed.	Changes to the fixed asset register and/or master file are promptly processed.

Risks and Control Objectives (Transactions-Fixed Assets)

RISK	CONTROL OBJECTIVE
Fixed asset acquisitions are not accurately recorded.	Fixed asset acquisitions are accurately recorded.
Fixed asset acquisitions are not recorded in the appropriate period.	Fixed asset acquisitions are recorded in the appropriate period.
Depreciation charges are not recorded in the appropriate period.	All depreciation charges are recorded in the appropriate period.
Fixed asset maintenance activity records are not updated in a timely manner.	Fixed asset maintenance activity records are updated in a timely manner.
Accounting entries pertaining to acquisition, disposals, transfers, retirement are not recorded in the correct GL account.	Accounting entries pertaining to acquisition, disposals, transfers, retirement are recorded in the correct GL account.

Q.No.2. write about General Ledger steps, Risks, Control objectives. (B)

GENERAL LEDGER (GL): Process refers to the process of recording the transactions in the system to finally generating the reports from financial transactions entered in the system.

The typical steps in general ledger porcess flow are as follows:

1) Entering financial transactions into the system

2) Reviewing Transactions

3) Approving Transactions

4) Posting of Transactions

5) Generating Financial Reports

CONFIGURATION

Risks and Control Objectives (Configuration-General Ledger)

RISKS	CONTROL OBJECTIVE
Unauthorized general ledger entries could be passed.	Access to general ledger entries is appropriate and authorized.
System functionality does not exist to segregate the posting and approval functions.	System functionality exists to segregate the posting and approval functions.
Out-of-balance entries are not prohibited.	Out-of-balance entries are prohibited.

System controls are not in place for appropriate approval of write-offs.	System controls are in place for appropriate approval of write-offs.
Journal entries of exceptional amount that were posted to the general ledger during the month are not flagged by the system and not subsequently reviewed for accuracy and approved by the controller or CFO after month-end.	Journal entries of exceptional amount that were posted to the general ledger during the month are flagged by the system and subsequently reviewed for accuracy and approved by the controller or CFO after month-end.
Transactions can be recorded outside of financial close cut off requirements.	Transactions cannot be recorded outside of financial close cut off requirements.
Adding to or deleting general ledger accounts are not limited to authorized accounting department personnel.	Adding to or deleting general ledger accounts are limited to authorized accounting department personnel.

Risks and Control Objectives (Masters-General Ledger)

RISKS	CONTROL OBJECTIVE
General ledger master file change reports are not generated by the system and are not reviewed as necessary by an individual who does not input the changes.	General ledger master file change reports are generated by the system and reviewed as necessary by an individual who does not input the changes.
A standard chart of accounts has not been approved by management and is not utilized within all entities of the corporation.	A standard chart of accounts has been approved by management and is not utilized within all entities of the corporation.

Risks and Control Objectives (Transactions-General Ledger)

RISKS	CONTROL OBJECTIVE
General ledger balances are not reconciled to sub ledger balances and such reconciliation are not reviewed for accuracy and not approved by supervisory personnel.	General ledger balances reconcile to sub ledger balances and such reconciliation are reviewed for accuracy and approved by supervisory personnel.
Account codes and transaction amounts are not accurate and not complete, and exceptions are not reported.	Account codes and transaction amounts are accurate and complete, with exceptions reported.
A report of all journal entries completed as part of the closing process is not reviewed by management to confirm the completeness and appropriateness of all recorded entries.	A report of all journal entries completed as part of the closing process is reviewed by management to confirm the completeness and appropriateness of all recorded entries.
Entries booked in the close process are not complete and accurate.	Entries booked in the close process are complete and accurate.

Q.No.3. what is Management's Responsibility As per ICAI's "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting"? (C)

MANAGEMENT'S RESPONSIBILITY

1) The 2013 Act has significantly expanded the scope of internal controls to be considered by the management of companies to cover all aspects of the operations of the company.

2) Clause (e) of Sub-section 5 of Section 134 to the Act requires the directors' responsibility statement to state that the directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

3) Clause (e) of Sub-section 5 of Section 134 explains the meaning of the term, "internal financial controls" as "the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information."

4) Rule 8(5)(viii) of the Companies (Accounts) Rules, 2014 requires the Board of Directors' report of all companies to state the details in respect of adequacy of internal financial controls with reference to the financial statements.

5) The inclusion of the matters relating to internal financial controls in the directors' responsibility statement is in addition to the requirement for the directors to state that they have taken proper and sufficient care for the maintenance of adequate accounting records in accordance with the provisions of the 2013 Act, for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities.

Q.NO. 4. Write about section 43 of IT Act. (C) (RTP-N20)

SECTION 43: Penalty and compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -

1) Accesses or secures access to such computer, computer system or computer network 1[or computer resource];

2) Downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

3) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

4) Damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

5) Disrupts or causes disruption of any computer, computer system or computer network;

6) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

7) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

8) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

9) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

10) Steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

He shall be liable to pay damages by way of compensation to the person so affected.

SECTION 43A: Compensation for failure to protect data.

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Q.NO. 5. Write about section 65 of IT Act. (C)

SECTION 65: Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both.

The explanation clarifies 'Computer Source Code" means the listing of programme, Computer Commands, Design and layout and program analysis of computer resource in any form.

Q.NO. 6. Write about section 66 of IT Act. (C)

SECTION 66: Computer Related Offences

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to 5 lakh rupees or with both.

SECTION 66-B: Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

SECTION 66-C: Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

SECTION 66-D: Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

SECTION 66-E: Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

SECTION 66-F: Punishment for cyber terrorism

Whoever -

1) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

- **a)** Denying or cause the denial of access to any person authorized to access computer resource; or
- **b)** Attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
- **c)** Introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

2) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

3) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Q.NO. 7. Write about section 67 of IT Act 2000. (C)

[Section 67] Punishment for publishing or transmitting obscene material in electronic form:

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

[Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form:

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

[Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form:

Whoever, -

1) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
2) Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
3) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
4) Facilitates abusing children online or
5) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

PROVIDED that provisions of Section 67, Section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form -

1) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
2) Which is kept or used for bona fide heritage or religious purposes.

Q.NO. 36. Explain the salient features of Section 134 & Section 143 of the Companies Act 2013.(C)

The Companies Act, 2013 has two very important Sections - **Section 134** and **Section 143**, which have a direct impact on the audit and accounting profession.

1) **SECTION 134: Section 134 of the Companies Act, 2013 on "Financial statement, Board's report, etc." states inter alia:**

   The **Directors' Responsibility Statement** referred to in clauses (c e) of sub-section (3) shall state that:

the Directors had taken proper and sufficient care for the maintenance of adequate accounting records in accordance with the provisions of this Act for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities;

♦ the Directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

2) **SECTION 143: Section 143, of the Companies Act 2013, on "Powers and duties of auditors and auditing standards" states inter alia:**

Section 143(3)(i) contains the **Auditor's Report** which shall state that:

"Whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls";

When we talk in terms of "adequacy and effectiveness of controls"; it refers to the adequacy of the control design and whether the control has been working effectively during the relevant financial year.

THE END