PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

Candidates are also required to answer any five questions

from the remaining six questions.

Question 1

ABC Limited, a large enterprise with more than 12000 employees, plans to implement an MIS to support middle and senior level management in administration and decision making. As an expert, what would be your response to the following:

(a) Major limitations of a Management Information System (5 Marks)

(b) Important implications of an MIS in business (5 Marks)

(c) What are the categories of system maintenance? (5 Marks)

(d) What are the major aspects to be looked into by an IS Auditor? (5 Marks)

Answer

(a) Major Limitations of Management Information Systems (MIS) are as follows:

- The quality of the outputs of MIS is basically governed by the quality of input and processes.
- MIS is not a substitute for effective management, which means that it cannot replace managerial judgment in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives or senior management.
- MIS is less useful for making non-programmed decisions. Such types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in enterprises, where the culture of hoarding information and not sharing with other holds.

- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

(b) Following are some of the important implications of Management Information Systems (MIS) in business:

- MIS supports the managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill the organizational goals.
- An organization can survive and thrive in a highly competitive environment on the strength of a well-designed Management Information system that provides flexible and speedy access to accurate data.
- MIS helps in making right decision at the right time i.e. just on time.
- A good MIS may help in generating innovative ideas for solving critical problems.
- Knowledge gathered though MIS may be utilized by managers in unusual situations.
- MIS may be viewed as a process; it can be integrated to formulate a strategy of action or operation.
- MIS provides reports to management that can help in making effective, structured types as applicable to decisions of day-to-day operations.

(c) System Maintenance can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled Maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- **Corrective Maintenance:** Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.

- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- **Preventive Maintenance:** Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

(d) The major aspects that an Information Systems (IS) Auditor must consider while implementing an MIS in a large enterprise ABC Limited, to support middle and senior level management in administration and decision making are as follows:

An auditor must–

- Assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored;
- Ensure 'what project control standards are to be complied with' and determining the extent to which compliance is being achieved;
- Examine system documentation such as functional specifications to arrive at an opinion on controls;
- Provide a list of the standard controls, over operational concerns such as response time, CPU usage, and random access space availability that he/she can use as an assessment criteria;
- Review Feasibility Study Report and different work products of the Feasibility study phase;
- Include technical experts to seek their opinion on the technical aspects of development of MIS;
- Give control objectives, directives and in general, validate the opinion expressed by technical experts;
- Review some of the control considerations like –
  - Documented policy and procedures;
  - Established Project team with all infrastructure and facilities;
  - Developers/ IT managers are trained on the procedures;
  - Appropriate approvals are being taken at identified mile-stones;
  - Development is carried over as per standards, functional specifications;
  - Separate test environment for development/ test/ production / test plans;
  - Design norms and naming conventions are as per standards and are adhered to;

  - Business owners testing and approval before system going live; Version control on programs;
  - Source Code is properly secured;
  - Adequate audit trails are provided in system; and
  - Appropriateness of methodologies selected.
- Determine whether the system adequately meets earlier identified business requirements and needs post -implementation review.
- Determine if the expected benefits of the new system are realized and whether users are satisfied with the new system.
- Review which of the phases till implementation of MIS have not met desired objectives and whether any corrective actions were taken in post implementation review.

Question 2

(a) You are appointed as a member of the IT Steering Committee for IT implementation and deployment in a large company. What are the major functions of this committee? (6 Marks)

(b) COBIT 5 has a specific process "MEA02 Monitor, Evaluate and Assess the system of Internal Control." Discuss in brief any 6 key practices for assessing and evaluating the system of Internal Control in an enterprise based on this process. (6 Marks)

(c) The Cloud Computing Architecture comprises of two parts. Briefly describe these two parts. (4 Marks)

Answer

(a) The major functions of the IT Steering Committee would include the following:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of Information Systems’ plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;

- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

(b) The key practices for assessing and evaluating the system of internal controls in an enterprise based on the process MEA 02 Monitor, Evaluate and Assess the System of Internal Control are as follows:

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
- **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers.
- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self- assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.
- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

(c) A Cloud computing architecture consists of two parts - a **Front End** and a **Back End** that connect to each other through a network, usually the Internet. A central server is established to be used for administering the whole system.

- **Front End Architecture:** The front end of the cloud computing system is the side - the computer user sees and interacts through and comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.
- **Back End Architecture:** Back end is the "cloud" section of the system and refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment.

