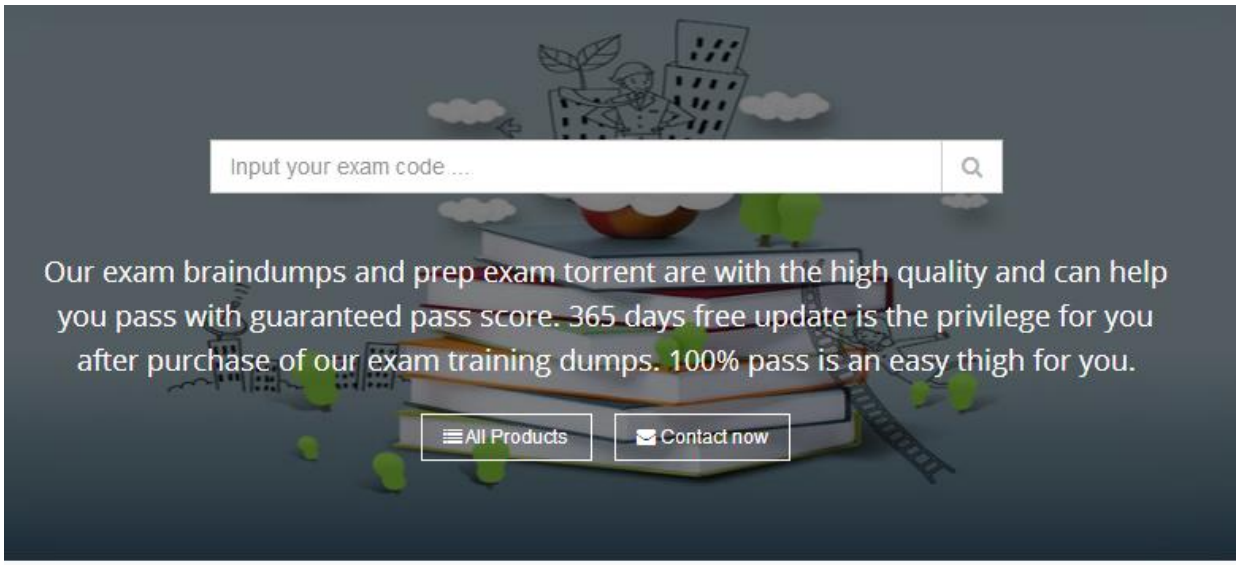
BraindumpsPrep



QUALITY AND VALUE

BraindumpsPrep Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our BraindumpsPrep testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

BraindumpsPrep offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.braindumpsprep.com

Prep your actual exam test with our valid braindumps for successful pass

Exam : **ISO-IEC-27001-Lead-Implementer-German**

Title : PECB Certified ISO/IEC 27001 Lead Implementer Exam (ISO-IEC-27001-Lead-Implementer Deutsch Version)

Vendor : PECB

Version : DEMO

QUESTION NO: 1
Szenario 10:
NetworkFuse ist ein führendes Unternehmen, das sich auf die Entwicklung, Produktion und den Vertrieb von Netzwerkhardware spezialisiert hat. In den letzten zwei Jahren verfügt NetworkFuse über ein operatives Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 und ein Qualitätsmanagementsystem (QMS) nach ISO 9001. Diese Systeme sollen das Engagement des Unternehmens für Informationssicherheit und höchste Qualitätsstandards gewährleisten.
Um sein Engagement für Best Practices und Branchenstandards weiter zu demonstrieren, hat NetworkFuse kürzlich ein kombiniertes Zertifizierungsaudit angesetzt. Ziel dieses Audits ist es, die Konformität von NetworkFuse mit ISO/IEC 27001 und ISO 9001 zu bestätigen und das starke Engagement des Unternehmens für die Einhaltung hoher Standards im Informationssicherheits- und Qualitätsmanagement zu unterstreichen. Der Prozess begann mit der sorgfältigen Auswahl einer Zertifizierungsstelle. Anschließend bereitete NetworkFuse seine Mitarbeiter auf das Audit vor, was für einen reibungslosen und erfolgreichen Auditprozess entscheidend war. Darüber hinaus beauftragte NetworkFuse Mitarbeiter mit der Verwaltung des ISMS und des QMS.
NetworkFuse verzichtete vor dem Audit auf eine Selbstevaluierung, ein häufig von Unternehmen durchgeführter Schritt, um proaktiv Verbesserungspotenziale zu identifizieren. Die Unternehmensleitung hielt eine solche Evaluierung für unnötig und vertraute auf die bestehenden Systeme und Praktiken. Diese Entscheidung spiegelte das Vertrauen in die Robustheit des ISMS und QMS wider. Im Rahmen der Vorbereitungen stellte NetworkFuse sorgfältig sicher, dass alle erforderlichen dokumentierten Informationen – einschließlich interner Auditberichte, Managementbewertungen, der technologischen Infrastruktur und der allgemeinen Funktionsweise des ISMS und QMS – für das Audit verfügbar waren. Diese Informationen waren für den Nachweis der ISO-Konformität von entscheidender Bedeutung.
Während des Audits forderte NetworkFuse die Zertifizierungsstelle auf, die Unterlagen nicht außer Haus zu bringen. Diese Aufforderung basierte auf der Verpflichtung des Unternehmens, vertrauliche und vertrauliche Informationen zu schützen, und spiegelte seinen Wunsch nach maximaler Sicherheit und Kontrolle während des Auditprozesses wider.
Trotz sorgfältiger Vorbereitungen verlief das eigentliche Audit nicht wie geplant. NetworkFuse äußerte Bedenken hinsichtlich des zugewiesenen Auditteamleiters und forderte einen Ersatz. Das Unternehmen behauptete, derselbe Auditteamleiter habe zuvor einem der Hauptkonkurrenten von NetworkFuse eine Zertifizierung empfohlen. Dieser potenzielle Interessenkonflikt löste in der Unternehmensführung Bedenken aus. Die Zertifizierungsstelle lehnte NetworkFuses Antrag auf einen Ersatz jedoch ab, und der Auditprozess wurde abgebrochen.
Welche der folgenden Maßnahmen ist für NetworkFuse bei der Vorbereitung auf das Zertifizierungsaudit KEINE Voraussetzung?
A. Fachexperten identifizieren
B. Vorbereitung des Personals
C. Dokumentierte Informationen sammeln
Answer: A

QUESTION NO: 2

Eine Organisation dokumentiert jede implementierte Sicherheitskontrolle, indem sie ihre Funktionen detailliert beschreibt. Ist dies mit ISO/IEC 27001 konform?

A. Nein, der Standard verlangt nur die Dokumentation der Funktionsweise von Prozessen und Kontrollen, daher ist keine Beschreibung der einzelnen Sicherheitskontrollen erforderlich

B. Nein, da die dokumentierten Informationen ein striktes Format haben sollten, einschließlich Datum, Versionsnummer und Autorenidentifikation

C. Ja, aber die Dokumentation jeder Sicherheitskontrolle und nicht des Prozesses im Allgemeinen erschwert die Überprüfung der dokumentierten Informationen

Answer: C

Explanation:

According to ISO/IEC 27001:2022, clause 7.5, an organization is required to maintain documented information to support the operation of its processes and to have confidence that the processes are being carried out as planned. This includes documenting the information security policy, the scope of the ISMS, the risk assessment and treatment methodology, the statement of applicability, the risk treatment plan, the information security objectives, and the results of monitoring, measurement, analysis, evaluation, internal audit, and management review. However, the standard does not specify the level of detail or the format of the documented information, as long as it is suitable for the organization's needs and context. Therefore, documenting each security control that is implemented by describing their functions in detail is not a violation of the standard, but it may not be the most efficient or effective way to document the ISMS. Documenting each security control separately may make it harder to review, update, and communicate the documented information, and may also create unnecessary duplication or inconsistency. A better approach would be to document the processes and activities that involve the use of security controls, and to reference the relevant controls from Annex A or other sources. This way, the documented information would be more aligned with the process approach and the Plan-Do-Check-Act cycle that the standard promotes.

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clauses 4.3, 5.2, 6.1, 6.2, 7.5, 8.2, 8.3, 9.1, 9.2, 9.3, and Annex A ISO/IEC 27001:2022 Lead Implementer objectives and content, 4 and 5

QUESTION NO: 3

Szenario 9:

OpenTech mit Hauptsitz in San Francisco ist auf Lösungen im Bereich Informations- und Kommunikationstechnologie (IKT) spezialisiert. Zu den Kunden zählen vor allem Datenkommunikationsunternehmen und Netzbetreiber. Das Kernziel des Unternehmens besteht darin, seinen Kunden den reibungslosen Übergang zu Multi-Service-Providern zu ermöglichen und ihre Geschäftsprozesse an die komplexen Anforderungen der digitalen Landschaft anzupassen.

Kürzlich führte Tim, der interne Prüfer von OpenTech, ein internes Audit durch, bei dem Abweichungen bei den Überwachungsverfahren und Systemschwachstellen aufgedeckt wurden. Als Reaktion auf diese Abweichungen entschied sich OpenTech für einen umfassenden Problemlösungsansatz, um die Probleme systematisch anzugehen. Diese Methode umfasst einen teamorientierten Ansatz mit dem Ziel, die Ursachen der Probleme zu

identifizieren, zu beheben und zu beseitigen. Der Ansatz umfasst mehrere Schritte: Zunächst wird eine Gruppe von Experten mit fundierten Prozess- und Kontrollkenntnissen zusammengestellt. Anschließend wird die Abweichung in messbare Komponenten zerlegt und vorläufige Eindämmungsmaßnahmen implementiert. Anschließend werden mögliche Ursachen identifiziert und dauerhafte Korrekturmaßnahmen ausgewählt und überprüft. Schließlich werden diese Maßnahmen in die Praxis umgesetzt, validiert, Schritte zur Verhinderung eines erneuten Auftretens unternommen und die Bemühungen des Teams anerkannt und gewürdigt.
Nach der Analyse der Ursachen der Abweichungen entwickelte Julia, ISMS-Projektmanagerin bei OpenTech, eine Liste mit möglichen Maßnahmen zur Behebung der festgestellten Abweichungen. Julia prüfte die Liste sorgfältig, um sicherzustellen, dass jede Maßnahme die Ursache der jeweiligen Abweichung effektiv beseitigte. Bei der Bewertung möglicher Korrekturmaßnahmen identifizierte Julia ein Problem als signifikant und schätzte dessen Wiederholungswahrscheinlichkeit als hoch ein. Daher entschied sie sich für die Umsetzung temporärer Korrekturmaßnahmen. Anschließend fasste Julia alle Abweichungen in einem Aktionsplan zusammen und holte die Genehmigung der Geschäftsleitung ein. Der vorgelegte Aktionsplan hatte folgenden Wortlaut:
„Es wird eine neue Version der Zugriffskontrollrichtlinie eingeführt und neue Beschränkungen eingeführt, um sicherzustellen, dass der Netzwerkzugriff von der Abteilung für Informations- und Kommunikationstechnologie (IKT) effektiv verwaltet und überwacht wird.“ Julias eingereichter Aktionsplan wurde jedoch nicht von der Geschäftsleitung genehmigt. Als Grund wurde angegeben, dass ein allgemeiner Aktionsplan, der alle Nichtkonformitäten beheben sollte, als inakzeptabel erachtet wurde. Daher überarbeitete Julia den Aktionsplan und reichte separate Pläne zur Genehmigung ein. Leider hielt sich Julia nicht an die vom Unternehmen vorgegebene Einreichungsfrist, was zu einer Verzögerung des Korrekturmaßnahmenprozesses führte. Darüber hinaus fehlte den überarbeiteten Aktionsplänen ein definierter Zeitplan für die Umsetzung.
Hatte OpenTech einen Plan zur Umsetzung dauerhafter Korrekturmaßnahmen zur Behebung der festgestellten Nichtkonformitäten?

