QUIZZES

CORRECTION KEY





CERTIFIED ISO/IEC 27001 LEAD IMPLEMENTER TRAINING COURSE

**Quiz 1: Standards and regulatory frameworks**

1. **Which standard below provides requirements for an information security management system (ISMS)?**
2. **ISO/IEC 27001**
3. ISO/IEC 27002
4. ISO/IEC 27000

*ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system. In addition, the standard includes requirements for the assessment and treatment of information security risks.*

1. **Which of the statements below is correct?**
2. **Organizations can obtain certification against ISO/IEC 27001**
3. Organizations can obtain certification against ISO/IEC 27005
4. Organizations cannot obtain certification against ISO/IEC 27001

*Organizations can obtain certification against ISO standards that specify requirements (also referred to as normative standards), but not against ISO standards that provide guidelines. ISO/IEC 27001 is a normative standard and, as such, organizations can obtain certification against it. On the other hand, ISO/IEC 27005 is a guideline standard and therefore organizations cannot obtain certification against it.*

1. **Which international standard provides a reference set of information security controls?**
2. **ISO/IEC 27002**
3. ISO/IEC 27701
4. ISO/IEC 27005

*ISO/IEC 27002 provides guidelines on the selection, implementation, and management of information security controls.*

1. **In what areas do ISO/IEC 27001 and the General Data Protection Regulation (GDPR) overlap?**
2. PII collection and processing and the rights of data subjects
3. **Data confidentiality, availability, and integrity, and risk assessment**
4. Physical security, access control, and continual improvement

*The implementation of ISO/IEC 27001 controls can help establish compliance with the GDPR in areas such as data confidentiality, availability, and integrity, as well as risk assessment.*

1. **What does STAR stand for in the cloud security alliance (CSA)?**
2. **Security, Trust, and Assurance Registry**
3. Security, Task, Action, and Results
4. Security, Transparency, Assurance, and Response

*CSA has a three-tiered cloud provider assurance program known as the CSA Security, Trust, and Assurance Registry (STAR) program. STAR consists of self-assessment, third party audit, and continuous monitoring.*

1. **Which of the following is NOT an advantage of ISO/IEC 27001?**
   1. Marketing
   2. Incremental revenue
   3. **Performance evaluation**

*The major advantages of ISO/IEC 27001 include, but are not limited to, the improvement of information security, good governance, conformity, marketing, and incremental revenue.*

**Quiz 2: Information security management system (ISMS)**

1. **A management system is a system that allows organizations to establish policies and objectives and to subsequently implement them.**
2. **True**
3. False

*Organizations use management systems to develop policies and put them into effect through objectives using: an organizational structure, systematic processes and associated resources, an effective assessment methodology, and a review process.*

1. **What is an integrated management system (IMS)?**
2. A management system that integrates all the guidelines and best practices so as to enable the achievement of its purpose and mission
3. **A management system that integrates all the components of a business into a coherent system so as to enable the achievement of its purpose and mission**
4. A management system that integrates all frameworks and resources so as to enable the achievement of its purpose and mission

*An integrated management system (IMS) enables the integration of all the components of a business, which allows an organization to achieve its purpose and mission.*

1. **Which of the options below is a benefit of an effective ISMS?**
2. **Reducing information security risks and minimizing exposure to information security breaches**
3. Processing and removing redundant information
4. Exposing the confidentiality of information

*An effective ISMS helps an organization in reducing information security risks and minimizing exposure to information security breaches, protecting assets and sensitive information, creating competitive advantage, improving reputation and increasing customer confidence, and protecting the confidentiality, availability, and integrity of information.*

1. **Annex A of ISO/IEC 27001 consists of 114 controls that organizations have to consider when intending to comply with the standard.**
2. True
3. **False**

*Annex A of ISO/IEC 27001 consists of 93 controls that should be considered by organizations that intend to comply with the standard.*

1. **Which process model does ISO/IEC 27001 adopt?**
2. Plan, improve, operate, and act
3. Plan, manage, check, and act
4. **Plan, do, check, and act**

*ISO/IEC 27001 adopts the “Plan-Do-Check-Act” (PDCA) process model, also known as the Deming wheel. This process model is applied to the structure of all the processes in an information security management system.*

1. **Which standard supports the controls of Annex A?** 
   1. **ISO/IEC 27002**
   2. ISO/IEC 27003
   3. ISO/IEC 27701

*The information security controls listed in Annex A of ISO/IEC 27001 are supported by the guidance of ISO/IEC 27002 in clauses 5 to 8.*

1. **What is the term for the identification and orderly management of processes within an organization?**
   1. Input element
   2. Information security control
   3. **Process approach**

*The identification and orderly management of processes within an organization, especially the interactions of processes, is called “process approach.”*

**Quiz 3: Fundamental information security concepts and principles**

1. **What are information, software, services, and people considered as?**
   1. Inventories
   2. **Assets**
   3. Information

*An asset is considered as an item, thing, or entity that has potential or actual value to an organization. Types of assets include information, software, computer, service, people and their qualifications and skills, reputation and image, etc.*

1. **Which of the following statements regarding information security is correct?**
2. **Information security protects the confidentiality, integrity, and availability of information regardless of its type and form**
3. Information security protects the confidentiality, integrity, and availability of information only in an electronic form
4. Information security protects the organization against threats by only identifying the threat source

*Information security covers information of all types, printed or handwritten, transmitted by email or website, as well as information given during conversations.*

1. **What does confidentiality ensure?**
   1. **That the information is accessible to the authorized individuals**
   2. That the information is accurate and complete
   3. That the information is available

*Confidentiality ensures that only authorized users have access to protected and sensitive data.*

1. **Which of the following is NOT an example of a threat?**
2. Theft of media or documents
3. **Complicated user interface**
4. Unauthorized use of equipment

*A threat is the potential cause of an unwanted incident, which can harm either the system or organization. Complicated user interface is not a threat but a software vulnerability.*

1. **Performance degradation can have an impact on the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of information.**
2. **Availability**
3. Confidentiality
4. Integrity

*Performance degradation can potentially affect the availability of information because in such cases the information may not be accessible when or as it is required.*

1. **Vulnerability is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.**
   1. True
   2. **False**

*Risk is often expressed in terms of a combination of the consequences of an event and the associated “likelihood” of occurrence: Risk = likelihood x consequence.*

1. **What type of controls are the segregation of duties, job rotations, and approval processes?**
2. Technical controls
3. Managerial controls
4. **Administrative controls**

*Segregation of duties, job rotations, and approval processes are controls related to the organizational structure, hence defined as administrative controls.*

1. **What type of control is the separation of development, testing, and operating environment?**
2. **Preventive control**
3. Detective control
4. Corrective control

*The separation of development, testing, and operating environment reduces the risk of unauthorized access or changes to the operational environment, thus preventing any potential incident. For that reason, it is a preventive control.*

1. **An organization has installed a fire alarm in its premises. What type of control is this?**
2. Preventive and administrative
3. Corrective and managerial
4. **Detective and technical**

*By function, alarms are detective controls that help detect risks. By type, a fire alarm is a technical control because it requires technical installation.*

1. **Assets and controls can present \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ that can be exploited by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**
   1. Threats, vulnerabilities
   2. **Vulnerabilities, threats**
   3. Threats, risks

*Vulnerability is the weakness of an asset or control that can be exploited by one or more threats.*

**Quiz 4: Initiation of the ISMS implementation**

1. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ includes the application of best practices in project management.**
2. Business approach
3. Iterative approach
4. **Systematic approach**

*The systematic approach includes the application of best practices in project management such as ISO 10006.*

1. **What is the correct definition of the term project?**
2. **A unique process consisting of a set of coordinated and controlled activities**
3. A small identified object of work
4. The process of planning, organizing, and controlling a set of activities

