

MOCK TEST PAPER
FINAL COURSE GROUP - II
PAPER - 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Answer Keys

Part I: MULTIPLE CHOICE QUESTIONS

1. (b) Vulnerability
2. (d) Automated, Deterministic, Open, Physical
3. (c) Controlled visitors' access to the library
4. (b) Differential Backup
5. (c) The programming languages used in the development of source code.
6. (a) Environmental
7. (b) Section 43
8. (b) Data as a Service
9. (d) A statement that the registered private accounting firm that audited the financial statements included in the monthly report has issued an attestation report on management's assessment of the company's internal control over financial reporting.
10. (c) Explicit knowledge is personal, experimental and context - specific.
11. (a) Identification, Authentication, Authorization
12. (a) With Incremental backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup only.
13. (a) Presentation by the selected vendor
14. (d) Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place or not.
15. (a) Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.
16. (a) Network
17. (c) To evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.
18. (b) A system has number of non-related and independent subsystems or components. The subsystems can function in isolation and do not depend on other subsystems.
19. (d) Adaptive maintenance in which the program is tuned to decrease the resource consumption
20. (c) Hot site
21. (b) Business Analyst
22. (b) System Control Audit Review File (SCARF)

Part-II: Descriptive Questions

1. (a) The key practices that may be adopted by an Auditor to determine the status of IT Governance in an enterprise are as follows:

- Who makes directing, controlling and executing decisions?
- How the decisions are made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How exceptions are handled?
- How the governance results are monitored and improved?

The benefits which are achieved by implementing IT governance of an enterprise, IT would depend on the specific and unique environment of every enterprise and include the following:

- Increased value delivered through enterprise IT;
- Increased user satisfaction with IT services;
- Improved agility in supporting business needs;
- Better cost performance of IT;
- Improved management and mitigation of IT-related business risk;
- IT becoming an enabler for change rather than an inhibitor;
- Improved transparency and understanding of IT's contribution to the business;
- Improved compliance with relevant laws, regulations and policies; and
- More optimal utilization of IT resources.

- (b) From the perspective of environmental exposures and controls, Information Systems resources with the primarily focus on facilities may be categorized as follows:

- **Hardware and Media:** This includes Computing Equipment, Communication equipment, and Storage Media.
- **Information Systems Supporting Infrastructure or Facilities:** This typically includes Physical Premises like Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities; Staging Room, and Storage Areas; Communication Closets; Cabling ducts; Power Source, and Heating, Ventilation and Air Conditioning (HVAC).
- **Documentation:** Physical and geographical documentation of computing facilities with **emergency** excavation plans and incident planning procedures.
- **Supplies:** The third-party maintenance procedures viz. air-conditioning, fire safety, and civil contractors whose entry and access with respect to their scope of work assigned are to be monitored and logged.
- **People:** The employees, contract employees, visitors, supervisors and third-party maintenance personnel are to be made responsible and accountable for environmental controls in their respective Information Processing Facility (IPF). Training of employees and other stake holders on control procedures is a critical component.

- (c) The Information Systems (IS) Audit is defined as a process to evaluate the adequacy of internal controls with regard to both specific computer program and the data processing environment as a whole. The IS Audit of an Information System environment may include one or both of the following:

- Assessment of internal controls within the IS environment to assure validity, reliability, and security of information and information systems.

- Assessment of the efficiency and effectiveness of the IS environment.
2. (a) Existence of an audit trail is a key financial audit requirement; since without an audit trail, the auditor may have extreme difficulty in gathering sufficient, appropriate audit evidence to validate the figures in the client's accounts. The performance of evidence collection and understanding the reliability of controls involves issues as mentioned below:
- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transaction on the computer system. For example, the client's computer system may save data on detachable storage device by summarising transactions into monthly, weekly or period end balances.
 - **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of Electronic Data Interchange (EDI) will result in less paperwork being available for audit examination.
 - **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
 - **Lack of availability of printed output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
 - **Audit evidence:** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
 - **Legal issues:** The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and which are the parties to the contract.
- (b) While developing the Business Continuity Management, the competencies necessary for personnel assigned specific management responsibilities within the system are as follows:
- Actively listens to others, their ideas, views and opinions;
 - Provides support in difficult or challenging circumstances;
 - Responds constructively to difficult circumstances;
 - Adapts leadership style appropriately to match the circumstances;
 - Promotes a positive culture of health, safety and the environment;
 - Recognizes and acknowledges the contribution of colleagues;
 - Encourages the taking of calculated risks;
 - Encourages and actively responds to new ideas;