A. Ja, OpenTech hatte einen umfassenden Plan zur Umsetzung dauerhafter Korrekturmaßnahmen

B. Nein, OpenTech hatte keinen klaren Plan zur Umsetzung einer dauerhaften Korrekturmaßnahme

C. Nein, OpenTech hat sich entschieden, diesen Weg nicht weiter zu verfolgen

Answer: B

QUESTION NO: 4
Ein Technologieunternehmen hat eine Sicherheitsmaßnahme implementiert, um das sichere Entfernen oder Überschreiben vertraulicher Daten und lizenzierter Software auf Geräten vor der Entsorgung oder Wiederverwendung zu gewährleisten. Welche Art von Sicherheitskontrolle wurde implementiert?

A. Physische Kontrolle

B. Technologische Kontrolle

C. Organisatorische Kontrolle

Answer: B

Explanation:
The secure removal or overwriting of data (data sanitization) is a technological control. It involves technical means to ensure that information stored on electronic media is securely erased so that it cannot be recovered.
"Media sanitization and secure erasure are technical measures designed to prevent unauthorized recovery of information from equipment prior to disposal or reuse."
- ISO/IEC 27001:2022, Annex A, Control 8.10 Storage media; ISO/IEC 27002:2022, 8.10

QUESTION NO: 5
Szenario 9: OpenTech bietet IT- und Kommunikationsdienste an. Es unterstützt Datenkommunikationsunternehmen und Netzwerkbetreiber dabei, Multi-Service-Anbieter zu werden. Bei einem internen Audit hat der interne Prüfer Tim Abweichungen im Zusammenhang mit den Überwachungsverfahren festgestellt. Er hat mehrere Schwachstellen des Systems identifiziert und bewertet.
Tim stellte fest, dass Benutzerkennungen für Systeme und Dienste, die vertrauliche Informationen verarbeiten, wiederverwendet wurden und die Zugriffskontrollrichtlinien nicht eingehalten wurden. Nach der Analyse der Ursachen dieser Nichtkonformität erstellte der ISMS-Projektmanager eine Liste möglicher Maßnahmen zur Behebung der Nichtkonformität. Anschließend analysierte der ISMS-Projektmanager die Liste und wählte die Aktivitäten aus, die die Beseitigung der Grundursache und die Vermeidung ähnlicher Situationen in der Zukunft ermöglichen würden. Diese Aktivitäten wurden in einen Aktionsplan aufgenommen. Der von der Geschäftsleitung genehmigte Aktionsplan lautete wie folgt:
Es wird eine neue Version der Zugriffskontrollrichtlinie eingeführt und es werden neue Beschränkungen geschaffen, um sicherzustellen, dass der Netzwerkzugriff von der Abteilung für Informations- und Kommunikationstechnologie (IKT) effektiv verwaltet und überwacht wird. Der genehmigte Aktionsplan wurde umgesetzt und alle im Plan beschriebenen Maßnahmen wurden dokumentiert.
Hat der ISMS-Projektmanager den Korrekturmaßnahmenprozess basierend auf Szenario 9 angemessen abgeschlossen?
A. Ja, der Korrekturmaßnahmenprozess sollte die Identifizierung der Nichtkonformität, die Situationsanalyse und die Umsetzung von Korrekturmaßnahmen umfassen
B. Nein, die Korrekturmaßnahme hat die Grundursache der Nichtkonformität nicht behoben.
C. Nein, der Korrekturmaßnahmenprozess sollte auch die Überprüfung der Umsetzung der ausgewählten Maßnahmen beinhalten
Answer: C
Explanation:
According to ISO/IEC 27001:2022, the corrective action process consists of the following steps12:
Reacting to the nonconformity and, as applicable, taking action to control and correct it and deal with the consequences Evaluating the need for action to eliminate the root cause(s) of the nonconformity, in order that it does not recur or occur elsewhere Implementing the action needed Reviewing the effectiveness of the corrective action taken Making changes to the information security management system, if necessary In scenario 9, the ISMS project manager did not complete the last step of reviewing the effectiveness of the corrective action taken. This step is important to verify that the corrective action has achieved the intended

results and that no adverse effects have been introduced. The review can be done by using various methods, such as audits, tests, inspections, or performance indicators3. Therefore, the ISMS project manager did not complete the corrective action process appropriately.
1: ISO/IEC 27001:2022, clause 10.2 2: Procedure for Corrective Action [ISO 27001 templates] 3: ISO 27001 Clause 10.2 Nonconformity and corrective action

QUESTION NO: 6
Szenario 2: NyvMarketing ist eine Marketingagentur, die Kunden aus unterschiedlichen Branchen verschiedene Dienstleistungen anbietet. Mit Expertise in digitalem Marketing, Branding und Marktforschung hat sich NyvMarketing einen guten Ruf für innovative und wirkungsvolle Marketingkampagnen erarbeitet. Angesichts der wachsenden Bedeutung von Datensicherheit und Informationsschutz in der Marketinglandschaft entschied sich das Unternehmen für die Implementierung eines ISMS nach ISO 27001.
Bei der Implementierung seines ISMS stieß NyvMarketing auf eine erhebliche Herausforderung: die Bedrohung durch unzureichende Ressourcen. Diese Herausforderung gefährdete die effektive Umsetzung der ISMS-Ziele und könnte die Bemühungen des Unternehmens zum Schutz vertraulicher Informationen beeinträchtigen. Um dieser Bedrohung zu begegnen, verfolgte NyvMarketing einen proaktiven Ansatz und beauftragte Michael mit der Verwaltung der mit Ressourcenengpässen verbundenen Risiken.
Michael spielte eine entscheidende Rolle bei der Identifizierung und Behebung von Ressourcenlücken, der Entwicklung von Strategien zur Risikominderung und der effektiven Zuweisung von Ressourcen für die ISMS-Implementierung bei NyvMarket*ng, wodurch die Widerstandsfähigkeit des Unternehmens gegenüber Ressourcenproblemen gestärkt wurde. Darüber hinaus priorisierte NyvMarketing Branchenstandards und Best Practices im Bereich Informationssicherheit und befolgte gewissenhaft die Richtlinien der ISO/IEC 27002. Dieses Engagement, das auf Exzellenz und den Anforderungen der ISO/IEC 27001 beruht, unterstrich NyvMarketings Engagement für die Einhaltung höchster Standards im Bereich Informationssicherheit.
Im Zuge der ISMS-Implementierung verzichtete NyvMarketing auf die Ausklammerung einer der Kompetenzanforderungen (gemäß ISO/IEC 27001, Abschnitt 7.2). Das Unternehmen war der Ansicht, dass seine Belegschaft über die erforderliche Kompetenz zur Erfüllung der ISMS-bezogenen Aufgaben verfügte. Es lieferte jedoch keine gültige Begründung für diese Auslassung. Darüber hinaus wurden bestimmte Kontrollen aus Anhang A der ISO/IEC 27001 nicht implementiert. NyvMarketing versäumte es, eine akzeptable Begründung für diese Ausschlüsse zu liefern.
Während der ISMS-Implementierung hat NFMarketing Schwachstellen, die die Informationssicherheit beeinträchtigen könnten, sorgfältig bewertet. Zu diesen Schwachstellen zählten unzureichende Wartung und fehlerhafte Installation von Speichermedien, unzureichende regelmäßige Austauschpläne für Geräte, unzureichende Softwaretests und ungeschützte Kommunikationsleitungen. NBMarketing war sich bewusst, dass diese Schwachstellen ein Risiko für die Datensicherheit darstellen könnten. Daher hat das Unternehmen Schritte unternommen, um diese spezifischen Schwachstellen durch die Implementierung der erforderlichen Kontrollen und Gegenmaßnahmen zu beheben.
Beantworten Sie anhand des obigen Szenarios die folgende Frage.
Im Szenario 2 sah sich NyvMarketing während der ISMS-Implementierung mit der Gefahr unzureichender Ressourcen konfrontiert. In welche der folgenden Kategorien fällt diese

Bedrohung?
Hat NyvMarketing gemäß Szenario 2 Maßnahmen ergriffen, die der ISO/IEC 27001 hinsichtlich der Implementierung der Kontrollen in Anhang A entsprechen?

A. Ja, die von NyvMarketing während der Implementierung der Kontrollen von Anhang A ergriffenen Maßnahmen entsprechen ISO/IEC 27001

B. Nein, die Maßnahmen von NyvMarketing entsprachen nicht der ISO/IEC 27001, da eine der Kontrollen in Anhang A ohne Angabe von Gründen ausgeschlossen wurde.

C. Nein, die Maßnahmen von NyvMarketing entsprachen nicht der ISO/IEC 27001, da sie alle Kontrollen des Anhangs A hätten enthalten müssen.

D. Ja, da ISO/IEC 27002 Ausnahmen zulässt

Answer: B

Explanation:
ISO/IEC 27001:2022 requires that when an organization excludes any Annex A controls, it must provide a valid justification for each exclusion (Clause 6.1.3.d). Simply omitting a control or a requirement (such as competence, Clause 7.2) without documented justification is a non-conformance with ISO/IEC 27001. All exclusions must be justified and based on the results of the risk assessment and risk treatment process.
" Any controls omitted must be justified, and such justification must be documented as part of the Statement of Applicability. "
- ISO/IEC 27001:2022, Clause 6.1.3 d)
" The organization shall produce a Statement of Applicability that... justifies inclusions and exclusions of controls. "
- ISO/IEC 27001:2022, Clause 6.1.3 d)

QUESTION NO: 7
Szenario 1: HealthGenic ist eine Kinderklinik, die mithilfe einer webbasierten medizinischen Software die Gesundheit und das Wachstum von Kindern vom Säuglingsalter bis ins frühe Erwachsenenalter überwacht. Die Software wird auch zur Terminvereinbarung, zur Erstellung individueller medizinischer Berichte, zur Speicherung von Patientendaten und der Krankengeschichte sowie zur Kommunikation mit allen Beteiligten, einschließlich Eltern, anderen Ärzten und dem medizinischen Laborpersonal, verwendet.
Im letzten Monat kam es bei HealthGenic aufgrund der steigenden Zahl von Benutzern, die auf die Software zugriffen, zu mehreren Dienstunterbrechungen. Ein weiteres Problem, mit dem das Unternehmen bei der Verwendung der Software konfrontiert war, war die komplizierte Benutzeroberfläche, deren Verwendung für ungeschultes Personal eine Herausforderung darstellte.
Die Geschäftsleitung von HealthGenic informierte umgehend das Unternehmen, das die Software entwickelt hatte, über das Problem. Das Softwareunternehmen behob das Problem, veränderte dabei jedoch einige Dateien mit vertraulichen Patienteninformationen. Die Änderungen führten zu unvollständigen und fehlerhaften medizinischen Berichten und verletzten – was noch schlimmer war – die Privatsphäre der Patienten.
Welche in Szenario 1 beschriebene Situation stellt eine Bedrohung für HealthGenic dar?

