NO.1 Integrity of data means

A. Accuracy and completeness of the data

B. Data should be viewable at all times

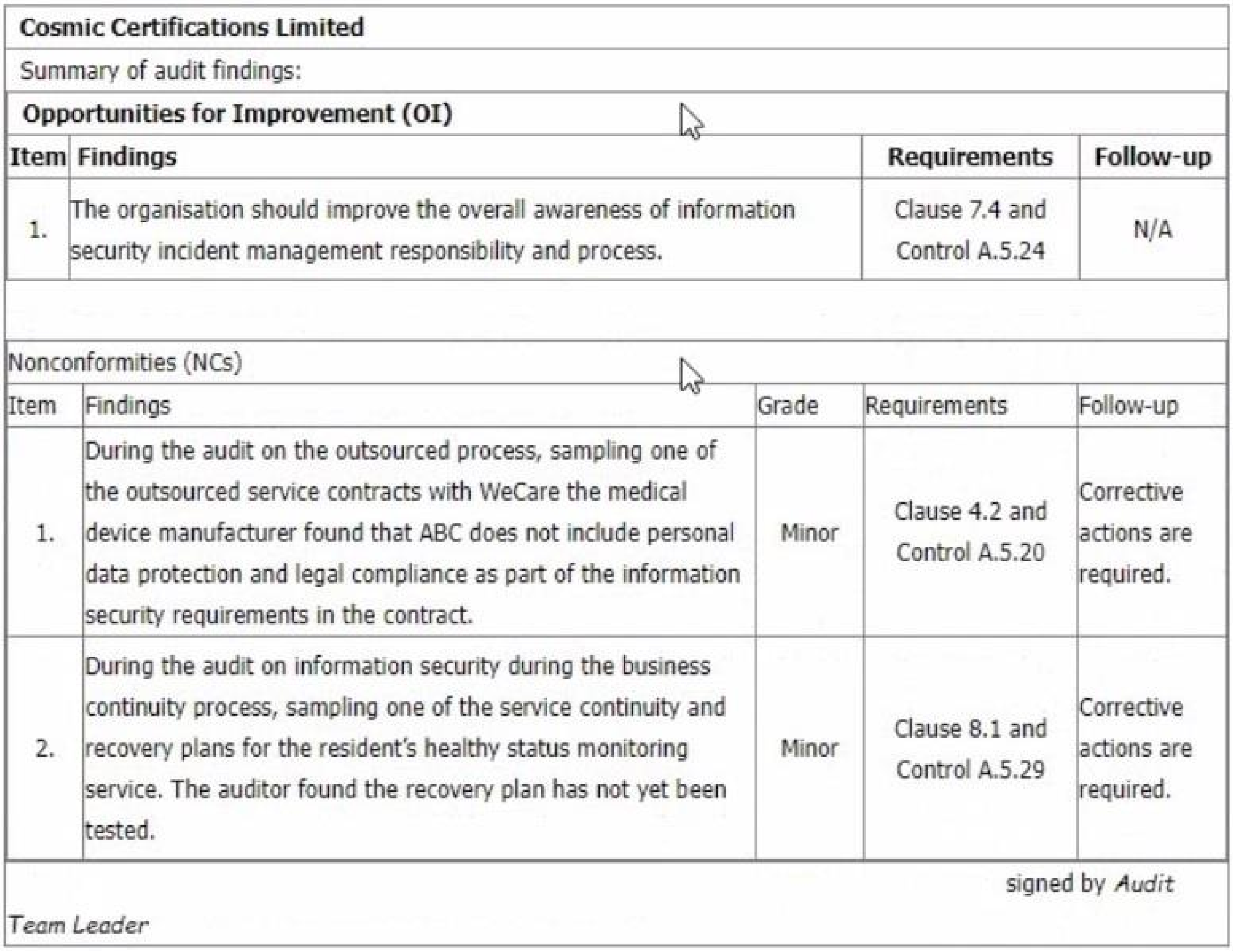
C. Data should be accessed by only the right people

Answer: A

Explanation:

Integrity of data means accuracy and completeness of the data. Integrity is one of the three main objectives of information security, along with confidentiality and availability. Integrity ensures that information and systems are not corrupted, modified, or deleted by unauthorized actions or events. Data should be viewable at all times is not related to integrity, but to availability. Data should be accessed by only the right people is not related to integrity, but to confidentiality. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : [ISO/IEC 27001 Brochures | PECB], page 4.