*According to ISO 9000, a project is defined as a unique process consisting of a set of coordinated and controlled activities with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost, and resources.*

1. **Which of the following statements is correct?**
2. The ISMS should be implemented with new technology because this helps the optimization of the processes
3. The roles and responsibilities of interested parties should be defined after the implementation process
4. **The ISMS should be integrated into existing processes of the organization**

*The initial system should be designed with the technology that is already in place within the organization; the optimization of the ISMS with more efficient technologies can be completed in the continual improvement phase. Roles and responsibilities of all interested parties should be defined early in the implementation process.*

1. **Which step follows the initiation of the ISMS implementation according to the PECB framework?**
2. Organizational structure
3. Risk management
4. **Understanding the organization**

*After the initiation of the ISMS implementation, understanding the organization is the next step in the PECB framework.*

1. **What does the iterative approach include?**
2. Integration of the ISMS into the context of commercial activities across the organization
3. **Rapid implementation of the ISMS by adhering to the minimum requirements of the standard and proceeding with continual improvement thereafter**
4. Harmonization of the ISMS with other management systems established in the organization

*An iterative approach involves the rapid implementation of the ISMS by giving more effort on its continual improvement later afterwards.*

**Quiz 5: Understanding the organization and its context**

1. **Why is it important to understand the mission, objectives, values, and strategies of an organization?**
2. To facilitate the internal audit process
3. To create a map of all the processes
4. **To understand the information security challenges the organization faces**

*To understand the information security challenges that an organization faces, it is necessary to obtain general information on its mission, strategy, objectives, and values.*

1. **Which of the options below represents an ISMS objective?**
2. Integration of new technologies
3. **Protection of critical assets**
4. Improvement of the information security incidents

*An information security management system should help an organization protect its critical assets.*

1. **Which of the following statements is correct?**
2. Standards take precedence over laws
3. **The implementation of an ISO standard is not a legal requirement**
4. Compliance with the ISO/IEC 27001 ensures compliance with data protection laws and regulations

*The implementation of an ISO standard is a voluntary decision, not a legal requirement. An organization must comply with the applicable laws and regulations because, in all cases, laws take precedence over standards.*

1. **Do outsourcing activities of an organization impact its ISMS?**
2. No, because outsourcing activities should not be included in the ISMS scope
3. Yes, because outsourcing activities do not directly support the business activities
4. **Yes, because outsourcing activities can affect the determination of the ISMS scope**

*An organization should consider all functions that are outsourced including those to independent suppliers when determining the scope of the ISMS.*

1. **What can be included when analyzing the internal environment of an organization?**
2. **Information systems, information flow, and decision-making processes**
3. Information systems boundaries and physical boundaries
4. Trends having impact on the objectives of the organization

*When analyzing its internal environment, the organization should identify the key aspects in which it seeks to achieve its objectives. Internal environment includes information systems, information flow, and decision-making processes.*

**Quiz 6: ISMS scope**

1. **What should an organization do when establishing its ISMS scope?**
2. Determine the amount of effort required for the ISMS implementation
3. Determine the internal and external information security risks
4. **Determine the boundaries and applicability of the ISMS**

*When establishing the ISMS scope, an organization should determine the boundaries and applicability of the ISMS.*

1. **Which of the following is considered an ISMS boundary?**
2. **Information systems boundaries**
3. Critical assets boundaries
4. Information security incident boundaries

*There are three main boundaries of the ISMS: information systems boundaries, physical boundaries, and organizational boundaries.*

1. **In which of the ISMS boundaries below should the evaluation of the responsibilities of decision-makers and their areas of influence in the organization be done?**
2. **Organizational**
3. Physical
4. Information systems

*The organizational boundaries of the ISMS scope comprise of the organizational structures and responsibilities of managers. Thus, they can be defined upon an evaluation of the responsibilities of decision-makers and their areas of influence in the organization.*

1. **Which of the following is included in the ISMS scope?**
2. The description of the changes in the external environment
3. The description of the information security risks related to the ISMS
4. **The description of the roles and responsibilities related to the ISMS**

*The ISMS scope should include the description of the roles and responsibilities related to the ISMS, key characteristics of the organization, organizational processes, list of information assets and systems, maps of geographic locations, and details and reasons for exclusions.*

1. **Which of the following statements regarding the ISMS scope is correct?**
   1. The ISMS scope should be categorized as confidential information
   2. The ISMS scope should not consider the information systems
   3. **The ISMS scope should be available as documented information**

*To comply with ISO/IEC 27001, an organization should keep its ISMS scope available as documented information.*

1. **When can an organization make a change in the ISMS scope?**
2. When the organization is applying for certification
3. **When new risk scenarios are to be considered**
4. When the list of information assets has been modified

*The ISMS scope can change over time for several reasons, including consideration of new risk scenarios that, if not considered, may prevent the organization from achieving its information security objectives. Other changes can be made due to the changes in the external environment of an organization or because the organization wants to extend the scope to other units.*

**Scenario-based quiz 1: Sections 1-7**

*YoMedia* is a marketing agency that primarily collects and analyzes customer and business data for targeted advertising campaigns. This is done to keep the data complete and accurate. Recently, *YoMedia* has decided to implement an information security management system (ISMS) to better protect its confidential information. The team assigned to implement the ISMS dedicated their time and resources to analyze the existing system by conducting interviews with the employees of the company and using various techniques to gather information on the existing processes, procedures, policies, and controls. They found out that the company uses an access control software that allows only authorized users to access sensitive information. However, their software application and programs have a complicated user interface that causes a lot of data input errors by the personnel on a daily basis. While conducting interviews, they learned that there were at least two employees of each department who did not receive any security trainings in the last two years. The team assigned to implement the ISMS concluded that the company should redefine the training needs and simplify its user interface.

Based on the above-mentioned scenario, answer the following questions:

1. ***YoMedia* has implemented an access control software that allows only authorized users to access sensitive data. What is the purpose of this information security control?**
2. **To avoid or prevent errors or malicious acts**
3. To detect the occurrence of errors or malicious acts
4. To correct the identified errors or malicious acts and prevent their recurrence

*Using an access control software is classified as a preventive control, its purpose being to avoid or prevent the occurrence of problems.*

1. **What controls should the company implement to ensure that the information is complete and accurate?**
2. Data encryption controls
3. **Data integrity controls**
4. Backup and recovery controls

*Data integrity controls are essential in ensuring that the information is accurate, complete, authentic, and safe from unauthorized access in order for users to be able to rely on the correctness of information when processing it.*

1. **Which of the situations presented in the scenario is considered a threat?**
2. **The data input error by the personnel**
3. The complicated user interface
4. The use of programs or applications by personnel on a daily basis

*The data input error by the personnel is a threat that has the potential to harm assets such as information, processes, systems, and the company. The complicated user interface on the other hand, presents a vulnerability of the system.*

1. **By analyzing the existing system and conducting interviews with the employees, *YoMedia* conducted a:**
2. Risk management process
3. Security control designation
4. **Gap analysis process**

*The first step of a gap analysis is to determine the current state which is done by analyzing the existing processes, procedures, policies, and controls or by gathering information and conducting interviews with the employees of the company.*

1. **What does the fact that at least two employees of each department in *YoMedia* did not receive any security trainings in the last two years indicate?**
2. The presence of a threat that is related to the possible functions of the company
3. The presence of an information security risk expressed as the combination of the impact and occurrence of an incident in the company
4. **The presence of a vulnerability in the existing personnel procedures of the company**

*The lack of regular security trainings for every employee is a vulnerability of the company that can be exploited by one or more threats.*