- Consults and involves team members to resolve problems;
 - Demonstrates personal integrity; and
 - Challenges established ways of doing things to identify improvement opportunities.
- (c) The impact of cyber frauds on enterprises can be viewed under the following dimensions:
- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.
 - **Legal Repercussions:** The entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
 - **Loss of credibility or Competitive Edge:** News that an organization's database has been hit by fraudsters, leads to loss of competitive advantage and credibility. There have been instances where share prices of such companies went down, as the news of such attack percolated to the market.
 - **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.
 - **Sabotage:** The above situation may lead to misuse of such information by enemy country.
3. (a) System can be classified based on various parameters like elements, interactive behavior, degree of human intervention and working output
- (i) **On the basis of Elements:** System may be categorized as Abstract or Physical System based on the elements used in the system.
- Abstract System also known as Conceptual System or Model can be defined as an orderly arrangement of interdependent ideas or constructs. For example, a system of theology is an orderly arrangement of ideas about God and the relationship of humans to God.
 - Physical System, on the other hand, is a set of tangible elements, which operated together to accomplish an objective e.g. Computer system, University system etc.
- (ii) **On the basis of Interactive behavior:** Systems may be classified as Open Systems or Closed System based on 'how the system interacts with environment'.
- An Open System interacts with other systems in its environment. For example, Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment.
 - Closed System does not interact with the environment and does not change with the changes in environment. Consider a 'throw-away' type sealed digital watch, which is a closed system as it is completely isolated from its environment for its operation.
- (iii) **On the basis of Degree of Human intervention:** According to the degree of human intervention, the system may be classified as Manual or Automated System.
- In a Manual System, the activities like data collection, maintenance and final reporting are done by human.
 - In an Automated System, the activities like data collection, maintenance and final reporting are carried out by computer system or say machine itself.

- (iv) **On the basis of Working/Output:** Based on working style and the output, the systems can be classified as Deterministic and Probabilistic System.
- A Deterministic System operates in a predictable manner. For example - software that performs on a set of instructions is a deterministic system.
 - A Probabilistic System can be defined in terms of probable behavior. For example - inventory system is a probabilistic system where the average demand, average time for replenishment, etc. may be defined, but the exact value at any given time is not known.
- (b) The major activities that senior management must perform are Planning, Organizing, Controlling and Leading. The role of auditor at each activity is discussed below:
- **Planning:** Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not. A poor-quality information system is ineffective and inefficient leading to losing of its competitive position within the marketplace.
 - **Organizing:** Auditors should be concerned about how well top management acquires and manages staff resources for three reasons:
 - The effectiveness of the IS function depends primarily on the quality of its staff. The IS staff need to remain up to date and motivated in their jobs.
 - Intense competition and high turnover have made acquiring and retaining good information system staff a complex activity.
 - Empirical research indicates that the employees of an organization are the most likely persons to perpetrate irregularities.
 - **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function. Auditors may use both formal and informal sources of evidence to evaluate how well top managers communicate with their staff. The formal sources include IS plans, documents standards and policies whereas the informal sources of evidence include interviews with IS staff about their level of satisfaction with the top management. Auditors must try to assess both the short-run and long-run consequences of poor communications within the information systems function and to assess the implications for asset safeguarding, data integrity, system effectiveness, and system efficiency.
 - **Controlling:** Auditors should focus on subset of the control activities that should be performed by top management – namely, those aimed at ensuring that the information systems function accomplishes its objectives at a global level. Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.
- (c) Enterprises need to take steps to ensure compliance with cyber laws. Some key steps for ensuring compliance are given below:
- Designate a Cyber Law Compliance Officer as required.
 - Conduct regular training of relevant employees on Cyber Law Compliance.
 - Implement strict procedures in HR policy for non-compliance.
 - Implement authentication procedures as suggested in law.
 - Implement policy and procedures for data retention as suggested.
 - Identify and initiate safeguard requirements as applicable under various provisions of the Act such as: Sections 43A, 69, 69A, 69B, etc.