NO.2 You are performing an ISMS initial certification audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to conduct the closing meeting. During the final audit team meeting, as an audit team leader, you agree to report 2 minor nonconformities and 1 opportunity for improvement as below:



Cosmic Certifications Limited

Summary of audit findings:

Opportunities for Improvement (OI)

Item	**Findings**	**Requirements**	**Follow-up**
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.	Clause 7.4 and Control A.5.24	N/A

Nonconformities (NCs)

Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.

signed by *Audit Team Leader*

Select one option of the recommendation to the audit programme manager you are going to advise to the auditee at the closing meeting.

A. Recommend certification immediately

B. Recommend that a full scope re-audit is required within 6 months

C. Recommend that an unannounced audit is carried out at a future date

D. Recommend certification after your approval of the proposed corrective action plan Recommend that the findings can be closed out at a surveillance audit in 1 year

E. Recommend that a partial audit is required within 3 months

Answer: D

Explanation:

According to ISO/IEC 17021-1:2015, which specifies the requirements for bodies providing audit and certification of management systems, clause 9.4.9 requires the certification body to make a certification decision based on the information obtained during the audit and any other relevant information1. The certification body should also consider the effectiveness of the corrective actions taken by the auditee to address any nonconformities identified during the audit1. Therefore, when making a recommendation to the audit programme manager, an ISMS auditor should consider the nature and severity of the nonconformities and the proposed corrective actions.

Based on the scenario above, the auditor should recommend certification after their approval of the proposed corrective action plan and recommend that the findings can be closed out at a surveillance audit in 1 year. The auditor should provide the following justification for their recommendation:

Justification: This recommendation is appropriate because it reflects the fact that the auditee has only two minor nonconformities and one opportunity for improvement, which do not indicate a significant or systemic failure of their ISMS. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. An opportunity for improvement is defined as a suggestion for improvement beyond what is required by ISO/IEC 27001:20222. Therefore, these findings do not prevent or preclude certification, as long as they are addressed by appropriate corrective actions within a reasonable time frame. The auditor should approve the proposed corrective action plan before recommending certification, to ensure that it is realistic, achievable, and effective. The auditor should also recommend that the findings can be closed out at a surveillance audit in 1 year, to verify that the corrective actions have been implemented and are working as intended.

The other options are not valid recommendations for the audit programme manager, as they are either too lenient or too strict for the given scenario. For example:

Recommend certification immediately: This option is not valid because it implies that the auditor ignores or accepts the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182, which provides guidelines for auditing management systems. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to consider the effectiveness of the corrective actions taken by the auditee before making a certification decision.

Recommend that a full scope re-audit is required within 6 months: This option is not valid because it implies that the auditor overreacts or exaggerates the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a re-audit is necessary based on the nature and extent of nonconformities and other relevant factors. A full scope re-audit is usually reserved for major nonconformities or multiple minor nonconformities that indicate a serious or widespread failure of an ISMS.

Recommend that an unannounced audit is carried out at a future date: This option is not valid because it implies that the auditor distrusts or doubts the auditee's commitment or capability to implement corrective actions, which is contrary to the audit principles and objectives of ISO

19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to conduct unannounced audits only under certain conditions, such as when there are indications of serious problems with an ISMS or when required by sector-specific schemes.
Recommend that a partial audit is required within 3 months: This option is not valid because it implies that the auditor imposes or prescribes a specific time frame or scope for verifying corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a partial audit is necessary based on the nature and extent of nonconformities and other relevant factors. A partial audit may be appropriate for minor nonconformities, but the time frame and scope should be agreed upon with the auditee and based on the proposed corrective action plan.

