ISO-IEC-27001-Lead-Implementer日本語独学書籍 |素晴らしい合格率のISO-IEC-27001-Lead-Implementer: PECB Certified ISO/IEC 27001 Lead Implementer Exam | ISO-IEC-27001-Lead-Implementer問題集

BONUS！！！ Xhs1991 ISO-IEC-27001-Lead-Implementerダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1NcMqVaZeUpx6HIIRRCJneiMWVaKGg5Cg

Xhs1991はもっぱらPECBプロISO-IEC-27001-Lead-Implementer認証試験に関する知識を提供するのサイトで、ほかのサイト使った人はXhs1991が最高の知識源サイトと比較しますた。Xhs1991の商品はとても頼もしいISO-IEC-27001-Lead-Implementer試験の練習問題と解答は非常に正確でございます。

PECB ISO-IEC 27001-Lead-Implementer認定試験は、情報セキュリティ分野の幅広い知識と実践的な経験が必要な厳しい試験です。試験は、多肢選択問題、ケーススタディ、実技演習から構成され、ISO/IEC 27001標準の理解とISMSの実装と維持能力を試験します。試験に合格すると、IT及び情報セキュリティ業界で広く認知され尊敬されているPECB認定ISO/IEC 27001リードインプリメンター資格が授与されます。

>> ISO-IEC-27001-Lead-Implementer日本語独学書籍 <<

ISO-IEC-27001-Lead-Implementer試験の準備方法｜有難いISO-IEC-27001-Lead-Implementer日本語独学書籍試験｜最新のPECB Certified ISO/IEC 27001 Lead Implementer Exam問題集

人の職業の発展は彼の能力によって進めます。権威的な国際的な証明書は能力に一番よい証明です。PECBのISO-IEC-27001-Lead-Implementer試験の認証はあなたの需要する証明です。この試験に合格したいなら、よく準備する必要があります。Xhs1991の提供するPECBのISO-IEC-27001-Lead-Implementer試験の資料は経験の豊富なチームに整理されています。現在あなたもこのような珍しい資料を得られます。我々のウェブサイトであなたはPECBのISO-IEC-27001-Lead-Implementer試験のソフトを購入できます。

PECB Certified ISO/IEC 27001 Lead Implementer Exam 認定 ISO-IEC-27001-Lead-Implementer 試験問題 (Q159-Q164):

質問 # 159
What is the main difference between an audit program and an audit plan?

- A. An audit program outlines the activities and arrangements for a particular audit, while an audit plan provides an overarching framework for a series of audits with specific timelines and purposes
- B. An audit program outlines the overarching framework for a series of audits with specific timelines and purposes, while an audit plan outlines the activities and arrangements for a particular audit
- C. An audit program outlines policies, procedures, or requirements for reference in audit evidence comparison, while an audit

plan provides an overarching framework for a series of audits with specific timelines and purposes

正解：B

解説：
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

質問 # 160
Scenario:
An employee at Reyae Ltd unintentionally sent an email containing critical business strategies to a competitor due to an autofill email suggestion error. The email included proprietary trade secrets and confidential client dat a. Upon receiving the email, the competitor altered the information and attempted to use it to mislead clients into switching services.
Which of the following statements correctly describes the security principles affected in this situation?

- A. Reyae Ltd's confidentiality was compromised first, while the competitor's actions led to an integrity violation
- B. Reyae Ltd's integrity was compromised first, while the competitor's actions led to an availability violation
- C. Reyae Ltd's availability was compromised first, while the competitor's actions led to an integrity violation

正解：A

質問 # 161
Scenario 6: CB Consulting iS a reputable firm based in Dublin, Ireland. providing Strategic business Solutions to diverse clients, With a dedicated team Of professionals, CB Consulting prides itself on its commitment to excellence, integrity, and client satisfaction.
CB Consulting started implementing an ISMS aligned with ISOflEC 27001 as part of its ongoing commitment to enhancing its information security practices. Throughout this process, ensuring effective communication and adherence to establi Shed security protocols is essential.
Sarah, an employee at CB has been appointed as the head Of a new project focused on managing sensitive client data, Additionally, she is responsible for Overseeing activities during the response phase of incident management, including regular reporting to the incident manager of the incident management team and keeping key stakeholders informed. Meanwhile, CB Consulting has reassigned Tom to serve as the company's legal consultant.
CB Consulting has also reassigned Clare. formerly an IT security analyst, as their information security officer to oversee the implementation Of the ISMS and ensure compliance with ISO/IEC 27001. Clare's primary responsibility iS to conduct regular risk assessments. identlfy potential vulnerabilities, and implement appropriate Security measures to mitigate risks effectively. Clare has established a procedure Stating that information security risk assessments are conducted only when significant changes occur. playing a crucial role in strengthening the companys security posture and safeguarding against potential threats.
TO ensure it has a Competent workforce to meet information security Objectives, CB Consulting has implemented a process to and verify that all employees, including Sarah, Tom, and Clare, possess the necessary competence based on their education. training, or experience. Where gaps were identified, the company has taken specific actions such as providing additional training and mentoring. Additionally, CB Consulting retains documented information as evidence of the competencies requ.red and acquired.
CB Consulting has established a robust communication strategy aligned with industry standards to ensure secure and effective information exchange. It identified the requirements for communication on relevant issues. First, the company designated specific toles. Such as a public relations officer for external communication and a Security officer for internal matters, to manage sensitive issues like data breaches. Then.
communication triggers, content. and recipients were carefully defined. with messages pre-approved by management where necessary. Lastly, dedicated channels were implemented to ensure the confidentiality and integrity of transmitted information.
Based on the scenario above, answer the following question.
CB Consulting prioritizes transparent and Substantive communication practices to foster trust, enhance Stakeholder engagement, and reinforce its commitment to information security excellence. Which principle of effective communication is emphasized by this approach?
Transparency
CB Consulting prioritizes transparent and substantive communication practices to foster trust, enhance stakeholder engagement, and reinforce its commitment to information security excellence. Which principle of effective communication is emphasized by this approach?