A. HealthGenic hat sein Personal nicht in der Verwendung der Software geschult

B. Das Softwareunternehmen hat Informationen zu den Patienten von HealthGenic geändert

C. HealthGenic nutzte eine webbasierte medizinische Software zur Speicherung vertraulicher

Patienteninformationen

Answer: B

Explanation:

According to ISO/IEC 27001:2022, a threat is any incident that could negatively affect the confidentiality, integrity or availability of an asset1. In this scenario, the asset is the information related to HealthGenic's patients, which is stored and processed by the web-based medical software. The software company's modification of some files that comprised sensitive information related to HealthGenic's patients is an incident that could negatively affect the confidentiality and integrity of the asset, as it resulted in incomplete and incorrect medical reports and invaded the patients' privacy. Therefore, this situation represents a threat to HealthGenic.

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Informatio n security management systems - Requirements ISO 27001 Key Terms - PJR

QUESTION NO: 8

Das Sicherheitsteam von NoAVision identifizierte ein Bedrohungsszenario, bei dem Benutzerrechte im IAM-System gefälscht werden könnten. Dies könnte es Unbefugten ermöglichen, ihre Berechtigungen zu erweitern und auf geschützte Daten zuzugreifen. Das Team ordnete dies einer spezifischen Bedrohungsart zu, die gezielte Gegenmaßnahmen erfordert.

In Szenario 1 fällt die identifizierte Bedrohung in welche Bedrohungskategorie?

A. Menschliche Handlungen

B. Beeinträchtigung von Funktionen oder Diensten

C. Infrastrukturausfälle

Answer: A

Explanation:

According to ISO/IEC 27005:2022 Annex C, threats are grouped into categories including human actions (deliberate or accidental acts by people), technical failures (hardware or software malfunctions), and environmental events. The forging of user rights - where a malicious actor intentionally manipulates the IAM system to escalate privileges - is a deliberate human action. This falls under the " Human actions " threat category, which includes unauthorized access, misuse of privileges, identity fraud, and social engineering. " Compromise of functions or services " relates to denial of service or service disruption. " Infrastructure failures " refers to physical or technical breakdowns. Since the threat originates from an intentional human decision to forge credentials, Human actions is the correct classification per ISO/IEC
27005 threat taxonomy.

QUESTION NO: 9

Welche der folgenden Optionen sollte in einer Informationssicherheitsrichtlinie behandelt werden?

A. Nach einem Informationssicherheitsvorfall durchzuführende Maßnahmen

B. Der Organisation auferlegte gesetzliche und behördliche Verpflichtungen

C. Die Komplexität von Informationssicherheitsprozessen und deren Wechselwirkungen

Answer: B

Explanation:
According to the ISO/IEC 27001:2022 standard, an information security policy is a high-level document that defines the management approach and objectives for information security within the organization. It should include, among other things, the legal and regulatory obligations imposed upon the organization, such as compliance with laws, contracts, agreements, and standards that are relevant to information security. The information security policy should also provide the basis for establishing, implementing, maintaining, and continually improving the information security management system (ISMS).
ISO/IEC 27001:2022, Clause 5.2 Policy
ISO/IEC 27002:2022, Clause 5.1 Policies for information security
PECB ISO/IEC 27001 Lead Implementer Course, Module 3: Information Security Management System (ISMS)

QUESTION NO: 10
Szenario 2:
Beauty ist ein etabliertes Kosmetikunternehmen in der Schönheitsbranche. Das Unternehmen wurde vor mehreren Jahrzehnten mit der Leidenschaft gegründet, hochwertige Hautpflege-, Make-up- und Körperpflegeprodukte zu entwickeln, die die natürliche Schönheit unterstreichen. Im Laufe der Jahre hat sich Beauty einen hervorragenden Ruf für sein innovatives Produktangebot, sein Engagement für Kundenzufriedenheit und sein Engagement für ethische und nachhaltige Geschäftspraktiken erarbeitet.
Als Reaktion auf die sich rasant verändernden Einkaufsgewohnheiten der Verbraucher vollzog Beauty den Übergang vom traditionellen Einzelhandel zum E-Commerce-Modell. Um diese Strategie umzusetzen, führte Beauty eine umfassende Risikobewertung der Informationssicherheit durch und analysierte potenzielle Bedrohungen und Schwachstellen des neuen E-Commerce-Projekts, abgestimmt auf seine Geschäftsstrategie und -ziele.
Um die identifizierten Risiken zu minimieren, implementierte das Unternehmen verschiedene Sicherheitsmaßnahmen. Alle Mitarbeiter mussten Vertraulichkeitsvereinbarungen unterzeichnen, um die Bedeutung des Schutzes sensibler Kundendaten zu unterstreichen. Das Unternehmen überprüfte die Benutzerzugriffsrechte sorgfältig und stellte sicher, dass nur autorisiertes Personal Zugriff auf vertrauliche Informationen hatte. Da das Unternehmen wertvolle Produkte und einzigartige Formeln im Lager lagert, installierte es außerdem Alarmsysteme und Überwachungskameras mit Echtzeit-Warnmeldungen, um möglichen Vandalismus zu verhindern.
Nach einiger Zeit analysierte das IT-Sicherheitsteam die Prüfprotokolle, um die Aktivitäten der neu implementierten Sicherheitskontrollen zu überwachen und zu verfolgen. Bei der Untersuchung und Analyse der Prüfprotokolle stellte sich heraus, dass sich ein Angreifer über veraltete Anti-Malware-Software Zugriff auf das System verschafft hatte und vertrauliche Kundendaten wie Namen und Adressen offengelegt hatte. Daraufhin ersetzte das IT-Team die Anti-Malware-Software durch eine neue, die Schadcode bei ähnlichen Vorfällen automatisch entfernen kann. Die neue Software wurde auf allen Arbeitsstationen installiert und regelmäßig mit den neuesten Malware-Definitionen aktualisiert, wobei eine automatische Update-Funktion aktiviert war. Für den Zugriff auf vertrauliche Informationen wurde außerdem ein Authentifizierungsprozess implementiert, der eine Benutzerkennung und ein Kennwort erfordert.
Während der Untersuchung stellte Maya, die Informationssicherheitsmanagerin von Beauty,

fest, dass die Verantwortlichkeiten für die Informationssicherheit in den Stellenbeschreibungen nicht klar definiert waren. Das Unternehmen ergriff daraufhin umgehend Maßnahmen. Angesichts der globalen Reichweite seiner E-Commerce-Aktivitäten recherchierte Beauty sorgfältig und hielt sich an die gesetzlichen, behördlichen und vertraglichen Anforderungen der Branche. Dabei wurden internationale und lokale Vorschriften berücksichtigt, darunter Datenschutzgesetze, Verbraucherschutzgesetze und globale Handelsabkommen.
Um diese Anforderungen zu erfüllen, investierte Beauty in Rechtsberater und Compliance-Experten, die die Einhaltung der gesetzlichen Standards in allen Märkten, in denen das Unternehmen tätig war, kontinuierlich überwachten und sicherstellten. Darüber hinaus führte Beauty mehrere Schulungen zur Sensibilisierung des IT-Teams und anderer Mitarbeiter mit Zugriff auf vertrauliche Informationen zum Thema Informationssicherheit durch und betonte dabei die Bedeutung der System- und Netzwerksicherheit.
Welche Informationssicherheitsanforderung wurde von Beauty basierend auf Szenario 2 NICHT bewertet?

A. Ausrichtung der Risikobewertung an der Strategie der Organisation

B. Einhaltung gesetzlicher, regulatorischer und vertraglicher Verpflichtungen

C. Grundsätze und Ziele für den Informationslebenszyklus

Answer: C

QUESTION NO: 11
Was sollte eine Organisation bereitstellen, um die Aufrechterhaltung und Verbesserung des Informationssicherheits-Managementsystems sicherzustellen?

A. Die entsprechende Übertragung an den Betrieb

B. Ausreichende Ressourcen, wie z. B. Budget, qualifiziertes Personal und erforderliche Werkzeuge

C. Die von ISO/IEC 27001 geforderten dokumentierten Informationen

Answer: B
Explanation:
According to ISO/IEC 27001:2022, clause 10.2.2, the organization shall define and apply an information security incident management process that includes the following activities: reporting information security events and weaknesses;
assessing information security events and classifying them as information security incidents; responding to information security incidents according to their classification; learning from information security incidents, including identifying causes, taking corrective actions and preventive actions, and communicating the results and actions taken; collecting evidence, where applicable.
The standard does not specify who should perform these activities, as long as they are done in a consistent and effective manner. Therefore, the organization may choose to conduct forensic investigation internally or by using external consultants, depending on its needs, resources, and capabilities. However, the organization should ensure that the external consultants are competent, trustworthy, and comply with the organization's policies and procedures.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clause 10.2.2; PECB ISO/IEC 27001 Lead

Implementer Course, Module 10: Incident Management.