**Quiz 7: Leadership and project approval**

1. **Which of the statements below regarding the definition of a business case is NOT true?**
2. **A tool that promotes ISO/IEC 27001**
3. A way to define clear objectives
4. A tool for decision-making support

*A business case is a tool that helps planning and decision-making, including decisions regarding the opportunities, choices, and the right time to initiate an action or a sequence of actions. A business case promotes the ISMS project, not the ISO/IEC 27001 standard.*

1. **Which resources are necessary for the implementation of an ISMS?**
2. Cloud, management, and human resources
3. Technology tools as they surpass the knowledge of employees for information security
4. **People, information, facilities, transportation, finance**

*In order for the implementation of the ISMS to be carried out successfully, the ISMS project manager must ensure that the necessary resources are identified. These resources include people, partners and suppliers, transportation, finance, information and data, facilities, ICT systems, etc.*

1. **Which of the following statements is correct for an ISMS project plan?**
2. The development of a project plan is a sequential process
3. **The development of a project plan is an iterative process**
4. The development of a project plan is an incremental process

*The development of a project plan is an iterative process. This process requires several repetitions. For example, the first step can describe the activities in general and does not specify the duration of activities, while the final step will detail the specific resources and specify the completion dates.*

1. **An ISMS project team consists of the project champion, project manager, project management team, project team, and interested parties.**
2. **True**
3. False

*The ISMS project team consists of the project champion, project manager, project management team, project team, and the interested parties.*

1. **Who must approve the ISMS business case and project plan?**
2. Any of the organization’s employees
3. **The organization’s management**
4. The head of the IT department

*The organization’s management must approve the ISMS business case and project plan. The declarations of support and authorization of the management must be formally documented.*

**Quiz 8: Organizational structure**

1. **Who shall ensure the assignment of ISMS roles and responsibilities according to ISO/IEC 27001?**
2. The human resources
3. **The top management**
4. The heads of departments

*The top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated in the organization.*

1. **What is one disadvantage of the traditional organizational model in information security governance?**
2. Strong capacity of influence because the CISO is on the same or lower hierarchical level with IT managers
3. No real or potential conflicts of interest
4. **Poor consideration to issues related to information security**

*Because of the traditional hierarchy, the information security manager cannot properly exercise their mandate on the organization, thus leading to poor consideration to issues related to information security.*

1. **What does “CISO” stand for in an information security infrastructure?**
2. **Chief information security officer**
3. Corporate information support officer
4. Champion information security officer

*One of the most important elements in defining the information security management and its governance is placing the chief information security officer (CISO) in the organization’s hierarchy.*

1. **It is advisable for the chief information security officer (CISO) to report directly to the information security committee.**
2. **True**
3. False

*To manage the risk of any interference of conflict of interest, it is advisable that the CISO send the reports directly to the information security committee rather than to the information resources management.*

1. **Which of the following is NOT a key committee in an organization’s information security management system implementation project?**
2. Information security committee
3. Operational committee
4. **A third party committee**

*Management committee, information security committee, and operational committee are considered the key committees in ensuring the proper functioning of the ISMS. A third party committee is usually not part of decision-making processes in an organization.*

1. **The main objective of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is to ensure the proper functioning of the ISMS and security controls.**
   1. Management committee
   2. **Information security committee**
   3. Operational committee

*The information security committee aims to ensure the proper functioning of the information security management system and security controls in the organization. It is usually chaired by the chief information security officer (CISO).*

**Quiz 9: Analysis of the existing system**

1. **What is a gap analysis?**
2. **A technique used to determine the steps to move from a current state to a desired future state**
3. A technique used to determine the ways in which a process might potentially fail, with the objective of eliminating the likelihood of such a failure
4. A technique used to evaluate the organization against its competitors and produce a comprehensive long-term planning

*Gap analysis is a technique that organizations utilize to determine what steps are needed to move from their current state to a desired state.*

1. **An organization has reported that its processes have reached the level of best practices. What level of maturity is this?** 
   1. Quantitatively managed
   2. **Optimized**
   3. Initial

*If the process has reached the level of best practice, following a steady improvement in comparison with other organizations, it means that the maturity level of the process is optimized.*

1. **Which of the following is NOT a level of maturity?**
2. Quantitatively managed level
3. Non-existent level
4. **Objective-based level**

*There are six levels of maturity: non-existent, initial, managed, defined, quantitatively managed, and optimized.*

1. **Which type of interviews prevents the “bandwagon effect”?**
2. **Individual interviews**
3. Group interviews
4. Questionnaires

*Individual interviews prevent any dominant member of the group from influencing the response of others, which is otherwise known as the “bandwagon effect.”*

1. **An organization has concluded that its processes are standardized, documented, and communicated. What level of maturity is this?**
   1. Level 2: Managed
   2. **Level 3: Defined**
   3. Level 4: Quantitatively managed

*If a process is standardized, documented, and communicated in an organization, it means that the maturity level of the process is defined.*

1. **Which of the following is an effective visual tool to present the gap analysis results?**
2. **Radar chart**
3. Ichikawa diagram
4. Cause-and-effect diagram

*Radar chart is an effective visual tool used to present the differences that have been examined during the gap analysis process.*

**Quiz 10: Information security policy**

1. **Who shall establish the information security policy according to ISO/IEC 27001?**
2. **The top management**
3. External interested parties
4. The information security manager

*ISO/IEC 27001 specifies that the top management shall establish an information security policy that is appropriate to the purpose of the organization and includes a commitment to continual improvement of the information security management system.*

1. **What is the difference between a policy and a guideline?**
2. **A policy states the intentions and direction of an organization, whereas a guideline states how something should be done**
3. A policy is a type of a guideline that provides guidance for different topics
4. A policy is a document stating how something should be done, whereas a guideline is an explanation of procedures

*The main goal of a policy is to provide guidance on a particular topic, whereas a guideline states a general rule, principle, or information for a procedure.*

1. **Which type of policy specifies the internal requirements of another policy and covers a very specific target audience?**
2. High-level general policies
3. High-level specific policies
4. **Topic-specific policies**

*In an ISMS, topic-specific policies are policies that support the information security policy. These policies determine how to proceed in order to ensure information security in specific application areas, e.g., access control policy.*

1. **Which of the options below is a high-level specific policy?**
2. Incident management policy
3. **Information security policy**
4. Policy on cryptography

*An information security policy addresses the general rules and practices for information security but can be applicable to specific areas or functions of the organization. As such, it is a high-level specific policy.*

1. **What is the first phase of the information security policy development life cycle?**
2. Policy construction
3. Policy monitoring and maintenance
4. **Risk assessment**

*Risk assessment is the first phase of the policy development life cycle. Risk assessment helps identify the assets that should be protected and potential threats and vulnerabilities to those assets.*

1. **Who shall communicate the information security policy to the relevant interested parties?**
2. The ISMS coordinator
3. The information security manager
4. **The top management**

*It is the responsibility of the top management to approve the policies and communicate them to the relevant interested parties.*

**Quiz 11: Risk management (Part 1)**

1. **What does ISO/IEC 27005 provide?**
   1. Requirements for information security risk management
   2. Practical methods for the management of all risks
   3. **Guidelines for information security risk management**

*ISO/IEC 27005 provides guidelines for organizations in meeting the requirements of ISO/IEC 27001 for information security risk management.*

1. **What criteria should be considered when selecting a risk assessment methodology?**
2. New technologies
3. **Personnel competence and training**
4. Risk treatment plan

*Criteria to consider when selecting a risk assessment methodology includes documentation, training, support, and competent personnel available.*

1. **What type of asset is information categorized as?**
2. Supporting asset
3. Secondary asset
4. **Primary asset**

*According to ISO/IEC 27005, information is a primary asset.*

1. **Which phase of risk assessment aims to find, recognize, and describe risks?**
   1. **Risk identification**
   2. Risk evaluation
   3. Risk analysis