- A. Clarity

- B. Timeliness
- C. Transparency

正解：C

解説：
Transparent communication involves openly sharing relevant information, fostering trust, and enhancing stakeholder engagement. ISO/IEC 27001:2022 (and ISO/IEC 27003:2017, Clause 8.6) emphasize transparency as a best practice in both internal and external communication to reinforce organizational trust and security culture.
"Transparent communication ensures that all relevant information is available to stakeholders, enhancing trust and supporting the objectives of information security."
- ISO/IEC 27001:2022, Clause 7.4; ISO/IEC 27003:2017, Clause 8.6

質問 # 162
Diana works as a customer service representative for a large e-commerce company. One day, she accidently modified the order details of a customer without their permission Due to this error, the customer received an incorrect product. Which information security principle was breached in this case7

- A. Integrity
- B. Availability
- C. Confidentiality

正解：A

解説：
According to ISO/IEC 27001:2022, information security controls are measures that are implemented to protect the confidentiality, integrity, and availability of information assets1. Controls can be preventive, detective, or corrective, depending on their purpose and nature2. Preventive controls aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Detective controls aim to detect or discover the occurrence of a security incident or its symptoms. Corrective controls aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact2.
In this scenario, Socket Inc. implemented several security controls to prevent information security incidents from recurring, such as:
Segregation of networks: This is a preventive and technical control that involves separating different parts of a network into smaller segments, using devices such as routers, firewalls, or VPNs, to limit the access and communication between them3. This can enhance the security and performance of the network, as well as reduce the administrative efforts and costs3.
Privileged access rights: This is a preventive and administrative control that involves granting access to information assets or systems only to authorized personnel who have a legitimate need to access them, based on their roles and responsibilities4. This can reduce the risk of unauthorized access, misuse, or modification of information assets or systems4.
Cryptographic controls: This is a preventive and technical control that involves the use of cryptography, which is the science of protecting information by transforming it into an unreadable format, to protect the confidentiality, integrity, and authenticity of information assets or systems. This can prevent unauthorized access, modification, or disclosure of information assets or systems.
Information security threat management: This is a preventive and administrative control that involves the identification, analysis, and response to information security threats, which are any incidents that could negatively affect the confidentiality, integrity, or availability of information assets or systems. This can help the organization to anticipate, prevent, or mitigate the impact of information security threats.
Information security integration into project management: This is a preventive and administrative control that involves the incorporation of information security requirements and controls into the planning, execution, and closure of projects, which are temporary endeavors undertaken to create a unique product, service, or result. This can ensure that information security risks and opportunities are identified and addressed throughout the project life cycle.
However, information backup is not a preventive control, but a corrective control. Information backup is a corrective and technical control that involves the creation and maintenance of copies of information assets or systems, using dedicated software and utilities, to ensure that they can be recovered in case of data loss, corruption, accidental deletion, or cyber incidents. This can help the organization to restore the normal state of information assets or systems after a security incident or mitigate its impact. Therefore, information backup does not prevent information security incidents from recurring, but rather helps the organization to recover from them.
Reference:
ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements ISO 27001 Key Terms - PJR Network Segmentation: What It Is and How It Works | Imperva ISO 27001:2022 Annex A 8.2 - Privileged Access Rights - ISMS.online
[ISO 27001:2022 Annex A 8.3 - Cryptographic Controls - ISMS.online]
[ISO 27001:2022 Annex A 5.30 - Information Security Threat Management - ISMS.online]

[ISO 27001:2022 Annex A 5.31 - Information Security Integration into Project Management - ISMS.online]
[ISO 27001:2022 Annex A 8.13 - Information Backup - ISMS.online]

質問 # 163
Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management
[