QUESTION NO: 12
Szenario 10: ProEBank
Die ProEBank ist ein österreichisches Finanzinstitut, das für sein umfassendes Angebot an Bankdienstleistungen bekannt ist.
Die ProEBank mit Hauptsitz in Wien profitiert vom fortschrittlichen Technologie- und Finanzökosystem der Stadt. Um ihre Sicherheitslage zu verbessern, hat sie ein Informationssicherheits-Managementsystem (ISMS) gemäß ISO/IEC 27001 implementiert.
Nach einem Jahr im Einsatz des ISMS beschloss das Unternehmen, ein Zertifizierungsaudit zu beantragen, um die Zertifizierung nach ISO/IEC 27001 zu erhalten.
Zur Vorbereitung auf das Audit informierte das Unternehmen zunächst seine Mitarbeiter und organisierte entsprechende Schulungen. Zudem wurden im Vorfeld Dokumente erstellt, um diese bei der Prüfung durch die externen Prüfer bereitzuhalten. Darüber hinaus wurde ermittelt, welche Mitarbeiter über das nötige Fachwissen verfügen, um die externen Prüfer bei der Erläuterung und Bewertung der Prozesse zu unterstützen.
In der Planungsphase des Audits prüfte ProEBank die von der Zertifizierungsstelle bereitgestellte Liste der beauftragten Auditoren. Dabei stellte ProEBank einen potenziellen Interessenkonflikt bei einem der Auditoren fest, der zuvor für den größten Konkurrenten von ProEBank im Bankensektor tätig gewesen war. Um die Integrität des Auditprozesses zu gewährleisten, verweigerte ProEBank die Durchführung des Audits, bis ein vollständig neues Auditteam eingesetzt wurde. Die Zertifizierungsstelle bestätigte den Interessenkonflikt und nahm die notwendigen Anpassungen vor, um die Unparteilichkeit des Auditteams sicherzustellen. Nach Behebung dieses Problems beurteilte das Auditteam, ob das ISMS sowohl den Anforderungen der Norm als auch den Unternehmenszielen entsprach. Dabei konzentrierte sich das Auditteam auf die Prüfung dokumentierter Informationen.
Drei Wochen später führte das Team einen Vor-Ort-Besuch beim Auditierten durch, um zu beurteilen, ob das ISMS den Anforderungen der ISO/IEC 27001 entsprach, effektiv implementiert war und dem Auditierten die Erreichung seiner Informationssicherheitsziele ermöglichte. Nach dem Besuch erstellte das Team die Audit-Schlussfolgerungen und informierte den Auditierten über einige festgestellte kleinere Abweichungen. Der Audit-Teamleiter sprach daraufhin eine Empfehlung zur Zertifizierung aus.
Nach Erhalt der Empfehlung des Leiters des Auditteams setzte die Zertifizierungsstelle einen Ausschuss ein, der über die Zertifizierung entscheiden sollte. Dem Ausschuss gehörten ein Mitglied des Auditteams und zwei weitere Experten der Zertifizierungsstelle an.
Nach dem Audit der Phase 2 wurden geringfügige Abweichungen festgestellt. Trotzdem sprach der Auditleiter eine positive Empfehlung für die Zertifizierung aus.
Frage:
Ist das akzeptabel?

A. Nein – der Auditor hätte eine negative Empfehlung für die Zertifizierung aussprechen müssen, da geringfügige Abweichungen festgestellt wurden.

B. Ja – eine Empfehlung zur Zertifizierung sollte ausgesprochen werden, wenn nur geringfügige Abweichungen festgestellt werden.

C. Nein – der Auditor hätte eine Empfehlung zur Zertifizierung unter der Bedingung aussprechen sollen, dass Korrekturmaßnahmenpläne für die geringfügigen Abweichungen

eingereicht werden.

Answer: B

Explanation:

ISO/IEC 17021-1:2015 Clause 9.4.5.2 states:

"A certification recommendation can be made when only minor nonconformities are identified, provided a corrective action plan is submitted and accepted." So long as the auditee commits to corrective actions within an agreed time, certification can proceed. Therefore, issuing a positive recommendation is compliant, assuming the organization has plans in place for resolution.

References:

ISO/IEC 17021-1:2015 Clause 9.4.5.2

ISO/IEC 27006:2015 Clause 8.3 - Handling of nonconformities==========

QUESTION NO: 13

Welches Feedback bezieht sich speziell auf die Leistung im Bereich Informationssicherheit während der Managementüberprüfung?

A. Möglichkeiten zur kontinuierlichen Verbesserung

B. Ergebnisse der Risikobewertung

C. Nichtkonformitäten und Korrekturmaßnahmen

Answer: B

Explanation:

Risk assessment results directly reflect information security performance because they show the current risk landscape, effectiveness of controls, and overall security posture. This is a specific input for management review under ISO/IEC 27001.

"Management review inputs shall include... results of risk assessment and status of risk treatment plan, which relate directly to information security performance."

- ISO/IEC 27001:2022, Clause 9.3.2

QUESTION NO: 14

Szenario 9:

OpenTech mit Hauptsitz in San Francisco ist auf Lösungen im Bereich Informations- und Kommunikationstechnologie (IKT) spezialisiert. Zu den Kunden zählen vor allem Datenkommunikationsunternehmen und Netzbetreiber. Das Kernziel des Unternehmens besteht darin, seinen Kunden den reibungslosen Übergang zu Multi-Service-Providern zu ermöglichen und ihre Geschäftsprozesse an die komplexen Anforderungen der digitalen Landschaft anzupassen.

Kürzlich führte Tim, der interne Prüfer von OpenTech, ein internes Audit durch, bei dem Abweichungen bei den Überwachungsverfahren und Systemschwachstellen aufgedeckt wurden. Als Reaktion auf diese Abweichungen entschied sich OpenTech für einen umfassenden Problemlösungsansatz, um die Probleme systematisch anzugehen. Diese Methode umfasst einen teamorientierten Ansatz mit dem Ziel, die Ursachen der Probleme zu identifizieren, zu beheben und zu beseitigen. Der Ansatz umfasst mehrere Schritte: Zunächst wird eine Gruppe von Experten mit fundierten Prozess- und Kontrollkenntnissen zusammengestellt. Anschließend wird die Abweichung in messbare Komponenten zerlegt und vorläufige Eindämmungsmaßnahmen implementiert. Anschließend werden mögliche

Ursachen identifiziert und dauerhafte Korrekturmaßnahmen ausgewählt und überprüft. Schließlich werden diese Maßnahmen in die Praxis umgesetzt, validiert, Schritte zur Verhinderung eines erneuten Auftretens unternommen und die Bemühungen des Teams anerkannt und gewürdigt.
Nach der Analyse der Ursachen der Abweichungen entwickelte Julia, ISMS-Projektmanagerin bei OpenTech, eine Liste mit möglichen Maßnahmen zur Behebung der festgestellten Abweichungen. Julia prüfte die Liste sorgfältig, um sicherzustellen, dass jede Maßnahme die Ursache der jeweiligen Abweichung effektiv beseitigte. Bei der Bewertung möglicher Korrekturmaßnahmen identifizierte Julia ein Problem als signifikant und schätzte dessen Wiederholungswahrscheinlichkeit als hoch ein. Daher entschied sie sich für die Umsetzung temporärer Korrekturmaßnahmen. Anschließend fasste Julia alle Abweichungen in einem Aktionsplan zusammen und holte die Genehmigung der Geschäftsleitung ein. Der vorgelegte Aktionsplan hatte folgenden Wortlaut:
„Es wird eine neue Version der Zugriffskontrollrichtlinie eingeführt und neue Beschränkungen eingeführt, um sicherzustellen, dass der Netzwerkzugriff von der Abteilung für Informations- und Kommunikationstechnologie (IKT) effektiv verwaltet und überwacht wird.“ Julias eingereichter Aktionsplan wurde jedoch nicht von der Geschäftsleitung genehmigt. Als Grund wurde angegeben, dass ein allgemeiner Aktionsplan, der alle Nichtkonformitäten beheben sollte, als inakzeptabel erachtet wurde. Daher überarbeitete Julia den Aktionsplan und reichte separate Pläne zur Genehmigung ein. Leider hielt sich Julia nicht an die vom Unternehmen vorgegebene Einreichungsfrist, was zu einer Verzögerung des Korrekturmaßnahmenprozesses führte. Darüber hinaus fehlte den überarbeiteten Aktionsplänen ein definierter Zeitplan für die Umsetzung.
Entsprach Julias Ansatz zur Einreichung von Aktionsplänen zur Behebung von Nichtkonformitäten den Best Practices?

A. Ja, da die Einreichung des Aktionsplans flexibel sein kann

B. Nein, da von Aktionsplänen normalerweise erwartet wird, dass sie bestimmte Fristen einhalten.

C. Ja, Julia hat den Aktionsplan überarbeitet, um die Übereinstimmung mit den Best Practices sicherzustellen

Answer: B

QUESTION NO: 15
Eine Gesundheitsorganisation muss sicherstellen, dass dem medizinischen Personal Patientenakten jederzeit zur Verfügung stehen. Welche Maßnahme sollte sie priorisieren, um dies zu erreichen?

A. Implementierung der Multi-Faktor-Authentifizierung

B. Festlegen von Richtlinien zur Datensatzaufbewahrung

C. Verwendung von Versionskontrollsystemen zur Datenverwaltung

Answer: B

QUESTION NO: 16
BioLooVitalis ist ein biopharmazeutisches Unternehmen mit Hauptsitz in Singapur, das für seine Pionierarbeit im Bereich der Humantherapie bekannt ist. BioLooVitalis legt großen Wert auf die Behandlung kritischer Gesundheitsprobleme, insbesondere in den Bereichen Herz-

Kreislauf-Erkrankungen, Onkologie, Knochengesundheit und Entzündungen. BioLooVitalis hat sein Engagement für Datensicherheit und -integrität durch die Aufrechterhaltung eines effektiven Informationssicherheitsmanagementsystems (ISMS) gemäß ISO/IEC 77001 in den letzten zwei Jahren unter Beweis gestellt. Nachdem über mehrere Wochen ein Anstieg fehlgeschlagener Anmeldeversuche festgestellt wurde, überprüfte das IT-Sicherheitsteam von BioLooVitalis die Protokolldaten, korrelierte sie mit Nutzerverhaltensmustern und ordnete sie bekannten Angriffsvektoren zu, um mögliche Ursachen zu ermitteln. Basierend auf ihren Erkenntnissen erstellten sie einen technischen Bericht, der die Art der Anomalien detailliert beschrieb, und reichten ihn bei der Compliance-Abteilung ein. Das Compliance-Team fasste die Ergebnisse zusammen und präsentierte sie der Geschäftsleitung im Rahmen der vierteljährlichen ISMS-Leistungsüberprüfung. Ziel war es, das Systemverhalten nach dem Anstieg der fehlgeschlagenen Anmeldeversuche proaktiv zu überwachen. Das IT-Sicherheitsteam von BioLooVitalis konfigurierte ein Dashboard, das Anmeldeaktivitäten in Echtzeit, Systemreaktionszeiten und die Verfügbarkeit von Endpunkten abteilungsübergreifend anzeigte. Dies half dem Team, ungewöhnliches Verhalten schnell zu erkennen, ohne auf formale Meldeverfahren warten zu müssen.
Nach der Implementierung des Echtzeit-Zugriffskontroll-Dashboards prüfte das interne Revisionsteam von BioLooVitalis, ob die neuen Prozesse und Tools unautorisierte Zugriffsversuche effektiv reduzierten und sowohl die technischen als auch die Richtlinienanforderungen erfüllten. Abschließend sammelten die internen Revisoren systemgenerierte Zugriffsprotokolle, überprüften Benutzerzugriffsberichte und führten Interviews mit IT-Mitarbeitern. Diese Datenquellen halfen ihnen zu verifizieren, ob die neuen Kontrollen wie vorgesehen funktionierten und mit den internen ISMS-Zielen übereinstimmten.
Beantworten Sie anhand des obigen Szenarios die folgende Frage.
Welcher Aspekt der internen Prüfung wurde von BioLooVital behandelt? Siehe Szenario 8.