*The purpose of risk identification is to find, recognize, and describe risks that might help or prevent an organization in achieving its objectives.*

1. **Which phase of risk management takes into consideration the source, likelihood, and consequences of risk?**
2. Risk treatment
3. **Risk analysis**
4. Risk evaluation

*Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness.*

1. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the process of comparing the results of risk analysis with the risk criteria to determine whether the risk is acceptable.**
2. Risk treatment
3. **Risk evaluation**
4. Risk acceptance

*To evaluate a risk, the organization should compare the results of risk analysis with the risk criteria defined during the context establishment.*

**Quiz 12: Risk management (Part 2)**

1. **Which phase of risk management is used to modify risk?**
2. Risk evaluation
3. Risk identification
4. **Risk treatment**

*The purpose of risk treatment is to select and implement options for addressing risks.*

1. **Upon an analysis of risk, an organization found out that around 0.4% of its electronic transactions are fraudulent. The organization has decided to outsource the payment process to an external organization in order to reduce the risk. What risk treatment option is this?**
2. Risk retention
3. **Risk sharing**
4. Risk modification

*Risk sharing is the decision to share certain risks with external parties, such as insurance or outsourcing.*

1. **The risk that remains after risk treatment is known as:**
2. Inherent risk
3. Treated risk
4. **Residual risk**

*Residual risk is defined as the risk that remains after the implementation of controls used to treat the inherent risk.*

1. **What is the aim of the communication and consultation activity?**
2. **To achieve agreement on how to manage risks**
3. To review and approve risk treatment plans
4. To determine whether a residual risk falls above or below the threshold

*The communication and consultation activity aims to achieve agreement on how to manage risks by exchanging and/or sharing information about risk with the risk owners and other relevant interested parties.*

1. **An organization has decided to move its information processing facilities to a place where the risk of flooding is low. Which risk treatment option has the organization chosen?**
   1. **Risk avoidance**
   2. Risk evaluation
   3. Risk sharing

*When the organization determines that it is more cost-effective to avoid a risk than treat it, the organization chooses to avoid the risk.*

1. **Which of the following is NOT a risk treatment option?**
2. Share the risk
3. Modify the risk
4. **Trade the risk**

*Risk treatment options are risk modification, risk retention, risk avoidance, and risk sharing.*

1. **Which of the following is an example of risk sharing?**
2. Removing the assets from an area at risk
3. Retaining the current risk
4. **Distributing risk to another party**

*Risk sharing is the decision to share risks with external parties.*

**Quiz 13: Statement of Applicability**

1. **Which statement regarding the Statement of Applicability (SoA) is correct?**
2. SoA is a tool for decision-making support
3. **SoA is a document that is specific to ISO/IEC 27001**
4. SoA is a key process of the ISMS

*A Statement of Applicability is a document specific to ISO/IEC 27001 and there is no equivalent in other management system standards such as ISO 9001 or ISO 14001.*

1. **How does an organization select the security controls of ISO/IEC 27001, Annex A?**
2. **Based on the risk assessment results**
3. Based on the top management’s decision
4. Based on the internal audit report

*An organization should review all the 93 security controls in Annex A and determine their applicability based on the results of risk assessment.*

1. **Why should an organization create a Statement of Applicability?**
2. **To document the justifications for inclusion and exclusion of Annex A controls**
3. To ensure that the ISMS is aligned with the mission of the organization
4. To ensure compliance with the industry best practices

*Statement of Applicability is a key document of the ISMS which documents the organization’s justifications for including and excluding controls of Annex A.*

1. **ISO/IEC 27001 requires that the organization select its security controls only from Annex A.**
2. True
3. **False**

*The list of security controls in Annex A of ISO/IEC 27001 is not exhaustive. The organization may add additional controls from other sources as well.*

1. **An organization has drafted its Statement of Applicability (SoA) which comprises of the list of applicable and inapplicable information security controls of Annex A along with the justification for the exclusion of the inapplicable controls. Does this SoA comply with the ISO/IEC 27001 requirements?**
2. Yes, because it has included the list of selected controls from Annex A and the reasoning of their selection
3. **No, because it does not justify the selection of information security controls of Annex A**
4. No, because it does not include the list of any controls from Annex A determined as inapplicable

*The SoA must include all the implemented controls and those that are planned but not yet implemented, the justification for their selection, and the list of controls deemed as inapplicable along with their justification for exclusion.*

**Scenario-based quiz 2: Sections 8-13**

*Research Metric* is a research development company, highly dependent on the protection of its development and research data and the availability of its IT systems. They have recently decided to implement an information security management system (ISMS) and, as such, the top management assigned the role of the ISMS project manager to Melanie based on her outstanding knowledge and skills in project and information security management. In addition, theydecided to include only the key processes in the ISMS scope and stop collecting and processing sensitive information of their customers until the ISMS becomes fully operational.

Since the company had a security policy in place, the ISMS project team decided to adopt it by renaming it to “Information security policy.” Following the conduct of a risk assessment, *Research Metric* prepared a document containing a list of all information security controls deemed applicable to their ISMS.

Answer the following questions by referring to the above-mentioned scenario:

1. **In addition to establishing the ISMS project and managing it throughout its operational life, Melanie is responsible for:**
2. **Formalizing the ISMS objectives**
3. Providing adequate resources for the ISMS implementation
4. Approving the risk acceptance criteria

*The ISMS project manager is responsible for formalizing the ISMS objectives. The other two options fall under the responsibilities of the top management of the company.*

1. **Which ISMS scope boundary has *Research Metric* defined?** 
   1. **Organizational boundaries**
   2. Physical boundaries
   3. Information systems boundaries

*Key processes are considered when defining the organizational boundaries of the ISMS scope.*

1. **Why should the security policy be updated instead of only being renamed to “Information security policy”?**
2. To address the information security risks
3. To provide an overview of information assets
4. **To reflect the information security objectives**

*An information security policy should include information security objectives or provide a framework for setting information security objectives; hence, the existing security policy should have been updated to reflect these requirements.*

1. **Which risk treatment option has *Research Metric* utilized when it decided to stop collecting and processing sensitive information of their customers until the ISMS was fully operational?**
2. **Risk avoidance**
3. Risk sharing
4. Risk retention

*Risk avoidance is the cancellation or modification of an activity or set of activities related to risk.*

1. ***Research Metric* has prepared a document containing a list of all information security controls deemed applicable to their ISMS.** **This document is known as:**
2. **Statement of Applicability**
3. Risk assessment report
4. Information security strategy

*A Statement of Applicability is a document describing the control objectives and controls that are relevant and applicable to the organization’s ISMS.*

**Quiz 14: Documented information management**

1. **What should an organization do in order to comply with ISO/IEC 27001?**
2. **Develop a procedure for the control of the documented information**
3. Develop a form for the control of the documented information that is visible only to the top management
4. Develop a guideline for the control of the documented information only when requested by an executive

*Organizations are required to develop a procedure for the control of documented information and records so that they are conform to ISO/IEC 27001.*

1. **In order to comply with ISO/IEC 27001, organizations should fulfill some mandatory requirements on how to document controls.**
2. True
3. **False**

*There is no mandatory requirement on how to document processes and security controls according to ISO/IEC 27001. As such, it is up to each organization to decide on how to document the processes and security controls.*

1. **What does a master list of documents in the context of ISMS contain?**
2. **All documentation related to the ISMS in a single list**
3. Key parts of the documentation related to the ISMS in single lists
4. A group of the most accessed documents in a single list

*Creating a master list is highly recommended because it facilitates the process of finding and accessing documents.*

1. **What does a procedure describe?**
2. **An orderly sequence of actions aimed at achieving a goal**
3. A guide to an actual description of policies
4. A detailed explanation of the functioning of a process

