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 : **IT Risk Fundamentals**

Title : IT Risk Fundamentals CertificateExam

Version : DEMO

1.Which of the following is considered an exploit event?
A. An attacker takes advantage of a vulnerability
B. Any event that is verified as a security breach
C. The actual occurrence of an adverse event
Answer: A
Explanation:
Ein Exploit-Ereignis tritt auf, wenn ein Angreifer eine Schwachstelle ausnutzt, um unbefugten Zugang zu einem System zu erlangen oder es zu kompromittieren. Dies ist ein grundlegender Begriff in der IT-Sicherheit. Wenn ein Angreifer eine bekannte oder unbekannte Schwachstelle in einer Software, Hardware oder einem Netzwerkprotokoll erkennt und ausnutzt, wird dies als Exploit bezeichnet.
Definition und Bedeutung:
Ein Exploit ist eine Methode oder Technik, die verwendet wird, um Schwachstellen in einem System auszunutzen.
Schwachstellen können Softwarefehler, Fehlkonfigurationen oder Sicherheitslücken sein.
Ablauf eines Exploit-Ereignisses:
Identifizierung der Schwachstelle: Der Angreifer entdeckt eine Schwachstelle in einem System.
Entwicklung des Exploits: Der Angreifer entwickelt oder verwendet ein bestehendes Tool, um die Schwachstelle auszunutzen.
Durchführung des Angriffs: Der Exploit wird durchgeführt, um unautorisierten Zugang zu erlangen oder Schaden zu verursachen.
Reference: ISA 315: Generelle IT-Kontrollen und die Notwendigkeit, Risiken aus dem IT-Einsatz zu identifizieren und zu behandeln.
IDW PS 951: IT-Risiken und Kontrollen im Rahmen der Jahresabschlussprüfung, die die Notwendigkeit von Kontrollen zur Identifizierung und Bewertung von Schwachstellen unterstreicht.

2.Potential losses resulting from employee errors and system failures are examples of:
A. operational risk.
B. market risk.
C. strategic risk.
Answer: A
Explanation:
Operationelle Risiken umfassen Verluste, die durch unzureichende oder fehlgeschlagene interne Prozesse, Personen und Systeme oder durch externe Ereignisse verursacht werden. Mitarbeiterfehler und Systemausfälle sind typische Beispiele für operationelle Risiken.
Definition und Kategorien von Risiken:
Operational Risk: Betrifft Verluste aufgrund interner Prozesse oder menschlicher Fehler.
Market Risk: Verluste aufgrund von Marktschwankungen.
Strategic Risk: Verluste aufgrund von Fehlentscheidungen im Management oder strategischen Planungsfehlern.
Beispiele für operationelle Risiken:
Mitarbeiterfehler: Fehlerhafte Dateneingabe, Nichtbeachtung von Arbeitsprozessen. Systemausfälle: IT-Systemabstürze, Hardware-Fehlfunktionen.
Reference: ISA 315: Operational risks and how they are identified and managed within the IT environment.

ISO 27001: Information security management systems that include measures for mitigating operational risks.

3.Which of the following would be considered a cyber-risk?
A. A system that does not meet the needs of users
B. A change in security technology
C. Unauthorized use of information
Answer: C
Explanation:
Cyber-Risiken betreffen Bedrohungen und Schwachstellen in IT-Systemen, die durch unbefugten Zugriff oder Missbrauch von Informationen entstehen. Dies schließt die unautorisierte Nutzung von Informationen ein.
Definition und Beispiele:
Cyber Risk: Risiken im Zusammenhang mit Cyberangriffen, Datenverlust und Informationsdiebstahl.
Unauthorized Use of Information: Ein Beispiel für ein Cyber-Risiko, bei dem unbefugte Personen Zugang zu vertraulichen Daten erhalten.
Schutzmaßnahmen:
Zugriffskontrollen: Authentifizierung und Autorisierung, um unbefugten Zugriff zu verhindern.
Sicherheitsüberwachung: Intrusion Detection Systems (IDS) und regelmäßige Sicherheitsüberprüfungen.
Reference: ISA 315: Importance of IT controls in preventing unauthorized access and use of information.
ISO 27001: Framework for managing information security risks, including unauthorized access.

4.Which of the following is the BEST way to interpret enterprise standards?
A. A means of implementing policy
B. An approved code of practice
C. Documented high-level principles
Answer: A
Explanation:
Unternehmensstandards dienen als Mittel zur Umsetzung von Richtlinien. Sie legen spezifische Anforderungen und Verfahren fest, die sicherstellen, dass die Unternehmensrichtlinien eingehalten werden.
Definition und Bedeutung von Standards:
Enterprise Standards: Dokumentierte, detaillierte Anweisungen, die die Umsetzung von Richtlinien unterstützen.
Implementierung von Richtlinien: Standards helfen dabei, die abstrakten Richtlinien in konkrete, umsetzbare Maßnahmen zu überführen.
Beispiele und Anwendung:
IT-Sicherheitsstandards: Definieren spezifische Sicherheitsanforderungen, die zur Einhaltung der übergeordneten IT-Sicherheitsrichtlinien erforderlich sind.
Compliance-Standards: Stellen sicher, dass gesetzliche und regulatorische Anforderungen eingehalten werden.
Reference: ISA 315: Role of IT controls and standards in implementing organizational policies.
ISO 27001: Establishing standards for information security management to support policy implementation.

5.Which of the following is the MAIN objective of governance?
A. Creating controls throughout the entire organization
B. Creating risk awareness at all levels of the organization
C. Creating value through investments for the organization
Answer: C
Explanation:
Governance is primarily concerned with ensuring that an organization achieves its objectives, operates efficiently, and adds value to its stakeholders. The main objective of governance is to create value through investments for the organization. This encompasses making strategic decisions that align with the organization's goals, ensuring that resources are used effectively, and that the organization's activities are sustainable and provide long-term benefits. While creating controls and risk awareness are essential aspects of governance, they serve the broader goal of value creation through strategic investments. This concept is aligned with principles found in corporate governance frameworks and standards such as ISO/IEC 38500 and COBIT (Control Objectives for Information and Related Technologies).