



TRUSTED, ACCURATE AND RELIABLE!

The most comprehensive IT certification
preparation materials in the industry!

All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, reselling, or distribution of this document is strictly prohibited and may result in legal action.

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

Isaca

IT-Risk-Fundamentals

IT Risk Fundamentals

Certificate

QUESTION: 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(s): A

Explanation:

An exploit event occurs when an attacker exploits a vulnerability to gain unauthorized access to or compromise a system. This is a fundamental term in IT security. When an attacker detects and exploits a known or unknown vulnerability in a software, hardware, or network protocol, it is called an exploit.

Definition and Meaning:

An exploit is a method or technique used to exploit vulnerabilities in a system.

Sequence of an exploit event:

Vulnerability identification: The attacker discovers a vulnerability in a system. Evolution of the exploit: The attacker develops or uses an existing tool to exploit the vulnerability.

or cause damage.

Reference:

ISA 315: General IT controls and the need to identify and address risks from IT deployment.

underlines the need for controls to identify and assess vulnerabilities.

QUESTION: 2

Potential losses resulting from employee errors and system failures are examples of:

- A. operational risk.
- B. market risk.
- C. strategic risk.

Answer(s): A

Explanation:

Operational risks include losses caused by inadequate or failed internal processes, people, and systems, or by external events. Employee error

Definition and categories of risks:

Operational Risk: Concerns losses due to internal processes or human error.

Market Risk: Losses due to market fluctuations.

Strategic risk: Losses due to bad management decisions or strategic planning errors.

Employee error: Incorrect data entry, non-observance of work processes.

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.

QUESTION: 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(s): C

Explanation:

Cyber risks relate to threats and vulnerabilities in IT systems that are exposed by unauthorized information.

Definition and examples:

Cyber Risk: Risks related to cyber attacks, data loss, and information theft.

Gain access to confidential data.

Access controls: Authentication and authorization to prevent unauthorized access.

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.

QUESTION: 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
- Q Documented high-level principles

Answer(s): A

Explanation:

Corporate standards serve as a means of implementing policies. They establish specific requirements and procedures that ensure that company policies are adhered to.

Definition and meaning of standards:

Enterprise Standards: Documented, detailed instructions that guide policy enforcement.

Implementation of guidelines: Standards help to translate the abstract guidelines into concrete,

Examples and application:

IT security standards: Define specific security requirements that are required to comply with the