NO.3 What controls can you do to protect sensitive data in your computer when you go out for lunch?

A. You activate your favorite screen-saver

B. You are confident to leave your computer screen as is since a password protected screensaver is installed and it is set to activate after 10 minutes of inactivity

C. You lock your computer by pressing Windows+L or CTRL-ALT-DELETE and then click "Lock Computer".

D. You turn off the monitor

Answer: C

Explanation:
You should lock your computer by pressing Windows+L or CTRL-ALT-DELETE and then click "Lock Computer", because this is the most effective way to protect sensitive data in your computer when you go out for lunch. By locking your computer, you are preventing unauthorized access to your computer and its contents, as well as complying with the organization's access control policy and information security policy. Locking your computer requires a password or a biometric authentication to unlock it, which adds a layer of security to your data. The other options are not sufficient or reliable, as they do not prevent someone from accessing your computer or viewing your screen.
Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], ISO/IEC 27001:2022 Information technology - Security techniques - Information security management system s - Requirements, How to lock your PC

NO.4 Which two activities align with the "Check" stage of the Plan-Do-Check-Act cycle when applied to the process of managing an internal audit program as described in ISO 19011?

A. Retains records of internal audits

B. Define audit criteria and scope for each internal audit

C. Update the internal audit programme

D. Establish a risk-based internal audit programme

E. Conduct internal audits

F. Verify effectiveness of the internal audit programme

G. Review trends in internal audit result

Answer: F,G

Explanation:
The Check stage of the PDCA cycle involves monitoring and measuring the performance of the

process and comparing it with the planned objectives and criteria. In the context of managing an internal audit programme, this stage includes verifying the effectiveness of the internal audit programme by evaluating whether it meets its objectives, scope, and criteria, and whether it is implemented in accordance with ISO 19011 guidelines1. It also includes reviewing the trends in internal audit results by analyzing the data collected from the audits, such as audit findings, nonconformities, corrective actions, opportunities for improvement, and customer feedback1.
Reference: ISO 19011:2018 - Guidelines for auditing management systems

NO.5 An administration office is going to determine the dangers to which it is exposed.
What do we call a possible event that can have a disruptive effect on the reliability of information?

A. dependency

B. threat

C. vulnerability

D. risk

Answer: B

Explanation:
A possible event that can have a disruptive effect on the reliability of information is a threat. A threat is anything that has the potential to harm an asset or its protection, such as a natural disaster, a human error, a malicious attack, etc. A threat can exploit a vulnerability or weakness in an asset or its protection and cause an adverse impact on the confidentiality, integrity or availability of information. ISO/IEC 27001:2022 defines threat as "potential cause of an unwanted incident, which can result in harm to a system or organization" (see clause 3.48). Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Threat?

NO.6 How are data and information related?

A. Data is a collection of structured and unstructured information

B. Information consists of facts and statistics collected together for reference or analysis

C. When meaning and value are assigned to data, it becomes information

Answer: C

Explanation:
Data and information are related concepts, but they are not the same. Data are simply facts or figures that represent raw facts or figures and form the basis of information. Information is data that has been given value through analysis, interpretation, or compilation in a meaningful form. When meaning and value are assigned to data, it becomes information that can be used for decision making, problem solving, or communication. Therefore, the correct answer is C. Reference: ISO/IEC 27000:2022, clause 3.7; Data vs Information - Difference and Comparison | Diffen.

NO.7 You are performing an ISMS audit at a nursing home where residents always wear an electronic wristband for monitoring their location, heartbeat, and blood pressure. The wristband automatically uploads this data to a cloud server for healthcare monitoring and analysis by staff.
You now wish to verify that the information security policy and objectives have been established by top management. You are sampling the mobile device policy and identify a security objective of this policy is "to ensure the security of teleworking and use of mobile devices" The policy states the following controls will be applied in order to achieve this.