A. Bewertung der Effektivität und Effizienz des ISMS-Lebenszyklus

B. Bewertung der Effektivität und Effizienz von Prozessen und Kontrollen

C. Bewertung der ISMS-Messung

Answer: B

Explanation:
In Scenario 8, BioLooVitalis's internal audit team assessed whether new processes and tools effectively reduced unauthorized access attempts and met both technical and policy-based requirements. This activity squarely addresses the evaluation of the effectiveness and efficiency of processes and controls, making Option B the correct answer.
ISO/IEC 27001:2022 Clause 9.2 - Internal audit requires that the organization conduct internal audits to provide information on whether the ISMS:
conforms to the organization's own requirements and ISO/IEC 27001 requirements; and is effectively implemented and maintained.
The scenario describes auditors examining specific controls (access controls, monitoring dashboards) and processes (log review, reporting, response) to verify that they function as intended and reduce risk. This aligns with evaluating controls and processes, not the entire ISMS lifecycle (Option A), nor a narrow review of measurement processes alone (Option C). Additionally, auditors collected logs, reviewed reports, and conducted interviews, which are classic audit techniques used to test control effectiveness and process efficiency. The focus was not on redesigning the ISMS or assessing maturity across all lifecycle phases, but on

verifying whether the implemented controls achieved their objectives.

QUESTION NO: 17
Ein Unternehmen entschied sich für einen Algorithmus, der verschiedene Merkmale des Kundenverhaltens, wie z. B. Suchmuster und demografische Merkmale, analysiert und Kunden anhand ähnlicher Merkmale gruppiert. Auf diese Weise kann das Unternehmen unter anderem Stammkäufer und Trendfolger identifizieren. Welche Art von maschinellem Lernen nutzt das Unternehmen?
A. Maschinelles Lernen von Entscheidungsbäumen
B. Überwachtes maschinelles Lernen
C. Unüberwachtes maschinelles Lernen
Answer: C
Explanation:
According to the ISO/IEC 27001 : 2022 Lead Implementer course, one of the objectives of information security incident management is to collect and preserve records that can be used as evidence for disciplinary and legal action, as well as for learning and improvement purposes1. Therefore, Anna should be aware of the collection and preservation of records when gathering data for the forensics team. She should follow the guidelines and procedures specified in the information security incident management policy of InfoSec, which defines the type, format, content, and location of the records to be created and maintained2. The records should be accurate, complete, consistent, and reliable, and should be protected from unauthorized access, modification, or deletion3.
1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 8: Information Security Incident Management, slide 16 2: PECB, ISO/IEC 27001 Lead Implementer Course, Module 8: Information Security Incident Management, slide 19 3: PECB, ISO/IEC 27001 Lead Implementer Course, Module 8: Information Security Incident Management, slide 20

QUESTION NO: 18
Szenario 8: SunDee ist ein biopharmazeutisches Unternehmen mit Hauptsitz in Kalifornien, USA. SunDee ist bekannt für seine Pionierarbeit im Bereich der Humantherapie und legt großen Wert auf die Behandlung kritischer Gesundheitsprobleme, insbesondere in den Bereichen Herz-Kreislauf-Erkrankungen, Onkologie, Knochengesundheit und Entzündungen. SunDee hat sein Engagement für Datensicherheit und -integrität unter Beweis gestellt, indem es seit zwei Jahren ein effektives Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 unterhält.
Zur Vorbereitung auf das Rezertifizierungsaudit führte SunDee ein internes Audit durch. Die Unternehmensleitung ernannte Alex, der in den letzten sechs Monaten das Tagesgeschäft der Compliance-Abteilung aktiv geleitet hatte, zum internen Auditor. In dieser Doppelrolle ist Alex damit beauftragt, ein Audit durchzuführen, das die Compliance sicherstellt und wertvolle Empfehlungen zur Verbesserung der Betriebseffizienz liefert.
Während des internen Audits wurden einige Abweichungen festgestellt. Um diese umfassend zu beheben, erstellte das Unternehmen in enger Zusammenarbeit mit dem Leiter des Auditteams für jede Abweichung einen Aktionsplan.
Die Geschäftsleitung von SunDee führte eine umfassende Überprüfung des ISMS durch, um dessen Angemessenheit, Zulänglichkeit und Effizienz zu bewerten. Diese Überprüfung wurde

in die regelmäßigen Management-Meetings integriert. Wichtige Dokumente, darunter Auditberichte, Aktionspläne und Ergebnisse der Überprüfung, wurden vor der Sitzung an alle Mitglieder verteilt. Die Tagesordnung umfasste den Status früherer Überprüfungsmaßnahmen, Änderungen am ISMS, Feedback, Stakeholder-Input und Verbesserungsmöglichkeiten. Entscheidungen und Maßnahmen zur Verbesserung des ISMS wurden getroffen. Der ISMS-Koordinator und das interne Audit-Team spielten eine wichtige Rolle bei der Ausarbeitung von Folgeaktionsplänen, die anschließend vom oberen Management genehmigt wurden.
Als Reaktion auf die Ergebnisse der Überprüfung ergriff SunDee umgehend Korrekturmaßnahmen und stärkte seine Informationssicherheitsmaßnahmen. Zusätzlich wurden Dashboard-Tools eingeführt, die einen umfassenden Überblick über die wichtigsten Leistungsindikatoren bieten, die für die Überwachung des Informationssicherheitsmanagements des Unternehmens unerlässlich sind. Diese Indikatoren umfassten Kennzahlen zu Sicherheitsvorfällen, deren Kosten, Systemschwachstellentests, der Erkennung von Abweichungen und Lösungszeiten und ermöglichten so eine effektive Aufzeichnung, Berichterstattung und Nachverfolgung der Überwachungsaktivitäten. Darüber hinaus startete SunDee einen umfassenden Messprozess, um den Fortschritt und die Ergebnisse laufender Projekte zu bewerten und implementierte umfangreiche Maßnahmen in allen Prozessen. Die Geschäftsleitung legte fest, dass die für die Informationen verantwortliche Person nicht nur Eigentümer der zu den Maßnahmen beitragenden Daten, sondern auch für die Durchführung dieser Messaktivitäten verantwortlich ist.
Beantworten Sie basierend auf dem obigen Szenario die folgende Frage:
Hat SunDee die Rollen für Messaktivitäten richtig definiert?

A. Ja, der Informationseigentümer kann auch für die Durchführung von Messaktivitäten verantwortlich sein

B. Nein, da der Informationseigentümer nicht verschiedene messbezogene Rollen und Verantwortlichkeiten übernehmen kann

C. Nein, da die Verantwortung für die Durchführung der Messaktivitäten dem Informationskommunikator übertragen werden sollte

Answer: A

QUESTION NO: 19
Infralink ist ein mittelständisches IT-Beratungsunternehmen mit Hauptsitz in Dublin, Irland. Es ist spezialisiert auf sichere Cloud-Infrastruktur, Softwareintegration und Datenanalyse und betreut einen vielfältigen Kundenstamm aus den Bereichen Gesundheitswesen, Finanzdienstleistungen und Recht, darunter Krankenhäuser, Versicherungen und Anwaltskanzleien. Zum Schutz sensibler Kundendaten und zur Sicherstellung der Geschäftskontinuität hat Infralink ein Informationssicherheits-Managementsystem (ISMS) gemäß den Anforderungen der ISO/IEC 27001 implementiert.
Bei der Entwicklung seiner Sicherheitsarchitektur setzte das Unternehmen auf Dienste zur zentralen Benutzeridentifizierung und abteilungsübergreifenden, gemeinsamen Authentifizierung. Diese Dienste regelten auch die Erstellung und Verwaltung von Zugangsdaten innerhalb des Unternehmens. Darüber hinaus implementierte Infralink Lösungen zum Schutz sensibler Daten während der Übertragung und im Ruhezustand, um

Vertraulichkeit und Integrität in allen Systemen zu gewährleisten.
Zur Vorbereitung der Implementierung von Informationssicherheitsmaßnahmen stellte das Unternehmen die Verfügbarkeit der notwendigen Ressourcen, die Kompetenz des Personals und eine strukturierte Planung sicher. Es führte eine Kosten-Nutzen-Analyse durch, legte Implementierungsphasen fest und erstellte Dokumentationen sowie Checklisten für jede Phase. Die angestrebten Ergebnisse wurden klar definiert, um die Sicherheitsmaßnahmen mit den Geschäftszielen in Einklang zu bringen.
Infralink begann mit der Implementierung mehrerer Kontrollen aus Anhang A der ISO/IEC 27001. Dazu gehörten die Regelung des physischen und logischen Zugriffs auf Informationen und Assets gemäß den Geschäfts- und Informationssicherheitsanforderungen, das Management des Identitätslebenszyklus sowie die Einrichtung von Verfahren zur Erteilung, Überprüfung, Änderung und zum Entzug von Zugriffsrechten. Kontrollen im Zusammenhang mit der sicheren Zuweisung und Verwaltung von Authentifizierungsinformationen sowie die Einrichtung von Regeln oder Vereinbarungen für die sichere Datenübertragung wurden jedoch noch nicht implementiert. Im Rahmen der Dokumentation stellte das Unternehmen sicher, dass alle ISMS-bezogenen Dokumente die Rückverfolgbarkeit durch Titel, Erstellungs- oder Aktualisierungsdatum, Autorennamen und eindeutige Referenznummern gewährleisten. Beantworten Sie vor dem Hintergrund des oben beschriebenen Szenarios die folgende Frage.
Welche Sicherheitsmaßnahmen hat Infrelink in Szenario 3 implementiert?

A. 5.14 Informationsübertragung und A.5.17 Authentifizierungsinformationen

B. 5.15 Zugriffskontrolle. A.5.16 Identitätsmanagement und A.5.18 Zugriffsrechte

C. 5.35 Unabhängige Überprüfung der Informationssicherheit

Answer: B
Explanation:
The correct answer is Option B, as it precisely reflects the Annex A controls explicitly implemented by Infralink in Scenario 3.
The scenario states that Infralink implemented controls that:
Regulate physical and logical access to information and assets
Manage the identity life cycle
Establish procedures for providing, reviewing, modifying, and revoking access rights These map directly to the following ISO/IEC 27001:2022 Annex A organizational controls:
A).5.15 - Access controlRequires access to information and assets to be restricted in accordance with business and security requirements.
A).5.16 - Identity managementCovers the establishment, maintenance, and removal of identities throughout their lifecycle.
A).5.18 - Access rightsRequires formal processes for granting, reviewing, and revoking access rights.
The scenario explicitly notes that A.5.17 (Authentication information) and A.5.14 (Information transfer) have not yet been implemented, which rules out Option A.
Option C is incorrect because A.5.35 - Independent review of information security relates to audit and governance activities, not access or identity controls, and is not referenced in the scenario.