Question 3

(a) What should an IS Auditor evaluate while reviewing the adequacy of data security controls? (6 Marks)

(b) "Information has become a key resource for any type of business activity." Briefly discuss the various attributes of information. (6 Marks)

(c) List out the major activities to be carried out in the implementation of a Business Continuity Plan. (4 Marks)

Answer

(a) An Information Systems (IS) Auditor is responsible to evaluate the following while reviewing the adequacy of Data Security Controls:

- Who is responsible for the accuracy of the data?
- Who is permitted to update data?
- Who is permitted to read and use the data?
- Who is responsible for determining who can read and update the data?
- Who controls the security of the data?
- If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?

- Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
- The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

(b) Some of the important attributes of useful and effective information are as follows:

- **Availability -** Information is useless if it is not available at the time of need. Database is a collection of files which is collection of records and data from where the required information is derived for useful purpose.
- **Purpose/Objective -** Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data. The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.
- **Mode and format -** The modes of communicating information to humans should be in such a way that it can be easily understandable by the people and may be in the form of voice, text and combination of these two. Format design should be simple, relevant and should highlight important point in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information, the different formats can be used e.g. diagrams, graphs, curves are best suited for representing the statistical data.
- **Current/Updated -** The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed interval of time so that the current score will be available.
- **Rate -** The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive. For example- the information available from internet site should be available at a click of mouse.
- **Frequency -** The frequency with which information is transmitted or received affects its value. For example- the weekly reports of sales show little change as compared to the quarterly and contribute less for accessing salesman capability.
- **Completeness and Adequacy -** The information provided should be complete and adequate in itself because only complete information can be used in policy making. For example-the position of student in a class can be find out only after having the information of the marks of all students and the total number of students in a class.

- **Reliability -** It is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
- **Validity -** It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee supports in evaluating his performance.
- **Quality -** It means the correctness of information. For example, an over-optimistic manager may give too high estimates of the profit of product which may create problem in inventory and marketing.
- **Transparency -** It is essential in decision and policy making. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.
- **Value of Information -** It is defined as difference between the value of the change in decision behaviour caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

(c) In the implementation of a Business Continuity Plan (BCP), the major activities that should be carried out include the following:

- Defining the scope and context;
- Defining roles and responsibilities;
- Engaging and involving all stakeholders;
- Testing of program on regular basis;
- Maintaining the currency and appropriateness of Business Continuity Program;
- Reviewing, reworking and updating the Business Continuity Capability, Risk Assessments (RA) and Business Impact Analysis (BIAs);
- Managing costs and benefits associated; and
- Convert policies and strategies into action.

Question 4

(a) Describe the categories of Information Systems Audits. (6 Marks)

(b) What are the major documents that should be mandatorily part of any Business Continuity Management system? (6 Marks)

(c) IS Auditors review risks relating to IT systems and processes. Briefly discuss these risks.

(4 Marks)

Answer

(a) Information Systems Audits has been categorized into following types:

(i) **Systems and Application:** It is an audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) **Information Processing Facilities:** This audit verifies that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

(iii) **Systems Development:** It is an audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

(iv) **Management of IT and Enterprise Architecture:** This audit verifies that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

(v) **Telecommunications, Intranets, and Extranets:** This is an audit to verify that controls are in place on the client (end point device), server, and on the network connecting the clients and servers.

(b) The following documents (representative only) are classified as being part of the Business Continuity Management System:

- The Business Continuity Policy;
- The Business Continuity Management System;
- The Business Impact Analysis report;
- The Risk Assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The Business Continuity strategies;
- The overall and specific Incident Management Plans;
- The Business Continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;

- Exercise schedule and results;
- Incident log; and
- Training program.

(c) Information Systems (IS) Auditors review risks relating to IT systems and processes; some of them are as follows:

- Inadequate information security controls. For example - missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.
- Inefficient use of resources, or poor governance. For example - Huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.
- Ineffective IT strategies, policies and practices including a lack of policy for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.
- IT-related frauds that includes phishing, hacking etc.