Personal mobile devices are prohibited from connecting to the nursing home network, processing, and storing residents' data.
The company's mobile devices within the ISMS scope shall be registered in the asset register.
The company's mobile devices shall implement or enable physical protection, i.e., pin-code protected screen lock/unlock, facial or fingerprint to unlock the device.
The company's mobile devices shall have a regular backup.
To verify that the mobile device policy and objectives are implemented and effective, select three options for your audit trail.

A. Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home

B. Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home

C. Review the internal audit report to make sure the IT department has been audited

D. Review the asset register to make sure all personal mobile devices are registered

E. Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register

F. Review the asset register to make sure all company's mobile devices are registered

G. Interview the supplier of the devices to make sure they are aware of the ISMS policy

H. Interview top management to verify their involvement in establishing the information security policy and the information security objectives

Answer: C,E,F

Explanation:
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 5.2 requires top management to establish an information security policy that provides the framework for setting information security objectives1. Clause 6.2 requires top management to ensure that the information security objectives are established at relevant functions and levels1. Therefore, when verifying that the information security policy and objectives have been established by top management, an ISMS auditor should review relevant documents and records that demonstrate top management's involvement and commitment.
To verify that the mobile device policy and objectives are implemented and effective, an ISMS auditor should review relevant documents and records that demonstrate how the policy and objectives are communicated, monitored, measured, analyzed, and evaluated. The auditor should also sample and verify the implementation of the controls that are stated in the policy.
Three options for the audit trail that are relevant to verifying the mobile device policy and objectives are:
Review the internal audit report to make sure the IT department has been audited: This option is relevant because it can provide evidence of how the IT department, which is responsible for managing the mobile devices and their security, has been evaluated for its conformity and effectiveness in implementing the mobile device policy and objectives. The internal audit report can also reveal any nonconformities, corrective actions, or opportunities for improvement related to the mobile device policy and objectives.
Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register: This option is relevant because it can provide evidence of how the mobile devices that are used by the medical staff, who are involved in processing and storing residents' data,

are registered in the asset register and have physical protection enabled. This can verify the implementation and effectiveness of two of the controls that are stated in the mobile device policy.
Review the asset register to make sure all company's mobile devices are registered: This option is relevant because it can provide evidence of how the company's mobile devices that are within the ISMS scope are identified and accounted for. This can verify the implementation and effectiveness of one of the controls that are stated in the mobile device policy.
The other options for the audit trail are not relevant to verifying the mobile device policy and objectives, as they are not related to the policy or objectives or their implementation or effectiveness. For example:
Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding physical security or access control, but not specifically to mobile devices.
Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security awareness or compliance, but not specifically to mobile devices.
Interview the supplier of the devices to make sure they are aware of the ISMS policy: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security within supplier relationships, but not specifically to mobile devices.
Interview top management to verify their involvement in establishing the information security policy and the information security objectives: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to verifying that the information security policy and objectives have been established by top management, but not specifically to mobile devices.

NO.8 What is the goal of classification of information?

A. To create a manual about how to handle mobile devices

B. Applying labels making the information easier to recognize

C. Structuring information according to its sensitivity

Answer: C

Explanation:
The goal of classification of information is to structure information according to its sensitivity and value for the organization. Classification of information helps to determine the appropriate level of protection and handling for each type of information. Applying labels making the information easier to recognize is not the goal of classification, but a method of implementing classification. Creating a manual about how to handle mobile devices is not related to classification of information, but to information security policies and procedures. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 33. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 34. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 35. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 36.

