PECB

ISO-IEC-27001-Lead-Implementer

PECB Certified ISO/IEC 27001 : 2022 Lead Implementer exam

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

Latest Version: 14.1

Question: 1

Has Bytes determined all the relevant factors that impact its ability to achieve the intended outcomes of its ISMS, in accordance with clause 4.1 "Understanding the organization and its context" of ISO/IEC 27001?

A. No, the company did not determine which requirements of interested parties will be addressed through the ISMS
B. Yes, the company determined all the relevant issues to its purpose that affect its ability to achieve the intended outcomes
C. No, the company did not determine whether climate change is a relevant issue

Answer: B

Explanation:
Bytes identified both external and internal issues relevant to its purpose and that impact its ability to achieve the intended ISMS outcomes, including social, cultural, political, legal, financial, technological, and other factors, as well as internal aspects like culture, policies, resources, infrastructure, etc. This approach fully aligns with ISO/IEC 27001:2022 Clause 4.1, which requires organizations to determine both internal and external issues relevant to the ISMS.
“The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.”
— ISO/IEC 27001:2022, Clause 4.1

Question: 2

Nimbus Route, a cloud-native logistics optimization company based in the Netherlands, offers Al-driven route planning fleet management tools, and real time shipment tracking solutions to clients across Europe and North America. To safeguard sensitive logistics data and ensure resilience across its cloud services. Nimbus Route has implemented an information security management system (ISMS) based on ISO/IEC 27001. The company is also integrating intelligent transport systems and predictive analytics to increase operational efficiency and sustainability. As part of the ISMS implementation process, the company is determining the competence levels required to manage its ISMS. It has considered various factors when defining these competence requirements, including technological advancements, regulatory requirements, the company's mission. strategic objectives, available resources. as well as the needs and expectations of its customers. Furthermore, the company has established clear guidelines for internal and external

communication related to the ISMS, defining what information to share, when to share it. with whom, and through which channels. However, not all communications have been formally documented: instead, the company classified and managed communication based on its needs. ensuring that documentation is maintained only to the extent necessary for the ISMS's effectiveness To support its expanding digital services and ensure operational scalability. Nimbus Route utilizes virtualized computing resources provided by an external cloud service provider. This setup allows the company to configure and manage its operating systems, deploy applications. and control storage environments as needed while relying on the provider to maintain the underlying cloud environment. To further enhance is predictive capabilities. Nimbus Route is adopting machine learning techniques across several of its core services Specifically, it uses machine learning for route optimization and delivery time estimation, leveraging algorithms such as logistic regression and support vector machines to identify patterns in historical transportation data. As Nimbus Route's ISMS matures, the company has chosen a chased approach to its transition into full operational mode Rather than waiting for a formal launch, individual elements of the ISMS, such as risk treatment procedures, access controls, and audit logging, are being activated progressively as soon as they are developed and approved Based on the scenario above answer the following question.
Which type of machine learning is Nimbus Route using to enhance its delivery and scheduling accuracy? Refer to scenario 6.

A. Reinforcement learning
B. Supervised learning
C. Unsupervised learning

Answer: B

Explanation:
The correct answer is B. Supervised learning, based on the explicit machine learning techniques described in the scenario.
Nimbus Route uses logistic regression and support vector machines (SVMs) to analyze historical transportation data and improve route optimization and delivery time estimation. These algorithms are classic supervised learning techniques, which rely on labeled datasets to learn relationships between input variables and known outcomes.
In supervised learning:
Input data is paired with correct outputs (labels),
Models are trained to predict outcomes based on historical examples,
Accuracy improves through evaluation against known results.
This exactly matches the scenario's description of learning from historical transportation data to predict delivery times and optimize routes.
Reinforcement learning (Option A) involves learning through trial-and-error interactions with an environment and reward signals, which is not described.
Unsupervised learning (Option C) focuses on discovering hidden patterns in unlabeled data, such as clustering, which is also not indicated.
While ISO/IEC 27001:2022 does not prescribe machine learning types, its risk-based approach (Clause 6.1) and emphasis on technology awareness (Clause 7.2) require organizations to understand and competently manage the technologies they deploy—including AI and ML systems.

By clearly identifying and competently applying supervised learning techniques, Nimbus Route demonstrates appropriate technological understanding and governance within its ISMS.

Question: 3

Which of the following processes may involve increasing risk in order to pursue an opportunity?

A. Risk analysis
B. Risk treatment
C. Risk identification

Answer: B

Explanation:

Question: 4

A manufacturing company faced a risk of production delays due to potential supply chain disruptions. After assessing the potential impact of the risk, the company decided to accept the risk, considering the disruption unlikely to significantly affect its operations. Which risk treatment option did the company select in this case?

A. Risk avoidance
B. Risk retention
C. Risk deflection

Answer: B

Explanation:
Risk retention means accepting the risk, either knowingly or by default, often because it is deemed acceptable or cost-effective compared to the mitigation effort. In this scenario, the company assessed the risk and decided to accept it, which is classic risk retention.
“Risk retention involves knowingly accepting a risk. Risk retention can be a conscious decision based on risk assessment.”
— ISO/IEC 27001:2022, Clause 6.1.3, ISO/IEC 27005:2022, Section 8.3.2

Question: 5

Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.

Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization’s topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.

The company also implemented a control to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. The implementation was based on all relevant agreements, legislation, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.

Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.

Based on the scenario above, answer the following question:

Based on scenario 3, did Socket Inc. comply with ISO/IEC 27001 organizational controls regarding its operating procedures?

A. Yes, it did comply with ISO/IEC 27001 requirements

B. No, operating procedures for information processing facilities should have been specifically provided to personnel who require them

C. No, operating procedures for information processing facilities should have been exclusively available to the Information Technology Department or a similar unit within the company

Answer: A

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/