- Implement applicable standards of data privacy on collection, retention, access, deletion etc.
 - Implement reporting mechanism for compliance with cyber laws.
4. (a) The major issues related to the implementation of Cloud computing are as follows:
- **Threshold Policy:** To test if the program works, develops, or improves and implements; a threshold policy is of immense importance in a pilot study before moving the program to the production environment. This involves the checking how the policy enables to detect sudden increases in the demand and results in the creation of additional instances to fill in the demand. Moreover, to determine how unused resources are to be de-allocated and turned over to other work, needs to be worked out in the context. That is working out thresholds is really a matter of concern and would go a long way to assure the effectiveness.
 - **Interoperability:** If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary Application Programming Interfaces (APIs) and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. We may need to reformat/reorganize data or change the logic in applications.
 - **Hidden Costs:** Like any such services in prevailing business systems, cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges from their service providers for storage and database applications containing terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. In another instance of incurring network costs; companies who are far from the location of cloud providers, could experience latency, particularly when there is heavy traffic.
 - **Unexpected Behavior:** It is important to test the application in the cloud with a pilot study to check for unexpected behavior. Let's suppose that credit card validation application works well at our company's internal data centre. Examples of tests include how the application validates credit cards, and how, in the scenario of the buying crunch, it allocates resources and releases unused resources, turning them over to other work. If the tests show unexpected results of credit card validation or releasing unused resources, we will need to fix the problem before executing or obtaining cloud services from the cloud.
 - **Software Development in Cloud:** To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate centre and extend resources temporarily for testing purposes. This allows project managers to control costs, manage security and allocate resources to clouds for a project. The project managers can also assign individual hardware resources to different cloud types: Web development cloud, testing cloud, and production cloud. The cost associated with each cloud type may differ from one another. The cost per hour or usage with the development cloud is most likely lower than the production cloud, as additional features, such as SLA and security, are allocated to the production cloud. The managers can limit projects to certain clouds.
 - **Environment Friendly Cloud Computing:** One incentive for cloud computing is that it may be more environment friendly. First, reducing the number of hardware components needed to run applications on the company's internal data centre and replacing them with cloud computing systems reduces energy for running and cooling hardware. By consolidating these systems in remote centers, they can be handled more efficiently as a group.
- (b) Input controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important since substantial time is spent on input of data, involve human intervention and are, therefore error and fraud prone.

Input controls are divided into the following broad classes:

- (i) **Source Document Controls:** In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from the organization. For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier. To control against this type of exposure, the organization must implement control procedures over source documents to account for each document. Some control procedures include usage of pre-numbered source documents, usage of source documents in sequence, and periodic audit of source documents.
- (ii) **Data Coding Controls:** Two types of errors can corrupt a data code and cause processing errors. These are transcription and transposition errors, which are as discussed below:
 - **Transcription Errors:** These fall into three classes:
 - Addition errors occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
 - Truncation errors occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
 - Substitution errors are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.
 - **Transposition Errors:** There are two types of transposition errors.
 - Single transposition errors occur when two adjacent digits are reversed. For instance, 12345 are recorded as 21345.
 - Multiple transposition errors occur when nonadjacent digits are transposed. For example, 12345 are recorded as 32154.

Any of these errors can cause serious problems in data processing if they go undetected.
- (iii) **Batch Controls:** Batching is the process of grouping together transactions that bear some type of relationship to each other. Various controls can be exercised over the batch to prevent or detect errors or irregularities. Two types of batches occur are discussed below:
 - **Physical Controls:** These controls are groups of transactions that constitute a physical unit. For example – source documents might be obtained via the email, assembled into batches, spiked and tied together, and then given to a data-entry clerk to be entered into an application system at a terminal.
 - **Logical Controls:** These are group of transactions bound together on some logical basis, rather than being physically contiguous. For example - different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions into an application system.
- (iv) **Validation Controls:** Input validation controls are intended to detect errors in the transaction data before the data are processed. There are three levels of input validation controls:
 - **Field Interrogation:** It involves programmed procedures that examine the characters of the data in the field. The following are some common types of field interrogation. Various field checks used to ensure data integrity are Limit Check, Picture Checks, Valid Code Checks, Check Digit, Arithmetic Checks and Cross Checks.
 - **Record Interrogation:** These are discussed as follows:
 - **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?