NO.9 Below is Purpose of "Integrity", which is one of the Basic Components of Information Security

A. the property that information is not made available or disclosed to unauthorized individuals

B. the property of safeguarding the accuracy and completeness of assets.

C. the property that information is not made available or disclosed to unauthorized individuals

D. the property of being accessible and usable upon demand by an authorized entity.

Answer: B

Explanation:

Integrity is one of the basic components of information security, along with confidentiality and availability. Integrity means that information is safeguarded from unauthorized or accidental changes that could affect its accuracy and completeness. Integrity ensures that information is reliable and trustworthy3. Reference: ISO/IEC 27001:2022 Lead Auditor Training Course - BSI

NO.10 Which of the following is an information security management system standard published by the International Organization for Standardization?

A. ISO9008

B. ISO27001

C. ISO5501

D. ISO22301

Answer: B

Explanation:

ISO/IEC 27001:2022 is an information security management system standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The standard is intended to be applicable to all organizations, regardless of type, size or nature. ISO/IEC 27001:2022 is part of the ISO/IEC 27000 family of standards, which provide a comprehensive framework for information security management. Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], ISO/IEC 27001:2022 Information technology - Security techniques - Information security managemen t systems - Requirements, ISO/IEC 27000 family - Information security management systems

NO.11 After a devastating office fire, all staff are moved to other branches of the company. At what moment in the incident management process is this measure effectuated?

A. Between incident and damage

B. Between detection and classification

C. Between recovery and normal operations

D. Between classification and escalation

Answer: A

Explanation:

After a devastating office fire, all staff are moved to other branches of the company. This measure is effectuated between incident and damage in the incident management process. Incident management is the process of detecting, investigating, and responding to incidents in as little time as possible. An incident is any disruption to a service or workflow. A fire is an example of an incident that can cause severe damage to the organization's assets, operations, and reputation. The incident management process consists of five steps: detection, classification, escalation, recovery, and closure2. The measure of moving staff to other branches is a form of recovery action that aims to restore normal service and minimize impact to the business. However, this measure is taken before the damage caused by the fire is fully assessed or contained. Therefore, this measure is effectuated between incident and damage in the incident management process. Reference: ISO/IEC 27000:2022, clause 3.24; Atlassian.

NO.12 A member of staff denies sending a particular message.
Which reliability aspect of information is in danger here?

A. availability

B. correctness

C. integrity

D. confidentiality

Answer: C

Explanation:
The reliability aspect of information that is in danger when a member of staff denies sending a particular message is integrity. Integrity implies that information is authentic and can be verified as such. If a member of staff denies sending a message, it means that either the message was forged or the sender is lying, both of which violate the integrity of the information. Availability, correctness and confidentiality are not directly affected by this scenario. ISO/IEC 27001:2022 defines integrity as "property of accuracy and completeness" (see clause 3.24). Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Integrity?

NO.13 Availability means

A. Service should be accessible at the required time and usable by all

B. Service should be accessible at the required time and usable only by the authorized entity

C. Service should not be accessible when required

Answer: B

Explanation:
Availability means that service should be accessible at the required time and usable only by the authorized entity. Availability is one of the three main objectives of information security, along with confidentiality and integrity. Availability ensures that information and systems are not disrupted or denied by unauthorized actions or events. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : ISO/IEC 27001 Brochures | PECB, page 4.

NO.14 What is the purpose of an Information Security policy?

A. An information security policy makes the security plan concrete by providing the necessary details

B. An information security policy provides insight into threats and the possible consequences

C. An information security policy provides direction and support to the management regarding information security

D. An information security policy documents the analysis of risks and the search for countermeasures

Answer: C

Explanation:
The purpose of an information security policy is to provide direction and support to the management regarding information security. An information security policy is a statement of intent or direction that provides guidance for decision making and actions within an organization. It defines the scope,

objectives, principles, and roles for information security management. It also establishes the general approach to information security and the expectations for compliance. An information security policy is the foundation of an information security management system (ISMS) based on ISO/IEC 27001:2022, which requires the organization to establish, implement, maintain, and continually improve an ISMS1. Therefore, the correct answer is C. Reference: ISO/IEC 27000:2022, clause 3.47; ISO/IEC 27001:2022, clause 5.2.