*A procedure contains specific instructions that explain clearly the steps to determine the implementation of the policy, guidelines, and supporting standards. Option B refers to a security manual and option C to a narrative process.*

1. **Which is the correct sequence of actions when establishing a procedure to manage the document life cycle?**
2. Approval, identification, classification, modification, disposal, archiving, adequate use, and distribution
3. **Creation, identification, classification, modification, approval, distribution, adequate use, archiving, disposal**
4. Distribution, identification, modification, classification, disposal, archiving, adequate use, and creation

*Neither approval nor distribution can be done without creation and its consequent steps taking place first. The process of managing the document life cycle is done in the following steps: creation, identification, classification, modification, approval, distribution, adequate use, archiving, and disposal.*

1. **During which of the following cases is the implementation of a documented information management system especially useful?**
2. **Facilitating access to, referencing, disseminating, and archiving documents**
3. Losing traceability of the documented information
4. Managing parts of the document life cycle

*A documented information management system ensures traceability and access to documents by managing the different levels of authorization to access, use, and dissemination of data by managing the entire document life cycle, not just parts of it.*

**Quiz 15: Selection and design of controls**

1. **What does an organization’s security architecture represent?**
2. A set of disciplines used to design solutions to address security requirements at a human level
3. A set of disciplines used to design solutions to address security requirements at an operational level
4. **A set of disciplines used to design solutions to address security requirements at a system level**

*The organization’s security architecture implements the building blocks of information security infrastructure across the entire organization. It focuses on a strategic design of a set of security services that can be leveraged by multiple applications, systems, or business processes, not on individual functional and nonfunctional components.*

1. **Which services aim at normalizing user identification and promoting shared authentication across the organization?**
2. Boundary control services
3. **Access control services**
4. Cryptographic services

*Access control services promote and use reduced-sign-on (RSO) or single-sign-on (SSO) services as common security services. These services aim at normalizing user identification and promoting shared authentication across the organization.*

1. **Boundary control services control the transfer of information from a state or set of systems to another.**
2. **True**
3. False

*Boundary control systems are intended to enforce security zones of control by isolating entry points from one zone to another (choke points). They also control the transfer of information from a state or set of systems to another.*

1. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ matrix for security architecture development covers six cascading levels, also known as the “6 Ws.”**
2. The IT Infrastructure and Library (ITIL)
3. The Open Group Architecture Framework (TOGAF)
4. **The Sherwood Applied Business Security Architecture (SABSA)**

*SABSA comprises frameworks, terminology, models, and processes. The six levels of design are asset (What?), motivation (Why?), process (How?), people (Who?), location (Where?), and time (When?).*

1. **What are some of the steps to take when preparing for the implementation of information security controls?**
2. **Conduct a cost analysis and prepare the required documented information**
3. Conduct a cost analysis and avoid the intended results and outputs
4. Conduct a cost analysis and prepare a general list of activities without providing details

*There are seven steps that organizations should take when preparing for the implementation controls. Conducting a cost analysis and preparing the required documented information are among those seven.*

1. **Why is it important to involve employees in the draft, review, and validation processes?**
2. Because it helps them gain experience and expertise for their personal intellect
3. **Because it helps them** **implement the information security controls within the organization**
4. Because it helps them automate procedures easily and work faster

*When employees are involved in the process of drafting, reviewing, and validating the information security procedures and policies, they are more likely to contribute to the implementation of information security controls within the organization.*

1. **ISO/IEC 27001 provides a specific documentation method to be used for designing and describing controls?**
2. True
3. **False**

*ISO/IEC 27001 does not explicitly suggest any documentation method. Organizations are free to use any method they deem suitable to them.*

**Quiz 16: Implementation of controls**

1. **Why should organizations review the information security policies after the occurrence of significant changes?**
2. **To ensure continuing suitability, adequacy, and effectiveness of the information security policy**
3. To ensure continuing reliability of the information security policy
4. To ensure continuing efficiency, performance, and correctness of the information security policy

*Based on ISO/IEC 27001, control 5.1 the policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.*

1. **Which is the main purpose of control 6.1 *Screening* of ISO/IEC 27001?**
2. **To ensure that all personnel are eligible and suitable for their roles**
3. To ensure that employees and contractors are aware of and fulfil their information security responsibilities
4. To protect the organization’s interests as part of the process of any changes in employment

*The purpose of control 6.1, as defined by ISO/IEC 27002, is to ensure all personnel are eligible and suitable for the roles for which they are considered.*

1. **Who shall have access to documented operating procedures?**
2. Only the top management
3. The person responsible for operating procedures
4. **Any user that needs them**

*Based on ISO/IEC 27001, control 5.37, operating procedures for information processing facilities shall be documented and made available personnel who need them.*

1. **What is the main requirement of control 8.34 *Protection of information systems during audit testing* of ISO/IEC 27001?**
2. The tester and appropriate management shall appropriately manage test information
3. **The tester and appropriate management shall plan and agree audit tests and other assurance activities involving assessment of operational systems**
4. The tester shall separate and secure the development, testing, and production environments

*According to ISO/IEC 27001, control 8.34, audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.*

1. **What is the purpose of control 5.7 *Threat intelligence* of ISO/IEC 27001?**
2. **To provide awareness of the organization’s threat environment**
3. To ensure appropriate flow of information takes place with respect to information security
4. To ensure authorized access to information and other associated assets

*The purpose of control 5.7, is to provide awareness of the organization’s threat environment so that the appropriate mitigation actions can be taken.*

**Quiz 17: Trends and technologies**

1. **Which of the options below is NOT part of the three V’s of big data?**
2. Volume
3. Velocity
4. **Voltage**

*The three V’s of big data include volume of data, variety, and velocity.*

1. **Structured data are based on binary data and do not have a data model.**
2. True
3. **False**

*Structured data have a defined data model and are based on relational databases.*

1. **Which of the following is an example of unstructured data?**
2. **MongoDB**
3. SQL (Structured Query Language)
4. Microsoft Excel files

*SQL databases and Microsoft Excel files have structured tables, rows, and columns. MongoDB is based on binary data.*

1. **Which of the following is a benefit of weak artificial intelligence?**
2. **Automated tasks**
3. Problem-solving
4. Critical thinking improvement

*Weak artificial intelligence is focused only on a specific task and outperforms humans when conducting technical and automated tasks.*

1. **Linear regression and logistic regression are algorithms utilized by:**
2. **Machine learning**
3. Outsources operations
4. Cloud computing

*The algorithms mentioned above are machine learning algorithms based on supervised learning.*

1. **Which cloud computing service ensures an efficient management of the application life cycle?**
2. Infrastructure as a service (IaaS)
3. **Platform as a service (PaaS)**
4. Software as a service (SaaS)

*One of the main advantages of PaaS is the efficient management of the application life cycle.*

1. **Which of the statements below regarding cloud computing is NOT true?**
2. Cloud computing reduces the costs needed to manage and maintain the network system
3. Cloud computing promotes security of information because data can be accessed no matter what happens to the machine
4. **Cloud computing requires too many tasks, such as software patching, hardware setup, and “racking and stacking”**

*One of the main benefits of cloud computing is that it improves productivity, meaning it removes the need for too many tasks.*

1. **Which services are delivered by the cloud provider when using Infrastructure as a Service (IaaS)?**
2. **Virtualization, servers, storage, network**
3. Virtualization, servers, application, data, network
4. Application, data, runtime, middleware, operating system

*When using the IaaS, the services you manage are application, data, runtime, middleware, and operating system, while services mentioned in option A are delivered as a service by the cloud provider.*

1. **New technologies do not require the use of more secure authentication methods since passwords are good enough to guarantee information security.**
2. True
3. **False**