QUESTION NO: 20

Szenario 1: HealthGenic ist eine Kinderklinik, die mithilfe einer webbasierten medizinischen Software die Gesundheit und das Wachstum von Kindern vom Säuglingsalter bis ins frühe Erwachsenenalter überwacht. Die Software wird auch zur Terminvereinbarung, zur Erstellung individueller medizinischer Berichte, zur Speicherung von Patientendaten und Krankengeschichte sowie zur Kommunikation mit allen Beteiligten, einschließlich Eltern, anderen Ärzten und dem medizinischen Laborpersonal, verwendet.
Im letzten Monat kam es bei HealthGenic aufgrund der steigenden Zahl von Benutzern, die auf die Software zugriffen, zu mehreren Dienstunterbrechungen. Ein weiteres Problem, mit dem das Unternehmen bei der Verwendung der Software konfrontiert war, war die komplizierte Benutzeroberfläche, deren Verwendung für ungeschultes Personal eine Herausforderung darstellte.
Die Geschäftsleitung von HealthGenic informierte umgehend das Unternehmen, das die Software entwickelt hatte, über das Problem. Das Softwareunternehmen behob das Problem, veränderte dabei jedoch einige Dateien mit sensiblen Patienteninformationen. Die Änderungen führten zu unvollständigen und fehlerhaften medizinischen Berichten und verletzten – was noch schlimmer war – die Privatsphäre der Patienten.
Beantworten Sie basierend auf dem obigen Szenario die folgende Frage:
Welches der folgenden Anzeichen deutet darauf hin, dass die Vertraulichkeit von Informationen verletzt wurde?

A. Dienstunterbrechungen aufgrund der gestiegenen Benutzerzahl

B. Verletzung der Privatsphäre von Patienten

C. Änderung der medizinischen Berichte der Patienten

Answer: B

Explanation:
Confidentiality of information is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. In other words, confidentiality ensures that only those who are authorized to access the information can do so. In the scenario, the confidentiality of information was compromised when the software company modified some files that contained sensitive information related to HealthGenic's patients. This modification resulted in the invasion of patients' privacy, which means that their personal and medical information was exposed to unauthorized parties. Therefore, the correct answer is B.
ISO/IEC 27001:2013, Information technology - Security techniques - Information securit y management systems - Requirements, clause 3.14.

QUESTION NO: 21
Szenario 5: Operaze ist ein kleines Softwareentwicklungsunternehmen, das Anwendungen für verschiedene Unternehmen weltweit entwickelt. Kürzlich führte das Unternehmen eine Risikobewertung durch, um die Informationssicherheitsrisiken zu ermitteln, die sich aus dem Betrieb in einer digitalen Landschaft ergeben können. Mithilfe verschiedener Testmethoden, darunter Penetrationstests und Code-Reviews, identifizierte das Unternehmen einige Probleme in seinen IKT-Systemen, darunter fehlerhafte Benutzerberechtigungen, falsch konfigurierte Sicherheitseinstellungen und unsichere Netzwerkkonfigurationen. Um diese Probleme zu beheben und die Informationssicherheit zu erhöhen, entschied sich Operaze für die Implementierung eines Informationssicherheits-Managementsystems (ISMS) nach

ISO/IEC 27001.
Da Operaze ein kleines Unternehmen ist, war das gesamte IT-Team an der ISMS-Implementierung beteiligt. Zunächst analysierte das Unternehmen die Geschäftsanforderungen sowie das interne und externe Umfeld, identifizierte die wichtigsten Prozesse und Aktivitäten und identifizierte und analysierte die interessierten Parteien. Darüber hinaus beschloss die Geschäftsleitung von Operaze, die meisten Abteilungen des Unternehmens in den ISMS-Umfang einzubeziehen. Der definierte Umfang umfasste die organisatorischen und physischen Grenzen. Das IT-Team entwarf eine Informationssicherheitsrichtlinie und kommunizierte diese an alle relevanten interessierten Parteien. Darüber hinaus wurden weitere spezifische Richtlinien entwickelt, um Sicherheitsaspekte zu erläutern, und allen interessierten Parteien wurden Rollen und Verantwortlichkeiten zugewiesen.
Anschließend behauptete der Personalleiter, dass der durch das ISMS erzeugte Papierkram dessen Wert nicht rechtfertige und die Implementierung des ISMS abgebrochen werden sollte. Das Topmanagement entschied jedoch, dass diese Behauptung ungültig war und organisierte eine Informationsveranstaltung, um allen interessierten Parteien die Vorteile des ISMS zu erläutern.
Operaze beschloss, seine physischen Server auf virtuelle Server auf einer Drittanbieter-Infrastruktur zu migrieren. Die neue Cloud-Computing-Lösung brachte zusätzliche Veränderungen für das Unternehmen mit sich. Das Top-Management von Operaze hingegen wollte nicht nur ein effektives ISMS implementieren, sondern auch dessen reibungslosen Ablauf sicherstellen. In dieser Situation kam das Top-Management von Operaze zu dem Schluss, dass die Umsetzung der Informationssicherheitsstrategien externe Experten erforderte. Das IT-Team wiederum beschloss, den Umfang des ISMS zu ändern und nahm die erforderlichen Anpassungen an den Unternehmensprozessen vor.
Beantworten Sie basierend auf dem obigen Szenario die folgende Frage:
Was hat Operaze dazu bewogen, das ISMS zu implementieren?

A. Identifizierung von Schwachstellen

B. Identifizierung von Bedrohungen

C. Identifizierung von Vermögenswerten

Answer: A
Explanation:
According to the scenario, Operaze conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration testing and code review, the company identified some issues in its ICT systems, such as improper user permissions, misconfigured security settings, and insecure network configurations. These issues are examples of vulnerabilities, which are weaknesses or gaps in the protection of an asset that can be exploited by a threat. Therefore, the identification of vulnerabilities led Operaze to implement the ISMS.
ISO/IEC 27001:2022 Lead Implementer Training Course Guide1
ISO/IEC 27001:2022 Lead Implementer Info Kit2

QUESTION NO: 22
Was ist der Hauptunterschied zwischen einem Auditprogramm und einem Auditplan?

A. Ein Auditprogramm beschreibt die Aktivitäten und Vorkehrungen für ein bestimmtes Audit,

während ein Auditplan einen übergreifenden Rahmen für eine Reihe von Audits mit spezifischen Zeitplänen und Zwecken bietet.

B. Ein Auditprogramm skizziert den übergreifenden Rahmen für eine Reihe von Audits mit spezifischen Zeitplänen und Zielen, während ein Auditplan die Aktivitäten und Vorkehrungen für ein bestimmtes Audit umreißt.

C. Ein Auditprogramm umreißt Richtlinien, Verfahren oder Anforderungen als Referenz für den Vergleich von Auditnachweisen, während ein Auditplan einen übergreifenden Rahmen für eine Reihe von Audits mit spezifischen Zeitplänen und Zwecken bietet.

Answer: B

Explanation:

An audit program provides the overall schedule, scope, and objectives for a series of audits. An audit plan is a document for a specific audit that describes activities, arrangements, and responsibilities.

"An audit program consists of one or more audits planned for a specific timeframe and direction. An audit plan describes how a particular audit will be conducted."

- ISO/IEC 19011:2018, Clause 5.1 & 5.4

QUESTION NO: 23

Frage:

Eine Organisation hat ihre tatsächliche Leistung mit vorab festgelegten Leistungszielen verglichen. Was ist der Hauptzweck dieser Maßnahme?

A. Um zu überprüfen, ob alle Sicherheitsvorfälle behoben wurden.

B. Um zu beurteilen, ob die Sicherheitsziele der Organisation erreicht werden

C. Um die Notwendigkeit der manuellen Nachverfolgung und Berichterstattung zu eliminieren

.

Answer: B

Explanation:

ISO/IEC 27001:2022 Clause 9.1 - Monitoring, measurement, analysis, and evaluation:

"The organization shall evaluate the performance and effectiveness of the information security management system. The evaluation shall include... comparison against performance indicators and security objectives." The purpose is to ensure that security objectives (Clause 6.2) are being met. Measuring performance allows organizations to determine whether controls and processes are effective and aligned with strategic goals.

Option A is too narrow, and Option C is incorrect because manual tracking may still be required in some cases.

References:

ISO/IEC 27001:2022 Clause 6.2 and 9.1

ISO/IEC 27004:2016 - Clause 7.2 (Use of metrics for objective evaluation)==========

QUESTION NO: 24

Wer sollte unter anderem an der Ausarbeitung, Überprüfung und Validierung von Verfahren zur Informationssicherheit beteiligt sein?

A. Ein externer Experte

B. Der Informationssicherheitsausschuss

C. Die für den ISMS-Betrieb zuständigen Mitarbeiter

Answer: B
Explanation:
According to ISO/IEC 27001:2022, clause 7.5.1, the organization shall ensure that the documented information required by the ISMS and by this document is controlled to ensure that it is available and suitable for use, where and when it is needed, and that it is adequately protected. This includes ensuring that the documented information is reviewed and approved for suitability and adequacy. The information security procedures are part of the documented information that supports the operation of the ISMS processes and the implementation of the information security controls. Therefore, they should be drafted, reviewed, and validated by the information security committee, which is the group of people responsible for overseeing the ISMS and ensuring its alignment with the organization's objectives and strategy. The information security committee should include representatives from different functions and levels of the organization, as well as external experts if needed. The information security committee should also ensure that the information security procedures are communicated to the relevant employees and other interested parties, and that they are periodically reviewed and updated as necessary.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clauses 5.3, 7.5.1, and 9.3 ISO/IEC 27001:2022 Lead Implementer objectives and content, 4 and 5

QUESTION NO: 25
Frage:
Welche der folgenden Aussagen beschreibt das Open Security Architecture (OSA)-Framework am besten?
A. Ein Rahmenwerk, das die Funktionalität und die technischen Kontrollen der Sicherheit erläutert und einen ganzheitlichen Überblick über wichtige Sicherheitsaspekte bietet.
B. Ein Rahmenwerk, das Organisationen bei der Festlegung der Ziele für die Entwicklung ihrer Sicherheitsarchitektur unterstützt und sich dabei auf die Anfangsphasen der Sicherheitsarchitektur konzentriert.
C. Ein Framework, das die Organisation von Artefakten der Unternehmensarchitektur, einschließlich Dokumenten, Spezifikationen und Modellen, unterstützt, indem es die Auswirkungen dieser Artefakte auf verschiedene Stakeholder berücksichtigt.
Answer: A
Explanation:
The Open Security Architecture (OSA) provides free, vendor-neutral security architecture patterns and guidance for implementing security controls. It is intended to:
"Present a holistic view of essential security components and technical measures to assist organizations in securing their IT environments." This aligns best with Option A, as it reflects the comprehensive and practical nature of OSA in cybersecurity architecture planning.
References:
ISO/IEC 27001:2022 Implementation Toolkit Reference - Security Architecture Best Practices
OSA official documentation overview==========

QUESTION NO: 26
Welche der folgenden Situationen können sich negativ auf den internen Auditprozess

auswirken?

A. Beschränkung des Zugangs des internen Prüfers zu Büros und Unterlagen

B. Durchführung interner Audit-Interviews mit allen Mitarbeitern der Organisation

C. Berichterstattung der Ergebnisse des internen Audits an die oberste Leitung

Answer: A

Explanation:

According to the ISO/IEC 27001 : 2022 Lead Implementer course, one of the factors that can negatively affect the internal audit process is the lack of cooperation from the auditees, which can manifest as restricting the internal auditor's access to offices and documentation1. This can hinder the auditor's ability to collect sufficient and appropriate audit evidence, verify the conformity of the information security management system (ISMS) with the audit criteria, and identify any nonconformities or opportunities for improvement2. Therefore, the auditees should be informed of the audit objectives, scope, criteria, and schedule in advance, and should provide the auditor with all the necessary information and resources to conduct the audit effectively3.

