KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

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

Title : PECB Certified ISO/IEC 27001 Lead Implementer exam

Version : DEMO

1.Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the involved parties, including parents, other physicians, and the medical laboratory staff.
Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Based on the scenario above, answer the following question:
Which of the following indicates that the confidentiality of information was compromised?
A. Service interruptions due to the increased number of users
B. Invasion of patients' privacy
C. Modification of patients' medical reports
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 security management systems — Requirements, clause 3.14.

2.Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff.
Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Based on scenario 1. what is a potential impact of the loss of integrity of information in HealthGenic?

A. Disruption of operations and performance degradation
B. Incomplete and incorrect medical reports
C. Service interruptions and complicated user interface
Answer: B
Explanation:
The loss of integrity of information in HealthGenic means that the information was modified or corrupted in an unauthorized or improper way, resulting in inaccurate, incomplete, or unreliable data. This can have a serious impact on the quality and safety of the medical services provided by HealthGenic, as well as the trust and satisfaction of the patients and their families. In particular, incomplete and incorrect medical reports can lead to:
Misdiagnosis or delayed diagnosis of the patients' conditions, which can affect their treatment and recovery.
Prescription of wrong or inappropriate medications or dosages, which can cause adverse effects or interactions.
Violation of the patients' privacy and confidentiality, which can expose them to identity theft, fraud, or discrimination.
Legal liability and reputational damage for HealthGenic, which can result in lawsuits, fines, or loss of customers.
Therefore, it is essential for HealthGenic to ensure the integrity of its information by implementing appropriate security controls and measures, such as encryption, authentication, backup, audit, and incident response.
ISO/IEC 27001:2022 Lead Implementer Course Guide1
ISO/IEC 27001:2022 Lead Implementer Info Kit2
ISO/IEC 27001:2022 Information Security Management Systems - Requirements3
ISO/IEC 27002:2022 Code of Practice for Information Security Controls4

3.Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff.
Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Intrinsic vulnerabilities, such as the_____ are related to the characteristics of the asset.
Refer to scenario 1.
A. Software malfunction
B. Service interruptions
C. Complicated user interface

Answer: C
Explanation:
Intrinsic vulnerabilities are related to the characteristics of the asset that make it susceptible to threats, regardless of the presence or absence of controls. In scenario 1, the complicated user interface of the web-based medical software is an intrinsic vulnerability, as it is a feature of the software that makes it difficult to use and increases the likelihood of human errors. The software malfunction and the service interruptions are not intrinsic vulnerabilities, but rather incidents that occurred due to external factors, such as the increased number of users or the software company's actions.
ISO/IEC 27001:2022 Lead Implementer Course Content, Module 6: Risk Assessment and Treatment1; ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection, Clause 6.1.2: Information security risk assessment2

4.Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff.
Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Which situation described in scenario 1 represents a threat to HealthGenic?
A. HealthGenic did not train its personnel to use the software
B. The software company modified information related to HealthGenic's patients
C. HealthGenic used a web-based medical software for storing patients' confidential information
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 — Information security management systems — Requirements ISO 27001 Key Terms - PJR

5.Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and

communicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff.

Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use. The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.

In scenario 1, HealthGenic experienced a number of service interruptions due to the loss of functionality of the software.

Which principle of information security has been affected in this case?

A. Availability

B. Confidentiality

C. Integrity

Answer: A

Explanation:

Availability of information is the property of being accessible and usable upon demand by an authorized entity. In other words, availability ensures that the information and the systems that support it are always ready for use when needed. In the scenario, the availability of information was affected when HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software. This means that the software was not able to handle the demand and provide the required functionality to the users. Therefore, the correct answer is A.

: ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements, clause 3.13.