*In the digital world, passwords are considered as poor security tools; organizations need to implement more secure authentication methods.*

1. **Which of the statements below is correct?**
2. Machine learning is synonymous to artificial intelligence and the terms can be used interchangeably
3. Machine learning includes the delivery of hosted services over the internet
4. **There are two types of machine learning: supervised machine learning and unsupervised machine learning**

*Machine learning is related to artificial intelligence but they are not interchangeable and the delivery of hosted services over the internet is included in cloud computing.*

**Quiz 18: Communication**

1. **What information aspect can transparency compromise in an efficient communication strategy, if not done properly?**
2. Ambiguity
3. **Confidentiality**
4. Accuracy

*An organization should take into account the confidentiality of information when communicating the processes, procedures, methods, and assumptions to all interested parties.*

1. **What do communication objectives reflect?**
2. **The information security objectives**
3. The organizational structure objectives
4. The ISMS scope objectives

*Communication is crucial in achieving the ISMS objectives. Hence, the communication objectives should be based on the information security objectives.*

1. **The information security communication approach is impacted by whether it wants to consult, understand, inform, or involve target groups.**
2. **True**
3. False

*Information security communication approach is influenced by its objective and involved target groups, including the use of appropriate language, visual images and electronic media, and behavioral aspects of the target groups.*

1. **Why should an organization provide a communication program?**
2. To integrate the ISMS into existing processes
3. To obtain management support for the ISMS
4. **To inform all interested parties about the ISMS and the changes that may affect them**

*An organization should provide relevant information to the interested parties about the ISMS and the changes that may affect them in order to enable them to participate fully in the ISMS implementation.*

1. **Which of the following is NOT an information security communication objective?**
2. Improving the credibility and reputation of the organization
3. **Enhancing information** **security risks**
4. Influencing public policy on information security issues

*Enhancing information security risks is neither an information security objective nor an information security communication objective; it is their exact opposite.*

**Quiz 19: Competence and awareness**

1. **How can an organization ensure employee competence for the proper functioning of the ISMS?**
2. **Through appropriate education, training, or experience**
3. Through understanding the information security policy
4. Through personal behavior

*Documented evidence of competence, including education, training, and experience helps organizations ensure that employees have the necessary competence to be directly or indirectly involved in the implementation of the ISMS.*

1. **What is the main objective of an ISMS training program?**
2. To inform the interested parties about information security
3. To promote the importance of information security within an organization
4. **To enable individuals to acquire general and specific skills related to the implementation of an ISMS.**

*An ISMS training program aims to help an individual acquire the knowledge, skills, and behavior required to meet specific requirements with regard to information security.*

1. **How can competence gap be identified?**
2. Based on statutory and regulatory requirements
3. **By comparing current and required competence levels**
4. Based on the training and awareness programs output

*An organization should review its current competence levels against the required levels to determine the competence gap.*

1. **Which of the options below should be included in an awareness program?**
2. The implementation of antivirus software
3. Documented information required by the ISMS
4. **The use of passwords**

*An awareness program should address the use of passwords, among others. The other two options are useful but do not raise awareness.*

1. **An employee has received an email with a link that, when clicked, redirects to a malicious website. The IT manager identifies the issue and immediately blocks the email forward system. What action should the organization take to prevent similar situations from recurring?**
2. **Conduct an awareness program to address social engineering and risks associated with emails**
3. Conduct a training program to inform the employees about the risks associated with phishing and spams
4. Conduct an awareness program to address problems related to access control

*An awareness program addressing social engineering and risks associated with emails, including spam and phishing, helps the organization prevent such situations from recurring.*

**Quiz 20: Security operations management (Part 1)**

1. **What does the measurement of change results include?**
2. **Generating the change metrics**
3. Verifying the change success
4. Approving or rejecting the change

*This phase involves performing a post-implementation review, conducting an audit, generating the change metrics, and distributing the reports.*

1. **Which of the statements below is NOT true?**
2. Organizations cannot get certified against ISO/IEC 27032
3. Organizations cannot get certified against ISO/IEC 27035-2
4. **Organizations can get certified against ISO/IEC 27035-1**

*Organizations cannot get certified against ISO/IEC 27035-1 or ISO/IEC 27035-2.*

1. **Which standard provides guidelines for security practices in the Cyberspace?**
2. **ISO/IEC 27032**
3. ISO/IEC 27035-1
4. ISO/IEC 27035-2

*ISO/IEC 27035-1 and ISO/IEC 27035-2 present basic concepts for information security incidents, while ISO/IEC 27032 provides guidelines for security practices for stakeholders in the Cyberspace.*

1. **What is a Security Operations Center (SOC) team?**
2. A group of information security program coordinators
3. **A group of expert individuals, security analysts, engineers, and managers who supervise security operations**
4. A group of internal auditors who uninterruptedly manage operational activities of the organization

*The Security Operations Center team is a group of expert individuals, security analysts, engineers, and managers who supervise security operations. This team works closely with other teams and departments of the organization to ensure that security issues are addressed prior to discovery.*

1. **The top management must ensure that all members within the ISMS scope understand the value and importance of an effective information security incident management policy.**
2. **True**
3. False

*This is important because it ensures that everyone involved in the ISMS will work in line with the management system’s requirements.*

**Quiz 21: Security operations management (Part 2)**

1. **Upon receiving an event report, the operations support group should complete the information security event ticket, analyze it (triage), and assign a priority. What process is this?**
2. **Initial assessment and decision**
3. Detection and reporting
4. Response

*After the initial receipt of the event, an evaluation should be conducted to determine if the event report needs further analysis. Essentially, the evaluation is conducted to determine the validity of the event being an incident.*

1. **A team where the responsibility for dealing with incidents is typically assigned to a specifically qualified group of individuals is known as:**
2. Security team
3. **Internal computer security incident response team (Internal CSIRT)**
4. Management team

*The responsibility for dealing with incidents is typically assigned to a qualified group of individuals, such as an internal computer security incident response team.*

1. **What type of control is cryptography?**
2. **Preventive control**
3. Detective control
4. Corrective control

*Cryptography uses encryption to protect data from disclosure to unauthorized parties, and as such is a preventive control.*

1. **What are the steps of a forensic analysis?**
2. Prepare, review, and analyze
3. Prepare, collect, archive, and report
4. **Prepare, collect and archive, review and analyze, and report**

*There are four main steps in a forensic analysis: preparation (investigators must have the skills necessary for this type of survey), collection and archiving of data (in accordance with the required procedures), review and analysis (interpretation of information for research purposes), and report (including conclusions and comments).*

1. **The performance of the incident management process should be regularly \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**
2. Measured using imperial units
3. Evaluated to identify corrective actions
4. **Re-evaluated to identify corrective and preventive actions**

*The incident management should be regularly re-evaluated to identify corrective and preventive actions and measured using performance indicators.*

1. **Disaster recovery (DR) defines the dangers that threaten an organization and protects the interests of various interested parties.**
2. True
3. **False**

*Disaster recovery (DR) involves stopping the disaster’s effects as quickly as possible and immediately addressing its consequences. The dangers that threaten an organization and interest protection are subject to business continuity (BC).*

**Scenario-based quiz 3: Sections 14-20**

*Pharm* is a pharmaceutical company that develops and distributes medication products. This company has been victim to several information security attacks in the last month due to the high amount of important data they had to collect for their development researches.

They, therefore, decided to restrict user access to information and application system functions only to specific persons by designing specific access controls. *Pharm* decided that all types of information, regardless of their importance or impact, will get the same level of protection so that the number of attacks can be reduced. A team of five competent persons was established to evaluate the information security attacks and confirm their nature, the way they are done, what or who they might affect, and what their potential impact in the company can be. They concluded that the attackers gained access to their systems through social engineering attacks.