1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide 22 2: PECB, ISO/IEC

27001 Lead Implementer Course, Module 9: Internal Audit, slide 23 3: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide 24

QUESTION NO: 27

Szenario 7: InfoSec mit Sitz in Boston, Massachusetts, ist ein multinationaler Konzern, der professionelle Elektronik-, Gaming- und Unterhaltungsprodukte anbietet. Nach mehreren Informationssicherheitsvorfällen hat InfoSec beschlossen, Expertenteams einzurichten und Maßnahmen zu ergreifen, um mögliche Vorfälle in Zukunft zu verhindern.

Emma, Bob und Anna wurden als neue Mitglieder des Informationssicherheitsteams von InfoSec eingestellt, das aus einem Sicherheitsarchitekturteam, einem Incident-Response-Team (IRT) und einem Forensikteam besteht. Emmas Aufgabe ist es, Informationssicherheitspläne, Richtlinien, Protokolle und Schulungen zu erstellen, um InfoSec auf die effektive Reaktion auf Vorfälle vorzubereiten. Emma und Bob werden Vollzeitmitarbeiter von InfoSec, während Anna als externe Beraterin engagiert wird.

Bob, ein Netzwerkexperte, implementiert eine abgeschirmte Subnetzarchitektur. Diese Architektur isoliert die demilitarisierte Zone (DMZ), an die gehostete öffentliche Dienste angeschlossen sind, und die öffentlich zugänglichen Ressourcen von InfoSec vom privaten Netzwerk. So kann InfoSec potenzielle Angreifer daran hindern, unerwünschte Ereignisse im Unternehmensnetzwerk zu verursachen. Bob ist außerdem dafür verantwortlich, die Art eines unerwarteten Ereignisses gründlich zu bewerten, einschließlich der Art und Weise, wie es dazu kam und wen oder wen es betreffen könnte.

Anna hingegen erstellt Aufzeichnungen der Daten, Überprüfungen, Analysen und Berichte, um Beweise für disziplinarische und rechtliche Maßnahmen zu sichern und diese zur Verhinderung künftiger Vorfälle zu nutzen. Um dies entsprechend zu erledigen, sollte sie sich im Voraus mit der Unternehmensrichtlinie zum Informationssicherheitsvorfallmanagement vertraut machen. Diese Richtlinie legt unter anderem fest, welche Art von Aufzeichnungen erstellt werden sollen, wo sie aufbewahrt werden sollen und welches Format und welchen Inhalt die einzelnen Aufzeichnungstypen haben sollen.

Im Rahmen der InfoSec-Initiative zur Stärkung der Informationssicherheit führt Anna nur dann Risikobewertungen zur Informationssicherheit durch, wenn wesentliche Änderungen vorgeschlagen werden, und dokumentiert die Ergebnisse dieser Risikobewertungen. Nach Abschluss des Risikobewertungsprozesses ist Anna für die Entwicklung und Umsetzung eines Plans zur Behandlung von Informationssicherheitsrisiken sowie für die Dokumentation der Ergebnisse der Risikobehandlung verantwortlich.
Darüber hinaus war das Top-Management von InfoSec im Rahmen der Umsetzung des Kommunikationsplans für Informationssicherheit für die Erstellung eines Fahrplans für die Entwicklung neuer Produkte verantwortlich. Dieser Ansatz hilft dem Unternehmen, seine Sicherheitsmaßnahmen mit den Produktentwicklungsbemühungen abzustimmen und so sein Engagement für die Integration von Sicherheit in alle Aspekte seiner Geschäftstätigkeit zu demonstrieren.
InfoSec nutzt ein Cloud-Service-Modell mit cloudbasierten Apps, auf die über das Internet oder eine Anwendungsprogrammierschnittstelle (API) zugegriffen werden kann. Alle Cloud-Dienste werden vom Cloud-Service-Anbieter bereitgestellt, die Datenverwaltung übernimmt InfoSec. Dies bringt besondere Sicherheitsaspekte mit sich und ist ein zentrales Anliegen des Informationssicherheitsteams, um den Schutz von Daten und Systemen in dieser Umgebung zu gewährleisten.
Beantworten Sie anhand dieses Szenarios die folgende Frage:
Hält sich InfoSec bei der Durchführung von Risikobewertungen zur Informationssicherheit an die Anforderungen von ISO/IEC 27001?

A. Ja, es entsprach den Anforderungen von ISO/IEC 27001

B. Nein, da es diese auch in geplanten Intervallen durchführen sollte

C. Nein, da sie unabhängig von wesentlichen Änderungen zweimal jährlich durchgeführt werden sollten.

Answer: B

QUESTION NO: 28
Muss NyvMarketing die Richtlinien von ISO/IEC 27002 befolgen, um die ISO/IEC 27001-Zertifizierung zu erhalten?

A. Nein, die Einhaltung der ISO/IEC 27002-Richtlinien ist für die ISO/IEC 27001-Zertifizierung nicht zwingend erforderlich

B. Ja, da es eine Anforderung gemäß ISO/IEC 27001 ist

C. Ja, da die in Anhang A der ISO/IEC 27001 vorgesehenen Kontrollen mit den Kontrollen der ISO/IEC 27002 übereinstimmen

D. Ja, da ISO/IEC 27002 ein auditierbarer Standard ist

Answer: A
Explanation:
ISO/IEC 27001:2022 is the certifiable standard for Information Security Management Systems (ISMS). While ISO/IEC 27002 provides guidelines and best practices to help organizations implement the controls listed in Annex A of ISO/IEC 27001, it is not mandatory to follow ISO/IEC 27002 to achieve ISO/IEC 27001 certification. Instead, organizations must select and implement appropriate controls from Annex A, or other controls as necessary, based on their risk assessment. ISO/IEC 27002 serves as guidance but is not itself an auditable or certifiable requirement.

" The controls listed in Annex A are not exhaustive and additional controls may be needed. ISO/IEC 27002 provides implementation guidance and is not mandatory for certification against ISO/IEC 27001. "
- ISO/IEC 27001:2022, Introduction and Clause 6.1.3; ISO/IEC 27002:2022, Foreword

QUESTION NO: 29
NoAVision ist ein mittelständischer Anbieter von Cybersicherheitslösungen mit Hauptsitz in Tartu, Estland, und Niederlassungen in Stockholm und Berlin. Das Unternehmen ist spezialisiert auf sicheres Cloud-Hosting, Identitäts- und Zugriffsmanagement (IAM) sowie das Lebenszyklusmanagement digitaler Zertifikate. Zu seinen Kunden zählen Unternehmen aus dem öffentlichen Sektor, dem Finanzdienstleistungssektor und dem Gesundheitswesen, darunter Ministerien, Privatkliniken und Fintech-Unternehmen im gesamten Europäischen Wirtschaftsraum (EWR). Um sensible Informationen strukturiert zu schützen, implementierte NoAVision ein Informationssicherheits-Managementsystem (ISMS) gemäß ISO/IEC. 27001. In der Planungs- und Entwurfsphase stützte sich das Unternehmen auf ein ISO -Leitfadendokument, das jede Klausel der Norm interpretierte. Anstatt zusätzliche Anforderungen einzuführen, bot das Dokument praktische Empfehlungen, Umsetzungsalternativen und Kontextinformationen, wodurch das Unternehmen Unklarheiten vermeiden und ein funktionsfähiges ISMS entwickeln konnte.
Auf welches Dokument stützte sich NoAVision während der Planungs- und Entwurfsphasen der ISMS-Implementierung?
A. PCI DSS
B. ISO/IEC 27701
C. ISO/IEC 27003
Answer: C
Explanation:
ISO/IEC 27003 is the official guidance document for ISO/IEC 27001. It interprets each clause of the standard without introducing new mandatory requirements. Instead, it provides practical recommendations, implementation options, and contextual insights to help organizations understand and apply each requirement effectively. This aligns perfectly with the scenario description - the document " interpreted each clause " and
" offered practical recommendations and implementation alternatives. " ISO/IEC 27701 extends ISO/IEC
27001 for privacy (PIMS), and PCI DSS is a payment card security standard. Neither fits the described role.
Per ISO/IEC 27003:2017, it serves as a guide to support organizations in implementing an ISMS in accordance with ISO/IEC 27001 by offering rationale and explanation for each requirement.

QUESTION NO: 30
Nimbus Route, ein in den Niederlanden ansässiges Unternehmen für Cloud-basierte Logistikoptimierung, bietet KI-gestützte Routenplanung, Flottenmanagement-Tools und Echtzeit-Sendungsverfolgung für Kunden in ganz Europa und Nordamerika. Um sensible Logistikdaten zu schützen und die Ausfallsicherheit seiner Cloud-Dienste zu gewährleisten, hat Nimbus Route ein Informationssicherheits-Managementsystem (ISMS) gemäß ISO/IEC

27001 implementiert. Das Unternehmen integriert zudem intelligente Transportsysteme und prädiktive Analysen, um die betriebliche Effizienz und Nachhaltigkeit zu steigern. Im Rahmen der ISMS-Implementierung ermittelt das Unternehmen die erforderlichen Kompetenzniveaus für das ISMS-Management. Dabei wurden verschiedene Faktoren berücksichtigt, darunter technologische Fortschritte, regulatorische Vorgaben und die Unternehmensmission. Strategische Ziele, verfügbare Ressourcen sowie die Bedürfnisse und Erwartungen der Kunden stehen im Mittelpunkt der Unternehmensstrategie. Darüber hinaus hat das Unternehmen klare Richtlinien für die interne und externe Kommunikation im Zusammenhang mit dem Informationssicherheitsmanagementsystem (ISMS) festgelegt. Diese definieren, welche Informationen wann, mit wem und über welche Kanäle geteilt werden. Allerdings wurden nicht alle Kommunikationsvorgänge formal dokumentiert: Stattdessen klassifiziert und steuert das Unternehmen die Kommunikation bedarfsgerecht und stellt sicher, dass die Dokumentation nur in dem für die Effektivität des ISMS erforderlichen Umfang geführt wird. Um die wachsenden digitalen Dienste zu unterstützen und die operative Skalierbarkeit zu gewährleisten, nutzt Nimbus Route virtualisierte Rechenressourcen eines externen Cloud-Service-Providers. Diese Konfiguration ermöglicht es dem Unternehmen, seine Betriebssysteme zu konfigurieren und zu verwalten, Anwendungen bereitzustellen und Speicherumgebungen nach Bedarf zu steuern, während der Provider die zugrunde liegende Cloud-Umgebung wartet. Zur weiteren Verbesserung der Vorhersagefähigkeiten setzt Nimbus Route Machine-Learning-Verfahren in mehreren seiner Kerndienste ein. Konkret nutzt das Unternehmen Machine Learning zur Routenoptimierung und Lieferzeitprognose und verwendet dabei Algorithmen wie logistische Regression und Support Vector Machines, um Muster in historischen Transportdaten zu erkennen. Mit zunehmender Reife des ISMS von Nimbus Route hat sich das Unternehmen für einen schrittweisen Ansatz beim Übergang in den vollen Betriebsmodus entschieden. Anstatt auf einen formellen Start zu warten, werden einzelne Elemente des ISMS, wie z. B. Risikomanagementverfahren, Zugriffskontrollen und Audit-Protokollierung, schrittweise aktiviert, sobald sie entwickelt und genehmigt sind. Beantworten Sie anhand des obigen Szenarios die folgende Frage zur Bohrinsel.
Hat Nimbus Route die zur Unterstützung ihres ISMS erforderlichen Kompetenzniveaus angemessen ermittelt?