- **Valid Sign:** The contents of one field may determine which sign is valid for a numeric field.
 - **Sequence Check:** If physical records follow a required order matching with logical records.
 - **File Interrogation:** These are discussed as follows:
 - **Version Usage:** Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.
 - **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading files, external labeling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labeling is more important.
 - **Data File Security:** Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.
 - **Before and after Image and Logging:** The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.
 - **File Updating and Maintenance Authorization:** Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.
 - **Parity Check:** When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.
 - (c) The advantages of Business Continuity are that the enterprise:
 - is able to proactively assess the threat scenario and potential risks;
 - can plan response to disruptions which can contain the damage and thus minimize the impact of it on the enterprise; and
 - is able to demonstrate a response through a process of regular testing and trainings.
5. (a) Mr. Mohan is punishable under Section 73 of Information Technology Act, 2000.
- [Section 73] Penalty for publishing Electronic Signature Certificate false in certain particulars.
- (1) No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that -
- (a) the Certifying Authority listed in the certificate has not issued it; or
 - (b) the subscriber listed in the certificate has not accepted it; or
 - (c) the certificate has been revoked or suspended,
- unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

- (b) Planning is one of the primary and important phases in an Information System Audit which ensures that the audit is performed in an effective manner. Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, those potential problems are identified and that the work is completed expeditiously.

Important points to be considered during Planning are as follows:

- The extent of planning will vary according to the size of the entity, the complexity of the audit and the auditor's experience with the entity and knowledge of the business.
- Obtaining knowledge of the business is an important part of planning the work. The auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.
- The auditor may wish to discuss elements of the overall audit plan and certain audit procedures with the entity's audit committee, the management and staff to improve the effectiveness and efficiency of the audit and to coordinate audit procedures with work of the entity's personnel. The overall audit plan and the audit program; however, remains the auditor's responsibility.
- The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit. While the record of the overall audit plan will need to be sufficiently detailed to guide the development of the audit program, its precise form and content will vary depending on the size of the entity, the complexity of the audit and the specific methodology and technology used by the auditor.
- The audit should be guided by an overall audit plan and underlying audit program and methodology. Audit planning is often mistaken as a one-time activity to be taken and completed in the beginning of the audit. While for all practical purposes, planning is a continuous activity which goes on throughout the entire audit cycle. Many times, changes in conditions or circumstances or unexpected findings during audit require changes in the audit procedures and methodology initially planned. Hence, an auditor is expected to modify the audit plan as warranted by the circumstances.

- (c) **Black Box Testing:** Black Box Testing takes an external perspective of the test object, to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects typical inputs including simple, extreme, valid and invalid input-cases and executes to uncover errors. There is no knowledge of the test object's internal structure.

This method of test design is applicable to all levels of software testing i.e. unit integration, functional testing, system and acceptance. The higher the level, hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested. If a module performs a function, which is not supposed to, the black box test does not identify it.

White Box Testing: It uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. Since the tests are based on the actual implementation, if the implementation changes, the tests probably will need to change, too. It is applicable at the unit, integration and system levels of the testing process; it is typically applied to the unit. While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be

conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.

6. (a) In order to finally deploy or implement the new system in the real operating environment, several activities are undertaken. Some of the generic key activities involved in System Implementation include the following:

- **Equipment Installation:** The hardware required to support the new system is selected prior to the implementation phase. The necessary hardware should be ordered in time to allow for installation and testing of equipment during the implementation phase. An installation checklist should be developed at this time with operating advice from the vendor and system development team. In those installations, where people are experienced in the installation of the same or similar equipment, adequate time should be scheduled to allow completion of the several activities that include site preparation, installation of new hardware/software, and equipment checkout.
- **Training Personnel:** A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps or hinders the successful implementation of information system. Thus, training is a major component of systems implementation. When a new system is acquired, which often involves new hardware and software, both users and computer professionals generally need some type of training. Often, this is imparted through classes, which are organized by vendor, and through hands-on learning techniques. Such training structure should be highly formalized and be based business process executions with actual data.
- **System Change-Over Strategies:** Conversion or changeover is the process of changing over or shifting over from the old system (may be the manual system) to the new system. It requires careful planning to establish the basic approach to be used in the actual changeover, as it may put many resources/assets/operations at risk. Different types of popular implementation strategies are Direct Implementation / Abrupt Change-Over, Phased Changeover, Pilot Changeover and Parallel Changeover.

- (b) **Corporate Governance:** Corporate Governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The corporate governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance. The corporate governance is monitored by the audit committee.

Business Governance: The Business Governance is business-oriented with pro-active and forward-looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required. The business governance in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee.

- (c) Section 66F of Information Technology Act, 2000 defines the Punishment for cyber terrorism.

[Section 66F] Punishment for cyber terrorism

- (1) Whoever -

- (A) 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 –
- (i) denying or cause the denial of access to any person authorized to access computer resource; or
 - (ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
 - (iii) 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
- (B) 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.

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