After completing the implementation of the new security controls and ensuring their successful operation, *Pharm* decided to provide a communication plan for the users and concluded that an awareness session for the staff was not necessary.

Based on the above-mentioned scenario, answer the following questions:

1. **What controls should *Pharm* implement to preserve the integrity and confidentiality of information?**
2. Event logging controls
3. **Cryptographic controls**
4. Secure areas controls

*Cryptographic controls aim at protecting the confidentiality, authenticity, and integrity of Pharm’s information.*

1. ***Pharm* provided the same level of protection for all information, regardless of importance or impact, to reduce the number of attacks. Does this comply with ISO/IEC 27001?**
2. Yes, because the same level of protection for all types of information is required by the standard
3. **No, because information should be protected according to its importance**
4. No, because information protection cannot reduce the number of attacks

*ISO/IEC 27001 requires from organizations to determine their information’s level of protection in accordance with its importance to the organization.*

1. **What type of security control did *Pharm* implement by establishing a team to evaluate the information security attacks?**
2. Preventive control
3. Detective control
4. **Corrective control**

*This team was established to solve the identified problems and prevent their recurrence; hence corrective.*

1. **The team of five competent persons established by *Pharm* is an:**
   1. Implementation security team
   2. Internal management team
   3. **Incident response team**

*The aim of an incident response team is to confirm the nature of the information security incident by determining how it was done, what or who it might affect, and what its impact can be.*

1. **Based on the scenario, *Pharm* will provide a communication plan after concluding that an awareness session for the staff is not necessary. How do you consider this situation?**
2. Acceptable; the communication plan regarding the implementation of the new security controls provided to the users is sufficient
3. **Unacceptable; *Pharm* should conduct awareness sessions to raise awareness regarding information security threats such as social engineering**
4. Unacceptable; the communication plan should not be provided to the users

*The organization should establish awareness programs to ensure the staff understands information security threats and how to protect from potential risks. The main areas that should be addressed by an awareness program, among others, include risks associated with emails and social engineering.*

**Quiz 22: Monitoring, measurement, analysis, and evaluation**

1. **Monitoring, measurement, analysis, and evaluation should define ‘information needs,’ which are usually expressed as a high-level information security question or statement that helps the organization evaluate information security performance and ISMS effectiveness.**
2. **True**
3. False

*In other words, monitoring and measurement are conducted for the purpose of fulfilling an information need. The attributes to be measured should be determined carefully. It is impracticable, costly, and counterproductive to measure a large number of irrelevant attributes.*

1. **What is performance evaluation?**
2. Process of determining the status of a system, process, or activity
3. **Process of determining measurable results**
4. Process of determining a value

*Performance evaluation can be defined as a systematic way of assessing an organization’s current achievements against its objectives. Performance evaluation measures are of little value per se, unless they are viewed within the context of organizational strategies and objectives.*

1. **ISO/IEC 27004 provides guidelines to help organizations in evaluating the ISMS performance in order to satisfy the requirements of ISO/IEC 27001.**
2. **True**
3. False

*The ISO/IEC 27004 standard exclusively addresses clause 9.1 Monitoring, measurement, analysis and evaluation of ISO/IEC 27001.*

1. **What does “SMART” stand for?**
2. Sophisticated, Measurable, Adversary, Realistic, and Timely
3. **Specific, Measurable, Attainable, Realistic, and Timely**
4. Specialized, Maintainable, Attainable, Realistic, and Timely

*SMART stands for:* ***specific:*** *clear and focused to avoid misconception;* ***measurable:*** *quantified and comparable to other data; a****ttainable:*** *achievable, reasonable, and acceptable in a particular context;* ***realistic:*** *fits into the organization’s culture and is cost-effective;* ***timely:*** *achievable within the set time frame.*

1. **According to ISO/IEC 27004, which of the options below is not included in ISMS processes and activities that are candidates for measurement?**
2. **Financing and business management**
3. Communicating and documenting
4. Planning and leadership

*Financing and business management are not included in ISO/IEC 27004.*

1. **What is the aim of monitoring, measurement, analysis, and evaluation in an ISMS?**
2. To begin the ISMS implementation
3. **To improve the ISMS implementation**
4. To prohibit the ISMS implementation

*The organization should evaluate its management system in order to ensure its continual suitability, adequacy, and effectiveness. This is why it is recommended to focus on monitoring and measurement activities that are linked to critical processes that enable the organization to achieve the information security performance objectives.*

**Quiz 23: Internal audit**

1. **What is an audit?**
2. **A systematic, independent, and documented process**
3. A symmetric and objective documents
4. A subjective opinion on the state

*According to ISO 19011, an audit is defined as a systematic, independent, and documented process for obtaining objective evidence to determine the extent to which the audit criteria are fulfilled.*

1. **What audit type determines whether the organization’s accounting practices are compliant with legal requirements?**
2. **A financial audit**
3. An administrative audit
4. An information security audit

*A financial audit determines the compliance of an organization’s accounting practices with legal requirements and recognized principles. An administrative audit determines the effectiveness of the overall administrative practices. An information security audit determines the appropriate protection of information assets.*

1. **Internal audits include audits known as second and third party audits.**
2. True
3. **False**

*Second and third party audits are external audits. Second party audits are conducted by parties that have an interest in the audited organization. Third party audits are conducted by external and independent audit organizations. Internal audits, on the other hands, are known as first party audits.*

1. **Which of the following is NOT a characteristic of internal audits?**
2. **They provide general recommendations and not an advisory role within the organization**
3. They consider the effectiveness and efficiency of the ISMS
4. They are independent of the activities audited (not of the organization)

*An internal audit plays an advisory role for the improvement of the ISMS within the organization, while an external audit provides only general recommendations by avoiding the advisory role.*

1. **Auditors should possess knowledge and skills in audit principles, processes, and methods.**
2. **True**
3. False

*Knowledge and skills in these areas enable the auditor to ensure audits are performed consistently and systematically.*

1. **A nonconformity report should NOT be \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**
2. **Ambiguous**
3. Explicit
4. Correct

*A nonconformity report should be explicit, related to an ISMS requirement, unambiguous, linguistically correct, and as concise as possible.*

1. **How many types of nonconformities are there?**
2. One: Minor nonconformities
3. One: Major nonconformities
4. **Two: Minor and major nonconformities**

*According to ISO 9000, a nonconformity is defined as the “non-fulfillment of a requirement.” There are two types of nonconformities, namely minor and major.*

1. **An auditor must always remember that it is highly unlikely that the organization is able to complete all the improvements simultaneously.**
2. **True**
3. False

*Every improvement requires time and resources. Action plans can be arranged in order of priority by the top management. Therefore, the auditor must try to ensure that improvement objectives are realistic in the specific context of the auditee.*

**Quiz 24: Management review**

1. **What is accomplished when the implemented management system fulfills the organization’s needs?**
2. Suitability
3. Adequacy
4. **Effectiveness**

*Effectiveness is the extent to which a management system may be expected to achieve its objectives and fulfill the organization’s need.*

1. **An organization wishing to comply with ISO/IEC 27001 should at least perform regular management reviews at scheduled intervals and maintain records.**
2. **True**
3. False

*According to clause 9.3.1 of ISO/IEC 27001, the organization should review the ISMS at planned intervals and retain documented information as evidence of the results of management reviews.*

1. **Who is responsible for ensuring that follow-up action plans are approved by the top management?**
2. **The ISMS coordinator and the internal audit team**
3. The top management
4. The information security manager

*The ISMS coordinator and the internal audit team have the responsibility of ensuring that follow-up action plans are approved by the top management.*

1. **What should be included in the management review output?**
2. Decisions related to risk opportunities
3. **Decisions related to continual improvement opportunities**
4. Decisions related to outsourcing opportunities