A. Ja, denn Nimbus Route hat nur die internen Faktoren berücksichtigt, die für den Betrieb am wichtigsten sind.

B. Nein, da Nimbus Route externe Aspekte, die für das ISMS relevant sind, nicht berücksichtigt hat.

C. Ja, denn Numbus Route berücksichtigte externe Gegebenheiten, interne Faktoren sowie die Bedürfnisse und Erwartungen relevanter Interessengruppen.

Answer: C

Explanation:
Nimbus Route appropriately determined the competence levels required to support its ISMS, making Option C the correct and verified answer.
ISO/IEC 27001:2022 requires organizations to define competence by considering both internal and external factors, as well as the needs and expectations of relevant interested parties. This requirement is explicitly addressed across several clauses.
Under Clause 7.2 - Competence, the standard requires the organization to:

"determine the necessary competence of person(s) doing work under its control that affects information security performance." Determining competence does not occur in isolation. It must be informed by:
Clause 4.1 - Understanding the organization and its context, which requires identification of internal and external issues relevant to the ISMS.
Clause 4.2 - Understanding the needs and expectations of interested parties, which includes customers, regulators, and partners.
The scenario clearly states that Nimbus Route considered:
Technological advancements (external/internal context),
Regulatory requirements (external issues),
Mission and strategic objectives (internal issues),
Available resources (internal capability),
Customer needs and expectations (interested parties).
This demonstrates full alignment with Clauses 4.1, 4.2, and 7.2.
Option A is incorrect because Nimbus Route did not consider only internal factors.
Option B is incorrect because the scenario explicitly states that external issues were considered.
Conclusion: Nimbus Route followed the ISO/IEC 27001:2022 requirements for determining competence in a comprehensive and context-aware manner. Therefore, Option C is 100% correct and verified.

QUESTION NO: 31
Welche Aussage zu organisatorischen Rollen, Verantwortlichkeiten und Befugnissen ist NICHT richtig?
A. Die oberste Leitung ist für die Berichterstattung über die Leistung des ISMS verantwortlich und kann diese Verantwortung nicht an jemand anderen delegieren.
B. Ein Projektmanager kann auch Verantwortung für die Informationssicherheit tragen
C. Die oberste Leitung muss die Verantwortung dafür übertragen, dass das ISMS der ISO/IEC 27001 entspricht.
Answer: A
Explanation:
Top management is responsible for ensuring that roles, responsibilities, and authorities for information security are assigned and communicated. While they are accountable for the performance of the ISMS, the responsibility for reporting on the performance of the ISMS can be delegated to others (e.g., ISMS manager, management representative), as explicitly stated in the standard.
"Top management shall assign the responsibility and authority for reporting on the performance of the ISMS to top management."
- ISO/IEC 27001:2022, Clause 5.3

QUESTION NO: 32
Ist die Entwicklung von Kommunikationsprotokollen durch Yefund akzeptabel?
A. Ja, denn die interne Kommunikation ist der wichtigste Faktor, der die Informationssicherheit beeinflusst.
B. Ja, da die externe Kommunikation für das ISMS nicht relevant ist

C. Nein, Yefund hätte die interne und externe Kommunikation festlegen sollen

Answer: C

Explanation:

ISO/IEC 27001:2022 Clause 7.4 requires that organizations determine both internal and external communications relevant to the ISMS. This includes what to communicate, when, with whom, and how, to ensure stakeholders-including clients and regulators-are properly informed. Focusing only on internal communications is noncompliant.

"The organization shall determine the need for internal and external communications relevant to the information security management system, including on what to communicate, when, with whom, and how."

- ISO/IEC 27001:2022, Clause 7.4

QUESTION NO: 33

NeuroTrustMed ist ein führendes Medizintechnikunternehmen mit Sitz in Seoul, Südkorea. Das Unternehmen ist auf die Entwicklung KI-gestützter Lösungen für die Neurobildgebung spezialisiert, die in der Früherkennung und Behandlungsplanung neurologischer Erkrankungen eingesetzt werden. Als datenintensives Unternehmen, das sensible Patientendaten und medizinische Forschungsdaten verarbeitet, legt NeuroTrustMed großen Wert auf Cybersicherheit und die Einhaltung gesetzlicher Bestimmungen. Das Unternehmen verfügt seit drei Jahren über ein nach ISO/IEC 27001 zertifiziertes Informationssicherheitsmanagementsystem (ISMS). Dieses wird kontinuierlich überprüft und verbessert, um aufkommenden Bedrohungen zu begegnen, Innovationen in der medizinischen Diagnostik zu fördern und das Vertrauen der Stakeholder zu erhalten. Im Rahmen seines Engagements für kontinuierliche Verbesserung verfolgt NeuroTrustMed aktiv potenzielle Abweichungen, führt Ursachenanalysen durch, implementiert Korrektur- und Präventivmaßnahmen und stellt sicher, dass alle Änderungen dokumentiert und mit den strategischen Zielen des Unternehmens abgestimmt werden. Als eine neue Datenschutzverordnung in Kraft trat, die die regionsübergreifende Datenverarbeitung betraf, führte das Informationssicherheitsteam eine Gap-Analyse zwischen den bestehenden Richtlinien und der neuen Verordnung durch. Anschließend wurden die relevanten Dokumentationen und Prozesse aktualisiert, um die Compliance zu gewährleisten. Nach diesen Überarbeitungen aktualisierte NeuroTrustMed die ISMS-Dokumentation und fügte einen neuen Eintrag im Verbesserungsregister hinzu. Das Register, das als strukturierte Tabelle geführt wurde, enthielt eine eindeutige Änderungsnummer, eine Beschreibung der Aktualisierung, eine Prioritätsklassifizierung aufgrund der Einhaltung gesetzlicher Bestimmungen, das Datum des Beginns und des Abschlusses sowie die Freigabe durch den Informationssicherheitsbeauftragten. Etwa zur gleichen Zeit identifizierte das Informationssicherheitsteam im Rahmen einer planmäßigen Managementprüfung ein Muster von Onboarding-Fehlern. Obwohl diese zu keinen Datenschutzverletzungen geführt hatten, stellten sie ein Risiko für unbefugten Zugriff dar. Daraufhin wurde das Onboarding-Verfahren überarbeitet und ein automatisierter Verifizierungsschritt hinzugefügt, um die Genauigkeit vor der Zugriffsgewährung sicherzustellen. Um die Ursache zu ermitteln, sammelte das Team Daten zum Bereitstellungsprozess. Es analysierte Prozessprotokolle, befragte Onboarding-Mitarbeiter und verfolgte Zugriffsfehler zurück zu einem falsch konfigurierten Schritt im Übergabeprozess zwischen Personalabteilung und IT. Das Team validierte diesen Befund

anhand von Testfällen, bevor Änderungen implementiert wurden. Nach der Bestätigung dokumentierte das Informationssicherheitsteam die Abweichung im ISMS-Protokoll. Die Dokumentation enthielt eine Beschreibung des Problems, der betroffenen Systeme und Benutzer sowie eine kurze Risikobewertung potenzieller Folgen im Zusammenhang mit der Zugriffsverwaltung. Beantworten Sie anhand des obigen Szenarios die folgende Frage.
Welche Maßnahmen hat NeuroTrustMed im Hinblick auf das identifizierte Muster bei Fehlern im Onboarding-Prozess für Benutzer ergriffen?
Siehe Szenario 9.

A. Korrektur

B. Korrekturmaßnahme

C. Vorbeugende Maßnahmen

Answer: B

Explanation:
In the scenario, NeuroTrustMed identified a pattern of onboarding errors that posed a risk of unauthorized access. Although no breach had yet occurred, the issue represented an existing nonconformity within the access provisioning process.
ISO/IEC 27001:2022 Clause 10.2 - Nonconformity and corrective action requires organizations to:
React to the nonconformity,
Determine the cause,
Implement actions to prevent recurrence.
NeuroTrustMed followed this process precisely:
Identified the issue,
Conducted root-cause analysis (misconfigured HR-to-IT handover),
Validated findings through testing,
Revised the onboarding procedure,
Added an automated verification step,
Documented the nonconformity with risk assessment.
This goes beyond a simple correction (Option A), which would only fix an isolated instance without addressing root cause. It is also not purely preventive action (Option C), because the nonconformity had already occurred.

QUESTION NO: 34

Nachdem sichergestellt war, dass die Angreifer keinen Zugriff auf ihr System hatten, beschlossen die Sicherheitsadministratoren, mit der forensischen Analyse fortzufahren. Sie kamen zu dem Schluss, dass ihr Zugriffssicherheitssystem nicht für die Erkennung von Bedrohungen ausgelegt war, einschließlich der Erkennung schädlicher Dateien, die mögliche zukünftige Angriffe auslösen könnten.
Auf Grundlage dieser Erkenntnisse beschloss Texas H$H Inc., sein Zugangssicherheitssystem zu ändern, um künftige Vorfälle zu vermeiden, und eine Richtlinie zum Vorfallmanagement in seine Informationssicherheitsrichtlinie zu integrieren, die den Mitarbeitern als Leitfaden für die Reaktion auf ähnliche Vorfälle dienen könnte.
Beantworten Sie basierend auf dem obigen Szenario die folgende Frage:
Welche in Szenario 7 beschriebene Situation weist darauf hin, dass Texas H&H Inc. eine Detektivkontrolle implementiert hat?

A. Texas H&H Inc. hat die Richtlinie zum Vorfallmanagement in seine Informationssicherheitsrichtlinie integriert

B. Texas H&H Inc. hat sein System auf bösartige Aktivitäten getestet und die Cloud-basierten E-Mail-Einstellungen überprüft

C. Texas H&H Inc. beauftragte einen Experten mit der Durchführung einer forensischen Analyse

Answer: C

QUESTION NO: 35

Welche Bereiche innerhalb der Organisation müssen auf Grundlage von ISO/IEC 27001 Regeln, Verfahren und Vereinbarungen für den Informationstransfer festlegen?

A. Interne Filesharing-Plattformen und freigegebene Laufwerke

B. Öffentliche und private Cloud-Dienste und Plattformen zur Zusammenarbeit mit Partnern

C. Alle Transfereinrichtungen innerhalb der Organisation

Answer: C