VirtuLearn

TRUSTED, ACCURATE AND RELIABLE!

The most comprehensive IT certification preparation materials in the industry!

https://www.virtulearner.com
support@virtulearner.com

PECB

ISO-IEC-27005-Risk-Manager

PECB Certified ISO/IEC 27005 Risk Manager

QUESTION: 1
Can organizations obtain certification against ISO 31000?

A. Yes, organizations of any type or size can obtain certification against ISO 31000
B. Yes, but only organizations that manufacture products can obtain an ISO 31000 certification
C. [No, organizations cannot obtain certification against ISO 31000, as the standard provides only guidelines

Answer(s): C

Explanation:
ISO 31000 is an international standard that provides guidelines for risk management. It is a framework that helps organizations develop a risk management strategy to effectively manage risk, taking into consideration their specific contexts. However, ISO 31000 is not designed to be used as a certifiable standard; instead, it offers principles, a framework, and a process for managing risk. Unlike other ISO standards, such as ISO/IEC 27001 for information security management systems, which are certifiable, ISO 31000 does not have a certification process because it does not specify any requirements that an organization must comply with. Therefore, option C is the correct answer because ISO 31000 is intended to provide guidelines and is not certifiable.

QUESTION: 2
Which of the following statements best defines information security risk?

A. The potential that threats will exploit vulnerabilities of an information asset and cause harm to an organization
B. Weakness of an asset or control that can be exploited by one or a group of threats
C. Potential cause of an unwanted incident related to information security that can cause harm to an organization

Answer(s): A

Explanation:
Information security risk, as defined by ISO/IEC 27005, is "the potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization." This definition emphasizes the interplay between threats (e.g., cyber attackers, natural disasters),

vulnerabilities (e.g., weaknesses in software, inadequate security controls), and the potential impact or harm that could result from this exploitation. Therefore, option A is the most comprehensive and accurate description of information security risk. In contrast, option B describes a vulnerability, and option C focuses on the cause of an incident rather than defining risk itself. Option A aligns directly with the risk definition in ISO/IEC 27005.

QUESTION: 3
Scenario:
The risk assessment process was led by Henry, Bontton's risk manager. The first step that Henry took was identifying the company's assets. Afterward, Henry created various potential incident scenarios. One of the main concerns regarding the use of the application was the possibility of being targeted by cyber attackers, as a great number of organizations were

experiencing cyberattacks during that time. After analyzing the identified risks, Henry evaluated them and concluded that new controls must be implemented if the company wants to use the application. Among others, he stated that training should be provided to personnel regarding the use of the application and that awareness sessions should be conducted regarding the importance of protecting customers' personal data. Lastly, Henry communicated the risk assessment results to the top management. They decided that the application will be used only after treating the identified risks.
Based on the scenario above, answer the following question:
Bontton established a risk management process based on ISO/IEC 27005, to systematically manage information security threats. Is this a good practice?

A. Yes, ISO/IEC 27005 provides guidelines for information security risk management that enable organizations to systematically manage information security threats
B. Yes, ISO/IEC 27005 provides guidelines to systematically manage all types of threats that organizations may face
C. No, ISO/IEC 27005 cannot be used to manage information security threats in the food sector

Answer(s): A

Explanation:
ISO/IEC 27005 is the standard that provides guidelines for information security risk management, which supports the requirements of an Information Security Management System (ISMS) as specified in ISO/IEC 27001. In the scenario provided, Bontton established a risk management process to identify, analyze, evaluate, and treat information security risks, which is in alignment with the guidelines set out in ISO/IEC 27005. The standard emphasizes a systematic approach to identifying assets, identifying threats and vulnerabilities, assessing risks, and implementing appropriate risk treatment measures, such as training and awareness sessions. Thus, option A is correct, as it accurately reflects the purpose and application of ISO/IEC 27005 in managing information security threats. Option B is incorrect because ISO/IEC 27005 specifically addresses information security threats, not all types of threats, and option C is incorrect because ISO/IEC 27005 is applicable to any sector, including the food industry, as long as it concerns information security risks.

QUESTION: 4
Scenario:

The risk assessment process was led by Henry, Bontton's risk manager. The first step that Henry took was identifying the company's assets. Afterward, Henry created various potential incident scenarios. One of the main concerns regarding the use of the application was the possibility of being targeted by cyber attackers, as a great number of organizations were experiencing cyberattacks during that time. After analyzing the identified risks, Henry evaluated them and concluded that new controls must be implemented if the company wants to use the application. Among others, he stated that training should be provided to personnel regarding the use of the application and that awareness sessions should be conducted regarding the importance of protecting customers' personal data. Lastly, Henry communicated the risk assessment results to the top management. They decided that the application will be used only after treating the identified risks. Based on scenario 1, Bontton used ISO/IEC 27005 to ensure effective implementation of all ISO/IEC 27001 requirements. Is this appropriate?