*Based on ISO/IEC 27001, clause 9.3.3, the outputs of the management review should include decisions related to continual improvement opportunities and any needs for changes to the information security management system.*

1. **Since there is no specific requirement regarding the frequency of management review meetings, annual meetings are enough to prevent or resolve issues**.
2. True
3. **False**

*The common practice for management review meetings is quarterly meetings.*

**Quiz 25: Treatment of nonconformities**

1. **An action taken to eliminate the cause of a potential nonconformity or other potential undesirable situation is known as:**
2. Correction
3. Corrective action
4. **Preventive action**

*Preventive actions are actions taken to eliminate the cause of a potential nonconformity or other potential undesirable situation.*

1. **What does the root-cause analysis involve?**
2. **Determining the source of the nonconformity**
3. Defining and analyzing the impacts of the nonconformity
4. Selecting the solutions

*The root-cause analysis involves determining the source of the nonconformity and analyzing its root causes.*

1. **An organization has integrated the identification of interruptions for business continuity in their annual ISMS risk assessment. How would you assess the situation?**
2. **Conformity**
3. Major nonconformity
4. Minor nonconformity

*The organization complies with the requirements of ISO/IEC 27001.*

1. **All nonconformities should be included in a single inclusive action plan.**
2. True
3. **False**

*Every nonconformity requires its own action plan.*

1. **The auditee has not submitted the action plans within the specified deadline. What follows?**
2. The certification body will be involved
3. The auditor will issue a minor nonconformity
4. **The organization will not be recommended for certification**

*If the action plans are not submitted within the specified deadline, the organization will not be recommended for certification.*

1. **What are the activities that should be included in the situation analysis phase of the corrective action process?**
2. Identification and documentation of the nonconformities
3. Follow- up on and review of corrective actions
4. **Evaluation of options and selection of solutions**

*Situation analysis phase of the corrective action process comprises of three activities: analysis of the root cause, evaluation of options, and selection of solutions.*

**Quiz 26: Continual improvement**

1. **Which of the following is an activity taken toward continual improvement?**
2. Determining measurement objectives
3. Establishing the ISMS performance indicators
4. **Establishing the change factors to be monitored**

*Processes and procedures may undergo several changes because of shifting business needs, technology upgrades, or new internal or external policies. By establishing the change factors to monitor, the organization ensures the continual improvement of its ISMS.*

1. **The continual \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ensures continual improvement.**
2. Changes in laws and regulations
3. Alterations in the business scope
4. **Update of documented information**

*Continual update of documented information provides a properly functioning management system. Hence, it ensures continual improvement.*

1. **What should be reviewed and updated on a continual basis?**
2. The information security incidents
3. **The information security policy**
4. The information security failures

*All the documented information relating to the ISMS, including the information security policy, should be continually updated and reviewed.*

1. **What is the correlation between continual improvement and information security errors?**
2. **Continual improvement helps reduce the number of errors**
3. Continual improvement helps increase the number of errors
4. Continual improvement introduces new errors

*The continual improvement process helps reduce the number of errors.*

1. **An action taken to eliminate the causes of a nonconformity helps in the creation of a continual improvement culture.**
2. True
3. **False**

*A corrective action aims to correct; it does not promote continual improvement in an organization, nor does it foster such culture.*

**Quiz 27: Preparing for the certification audit**

1. **Which step should be completed before the certification audit?**
2. **Selecting a certification body**
3. Preparing for audit follow-up
4. Conducting on-site audit activities

*Before the audit, the organization should select a certification body.*

1. **Which of these scenarios is a valid reason for rejecting an auditor?**
2. The auditor is not familiar with the local customs of the area the organization operates in
3. The auditor has issued an unfavorable certification recommendation
4. **The auditor has worked for one of the organization’s competitors**

*The auditee can reject an auditor only for valid reasons, such as if the auditor has worked for one of the organization’s competitors; the first two options are not valid reasons.*

1. **What is the main activity of stage 1 audit?**
2. Verifying the efficiency of the management system
3. **Reviewing the documented information**
4. Evaluating compliance with the requirements of the standard

*The review of documented information is the main activity of stage 1 audit. The other two alternatives are stage 2 audit activities.*

1. **The auditor issues the final certification decision upon concluding the audit.**
2. True
3. **False**

*Upon concluding the audit, the auditor issues a certification recommendation. The final certification decision is made by the certification committee of the certification body.*

1. **What is the main objective of the audit follow-up?**
2. To validate the operational control of the auditee processes
3. To verify the “design” of the management system
4. **To validate the action plans and corrective actions implemented by the auditee**

*The audit follow-up is usually initiated after a major nonconformity, before the organization is recommended for certification. Hence, its main objective is to validate the effectiveness of action plans and corrective actions.*

**Scenario-based quiz 4: Sections 21-27**

*Markt* is a recruiting corporate that works towards finding suitable employees for various positions that companies need. Upon the successful implementation of the ISMS, *Markt* has decided to hire Lisa as an internal auditor to determine the extent to which their audit criteria are fulfilled. Lisa has over 15 years of IT experience but little to no experience in auditing. The internal audit results, the treatment of nonconformities, and the corrective actions were to be discussed during the annual management review meeting.

The meeting showed that Lisa had missed out on several easily identifiable nonconformities. The audit documented information presented sufficient evidence that no logs were preserved for user access control other than the ones in the active directory. The program functions of maintaining records were either non-configured or not enabled due to the lack of storage capacity. Lisa did not include this in the internal audit report.

Answer the following questions by referring to the above-mentioned scenario:

1. **Despite her accomplishments on the IT sector, should *Markt* have hired Lisa as an internal auditor, even though she had no audit experience?**
   1. Yes, she is an IT experienced individual that would quickly learn the process
   2. **No, because she lacks the skills and experience to perform an internal audit**
   3. Yes, because even if a minor issue would arise, it would be quickly recuperated after the annual meeting

*Every hired internal auditor should have the necessary knowledge and skills to confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions.*

1. **In the context of *Markt*, is it sufficient that management review meetings are held on an annual basis?**
   1. Yes, annual management reviews enable the company to review the effectiveness of the ISMS
   2. **No, annual management reviews are not enough for the company to resolve issues in a timely manner**
   3. No, annual management reviews do not contribute to the continual improvement of the ISMS

*There is no specific requirement for the frequency of management review meetings. Yet, through annual management reviews, the organization may not be able to prevent or resolve issues in a timely manner. The recommended practice is quarterly meetings.*

1. **What action could *Markt* have taken to detect the issues with the access control logs before the occurrence of a potential risk?**
   1. Focus on recruiting more trained internal auditors
   2. **Establish a continual risk management process**
   3. Prioritize investment on detective controls rather than other controls

*By establishing a continual risk management process, Markt is more likely to detect a change in the risk factors that concern the company, because risks are not static.*

1. **What is the root cause of the nonconformity with regard to the access control logs?**
   1. Lack of security measures for protecting the stored data logs
   2. Lack of logs preserved for user access control on the active directory
   3. **Lack of storage capacity and mechanisms for keeping records**

*Some of the root causes of the nonconformity are the lack of storage capacity for storing data in Markt, the lack of mechanisms on other systems for keeping records, and the lack of the organization’s awareness on the importance of keeping access control records.*

1. **Which of the following corrective actions is the most suitable to treat the access control logs nonconformity?**
   1. Outsource the audit findings to an expert
   2. Have the organization hire a trained person with hands-on experience to train Lisa on the spot
   3. **Analyze the information systems to identify records that have to be maintained and generate a records retention schedule**

*All the user access controls need to be kept on record as audit evidence. Additionally, all the functions for maintaining records should be enabled and configured.*