Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/28/2022 8:55:16 am • Time spent: 02:49

Score: 30%

Passing Score: 80%

▼ Question 1: ✕ Incorrect

Which of the following are control categories? (Select three.)

- □ Preventative
- ➡ □ Managerial
- ☑ ~~Physical~~
- ☑ ~~Deterrent~~
- ➡ □ Operational
- □ Compensating
- ➡ ☑ Technical

EXPLANATION

Control categories are:

- Managerial controls (consist of management techniques and administrative procedures)
- Operational controls (performed everyday by the security team)
- Technical controls (based around software, applications, and security appliances)

The remaining items are all control types. Control types consist of different strategies to prevent, detect, mitigate, and correct any network breach.

REFERENCES

14.2.2 Control Categories and Types Facts

q_ctrl_cattypes_categories_secp7.question.fex

Question 2: ✓ Correct

Which of the following BEST describes compensating controls?

- ➡ ● Partial control solution that is implemented when a control cannot fully meet a requirement.
- ○ Discourages malicious actors from attempting to breach a network.
- ○ Monitors network activity and informs the security team of a potential security event.
- ○ Attempts to fix any controls that aren't working properly.

EXPLANATION

Compensating controls are a partial control solution that is implemented when a control cannot fully meet a requirement.

Detective controls monitor network activity and inform the security team of a potential security event.

Corrective controls attempt to fix any controls that aren't working properly.

Deterrent controls discourage malicious actors from attempting to breach a network.

REFERENCES

14.2.2 Control Categories and Types Facts

q_ctrl_cattypes_compensating_secp7.question.fex

Question 3: ✕ Incorrect

Which type of control is used to discourage malicious actors from attempting to breach a network?

- ● ~~Preventative~~
- ➡ ○ Deterrent
- ○ Detective
- ○ Physical

EXPLANATION

The deterrent control type discourages malicious actors from trying to breach a network. The more deterrents are implemented, the less likely it is that anyone tries. These could include internal security policies, access-protected doors for a server room, entry-point access restriction, biometric sensors, man traps, security cameras, security training, and security guards.

Detective controls monitor network activity and inform the security team of a potential security event. Detective controls also log activities and provide artifacts to help investigate the event. Intrusion detection systems are an example of detective controls.

Physical deterrents keep unauthorized people from physically accessing a company's assets. Locked doors, proximity cards, fences, cameras, and guards are all ways to physically protect a network.

Preventative controls, such as an IPS, are used to prevent security breaches.

REFERENCES

14.2.2 Control Categories and Types Facts

q_ctrl_cattypes_deterrent_secp7.question.fex

▼ **Question 4:** ✕ Incorrect

Which type of control makes use of policies, DPRs, and BCPs?

- ○ Preventative
- ➡ ○ Managerial
- ○ Technical
- ● ~~Operational~~

EXPLANATION

Managerial controls consist of management techniques and administrative procedures. These can include security policies, hiring policies, disaster recovery plans (DPRs), and business continuity plans (BCPs).

Operational controls are ones that the security team performs daily.

Technical controls are based around software, applications, and security appliances.

Preventative controls, such as an IPS, are used to prevent security breaches.

REFERENCES

14.2.2 Control Categories and Types Facts

q_ctrl_cattypes_managerial_secp7.question.fex

Question 5: ✕ Incorrect

Which of the following is an example of a preventative control type?

○ Network monitoring applications

○ Real-time monitoring alerts

➡ ○ An advanced network appliance

● ~~Intrusion detection systems~~

EXPLANATION

The easiest prevention control is an advanced network appliance, which is sometimes called an adaptive security appliance (ASA).

Examples of detective controls are intrusion detection systems (ISPs), network monitoring applications, collectors logs, and real-time monitoring alerts.

REFERENCES

14.2.2 Control Categories and Types Facts

q_ctrl_cattypes_preventitve_secp7.question.fex

▾ **Question 6:** ✕ Incorrect

Which ISO publication lays out guidelines for selecting and implementing security controls?