Question 5

(a) Discuss "Authentication of Electronic Records" with reference to the IT Act. (6 Marks)

(b) In today's fiercely competitive business environment which allows for no downtime, a comprehensive Business Continuity Plan is of paramount importance. What are the various components of a BCM process? (6 Marks)

(c) What is a "Protected System" under the IT Act? (4 Marks)

Answer

(a) In IT Act, 2000, Section 3 defines “Authentication of Electronic Records”. This section provides the conditions subject to which an electronic record may be authenticated by means of affixing Digital Signature. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

The provisions stated in the Act are as follows:

Authentication of Electronic Records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair. ***[Section 3]***

(b) The various components of Business Continuity Management (BCM) Process are as follows:

- **BCM – Process:** The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.
- **BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
- **BCM – Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services.
- **BCM – Development and Implementation Process:** Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
- **BCM – Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.
- **BCM – Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

(c) In IT Act, 2000, Section 70 defines "Protected System" that is as follows:

Protected System

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system. ***[Section 70]***

Question 6

(a) You are appointed as the IS Auditor of a large company with multiple locations across the globe which are connected to a common platform. What are the steps you would take as part of your preliminary evaluation to fully comprehend the technology environment and control issues? (6 Marks)

(b) Discuss in brief the major concerns to be addressed by an auditor in the different activities of the Programming Management Control Phase. (6 Marks)

(c) What are the key benefits of GEIT? (4 Marks)

Answer

(a) An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

- Analysis of business processes and level of automation;
- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business;
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture;
- Studying network diagrams to understand physical and logical network connectivity;
- Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government;
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems; and
- Finally, Studying Information Technology policies, standards, guidelines and procedures.

(b) Some of the major concerns that an Auditor should address under different activities involved in Programming Management Control Phase are as under:

Phase	**Audit Trails**
Planning	• They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired. • They must evaluate how well the planning work is being undertaken.
Control	• They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. • They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample if past and current software development and acquisition projects carried out at different locations in the organization they are auditing.
Design	• Auditors should find out whether programmers use some type of systematic approach to design. • Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
Coding	Auditors should seek evidence – • On the level of care exercised by programming management in choosing a module implementation and integration strategy. • To determine whether programming management ensures that programmers follow structured programming conventions. • To check whether programmers employ automated facilities to assist them with their coding work.
Testing	• Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. • Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. • Auditors primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.

Operation and Maintenance	• Auditors need to ensure that effective and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. • Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

(c) Benefits of Governance of Enterprise IT (GEIT) are as follows:

- It provides a consistent approach integrated and aligned with the enterprise governance approach.
- It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.
- It ensures that IT-related processes are overseen effectively and transparently.
- It confirms compliance with legal and regulatory requirements.
- It ensures that the governance requirements for board members are met.

Question 7

Write short notes on any ***four*** *of the following:*

(a) Time Bomb vs. Logic Bomb

(b) Cloud vs. Grid Computing

(c) Boundary Control techniques

(d) Community Cloud

(e) ISO 27001 *(4 x 4 = 16 Marks)*

Answer

(a) **Time Bomb:** These are the programs that cause perverse activity, such as disruption of computer system, modifications, or destructions of stored information etc. on a date and time for which it has been developed. In other words, time bomb lies idle until some date or time triggers it. The computer clock initiates it.

Logic Bomb: These are the programs that are activated by combination of events. In other words, logic bombs lie idle until some specified circumstances trigger it. Once triggered, the bomb sabotages the system by destroying programs, data or both.

(b) Some pertinent differences between Grid Computing and Cloud Computing are as follows:

Grid Computing	Cloud Computing
Grid Computing enables heterogeneous resources of computers to work	Cloud computing provides the facility to access shared resources and common

cooperatively and collaboratively to solve a scientific problem.	infrastructure offering services on demand over the network to perform operations that meet changing business needs.
While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit.	While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
A computational grid focuses on computationally intensive operations.	Cloud computing offers two types of instances: standard and high-CPU.

(c) Major Boundary Control Techniques are as follows:

- **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst.
- **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.
- **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database; independent to a user identification details, or a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
- **Biometric Devices:** Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

(d) **Community Cloud:** In Cloud Computing, the Community Cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

Community Cloud supports Collaborative and Distributive Maintenance, Partial Security, cost Effectiveness, collaborative work on the cloud, sharing of responsibilities among the organizations. The limitation of the community cloud is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud. It is not suitable in the cases where there is no collaboration.

(e) **ISO 27001:** ISO 27001 is the international best practice and certification standard for an Information Security Management System (ISMS). An ISMS is a systematic approach to manage Information security in an IS environment through which an organization identifies, analyzes and addresses its information security risks. It encompasses people, processes and IT Systems. ISO 27001 defines how to organise information security in any kind of organization, profit or non-profit, private or state-owned, small or large. This standard is the foundation of information security management that enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the organisation as defined policies and procedures.

The ISO 27001 can act as the extension of the current quality system to include security; provides an opportunity to identify and manage risks to key information and systems assets; provides confidence and assurance to trading partners and clients; acts as a marketing tool and allows an independent review and assurance to you on information security practices.