○ 31000

○ 27701

➡ ○ 27002

● ~~27001~~

EXPLANATION

Publication 27002 lays out guidelines for selecting and implementing security controls.

ISO 27001 is the publication that covers implementing and improving a security management system as well as an assessment guideline.

31000 covers risk management as it pertains to business continuity, safety, environmental results, and the professional reputation of a company.

ISO 27701 covers establishing, implementing, and improving a privacy information management system.

REFERENCES

14.2.4 Security Frameworks Facts

q_sec_frmwk_27002_secp7.question.fex

Question 7: ✗ Incorrect

Which of the following frameworks introduced the first cloud-centric individual certification?

- ➡ ○ CSA
- ○ ISO
- ● ~~NIST~~
- ○ CCM

EXPLANATION

The Cloud Security Alliance (CSA) is a relatively new, ten-year-old security framework. With the exponential growth of cloud computing, the need for a cloud security framework was crucial. Along with best practices in cloud security, CSA also introduced the first cloud-centric individual certification.

The Cloud Control Matrix (CCM) is a guide to assist prospective cloud users in evaluating a cloud provider's security risk.

The National Institute of Standards and Technology (NIST) is one of the largest security frameworks. It is used by the federal government and all its departments, including the Department of Defense.

The International Organization for Standardization (ISO) is a worldwide organization that is currently the standardizing body in 164 different countries.

REFERENCES

14.2.4 Security Frameworks Facts

q_sec_frmwk_csa_secp7.question.fex

▼ **Question 8:** ✕ Incorrect

Which type of report is used for marketing and letting future partners know that compliance has been met?

- ○ ISO 27001
- ● ~~SOC Type II~~
- ➡ ○ SOC Type III
- ○ ISO 31000

EXPLANATION

A SOC Type III report is a non-detailed report attesting to a company's compliance. This type of report is used for marketing and letting future partners know that compliance has been met.

A SOC Type II report focuses on predetermined controls that are audited and a detailed report that attests to the company's compliance.

ISO 27001 is the publication that covers implementing and improving a security management system as well as an assessment guideline.

ISO 31000 covers risk management as it pertains to business continuity, safety, environmental results, and the professional reputation of a company.

REFERENCES

14.2.4 Security Frameworks Facts

q_sec_frmwk_iso_secp7.question.fex

Question 9: ✓ Correct

Which of the following security frameworks is used by the federal government and all its departments, including the Department of Defense?

○ CSA

➡ ● NIST

○ ISO

○ SOC Type II/III

EXPLANATION

The National Institute of Standards and Technology (NIST) is one of the largest security frameworks. It is used by the federal government and all its departments, including the Department of Defense. Security is one of the many verticals that NIST provides guidance for, and NIST's cybersecurity frameworks are the gold standard.

The International Organization for Standardization (ISO) is a worldwide organization that is currently the standardizing body in 164 different countries.

The System and Organization Controls (SOC) is made up of controls and has three types of reports that help a third party determine (through an audit) how a company is adhering to systems and controls.

The Cloud Security Alliance (CSA) is a relatively new, ten-year-old security framework that focuses on cloud security.

REFERENCES

14.2.4 Security Frameworks Facts

q_sec_frmwk_nist_secp7.question.fex

▼ Question 10: ✓ Correct

Which SOC type reports focus on predetermined controls that are audited and a detailed report that attests to a company's compliance?

➡ ● II

○ III

○ I

○ IV

EXPLANATION

An SOC Type I report is an attestation of controls at an organization for a specific point in time.

An SOC Type II report focuses on predetermined controls that are audited and a detailed report that attests to a company's compliance.

An SOC Type III report is a non-detailed report attesting to a company's compliance. This type of report is used for marketing and letting future partners know that compliance has been met.

There is no SOC Type IV.

REFERENCES

14.2.4 Security Frameworks Facts

q_sec_frmwk_soc_secp7.question.fex