◀ 100

CompTIA Security+ Certification Practice Test 5 (Exam SY0-401)

Send results by email

Name	Enter your name
Email	Enter your email

Send Results

▸ Which of the following terms is used to describe the loss of value to an asset based on a single security incident?

○ ✔ 👎 SLE (✖ Missed)

○ ○ ○ ARO

○ ○ ○ ALE

○ ○ ○ ARP

⊟ Your answer to this question is incorrect.

▸ An estimate based on the historical data of how often a threat would be successful in exploiting a vulnerability is known as:

○ ○ ○ ALE

○ ✔ 👎 ARO (✖ Missed)

○ ○ ○ SLE

○ ○ ○ AUP

⊟ Your answer to this question is incorrect.

▸ Which of the answers listed below refers to the correct formula for calculating probable financial loss due to a risk over a one-year period?

○ ○ ○ SLE = AV x EF

○ ✔ 👎 ALE = ARO x SLE (✖ Missed)

○ ○ ○ SLE = ALE x AV

○ ○ ○ ALE = AV x EF

⊟ Your answer to this question is incorrect.

▸ Which of the following terms is used to describe the average time required to repair a failed component or device?

○ ○ ○ MTBF

○ ○ ○ MTU

○ ✔ 👎 MTTR (✖ Missed)

In order to provide you with the best online experience this website uses cookies.

○ ○ ○ MPLS

By using our website, you agree to our use of cookies. **Learn more**

⊟ Your answer to this question is incorrect.

I agree

▸ High MTBF value indicates that a component or system provides low reliability and is more likely to fail.

○ ○ ○ True

○ ✔ 👎 False (✖ Missed)

▬ Your answer to this question is incorrect.

▸ A calculation of the Single Loss Expectancy (SLE) is an example of:

👆 ✔ ☑ Quantitative risk assessment (☑ Your answer)

○ ○ ○ Risk deterrence

○ ○ ○ Qualitative risk assessment

○ ○ ○ Incident management

☑ You correctly answered this question.

▸ Assessment of risk probability and its impact based on subjective judgment falls into the category of:

○ ○ ○ Environmental controls

○ ○ ○ Quantitative risk assessment

○ ○ ○ Forensic procedures

👆 ✔ ☑ Qualitative risk assessment (☑ Your answer)

☑ You correctly answered this question.

▸ A path or tool allowing an attacker to gain unauthorized access to a system or network is known as:

○ ○ ○ Backdoor

○ ✔ 👎 Threat vector (✖ Missed)

○ ○ ○ Discretionary access

👆 ○ ▬ Rootkit (✖ Your answer)

▬ Your answer to this question is incorrect.

▸ In quantitative risk assessment, this term is used for estimating the likelihood of occurrence of a future threat.

○ ○ ○ ALE

○ ○ ○ AV

👆 ✔ ☑ ARO (☑ Your answer)

○ ○ ○ SLE

☑ You correctly answered this question.

▸ Contracting out a specialized technical component when the company's employees lack the necessary skills is an example of:

○ ○ ○ Risk deterrence **In order to provide you with the best online experience this website uses cookies.**

○ ○ ○ Risk avoidance

○ ○ ○ Risk acceptance

👍 ✔ ☑ Risk transference (☑ Your answer)

☑ You correctly answered this question.

▸ Disabling certain system functions or shutting down the system when risks are identified is an example of:

◯ ◯ ◯ Risk acceptance

👍 ✔ ☑ Risk avoidance (☑ Your answer)

◯ ◯ ◯ Risk transference

◯ ◯ ◯ Risk deterrence

☑ You correctly answered this question.

▸ Which of the answers listed below exemplifies an implementation of risk transference methodology?

👍 ✔ ☑ Insurance policy (☑ Your answer)

◯ ◯ ◯ Security guard

◯ ◯ ◯ Antivirus software

◯ ◯ ◯ User education

☑ You correctly answered this question.

▸ Which of the following terms relates closely to the concept of residual risk?

◯ ◯ ◯ Firewall rules

◯ ◯ ◯ Virtualization

👍 ✔ ☑ Risk acceptance (☑ Your answer)

◯ ◯ ◯ Quantitative risk assessment

☑ You correctly answered this question.

▸ What type of risk management strategy is in place when accessing the network involves a login banner warning designed to inform potential attacker of the likelihood of getting caught?

◯ ◯ ◯ Risk avoidance

◯ ◯ ◯ Risk acceptance

👍 ✔ ☑ Risk deterrence (☑ Your answer)

◯ ◯ ◯ Risk transference

☑ You correctly answered this question.

▸ Which of the following security control types can be used in implementing a risk mitigation strategy? (Select all that apply)

☐ ✔ 👎 Technical (✘ Missed)

👍 ✔ ☑ Management (☑ Your answer)

👍 ✔ ☑ Operational (☑ Your answer)

☐ ☐ ☐ Zero-day

◼ Your answer to this question is incorrect.

▶ Which of the terms listed below refers to one of the hardware-related disadvantages of the virtualization technology?

- 👆 ✔ ☑ Single point of failure (☑ Your answer)
- ○ ○ ○ Server clustering
- ○ ○ ○ Privilege escalation
- ○ ○ ○ Power and cooling costs

☑ You correctly answered this question.

▶ Which of the following acronyms refers to a maximum tolerable period of time required for restoring business functions after a failure or disaster?

- ○ ○ ○ RAS
- 👆 ✔ ☑ RTO (☑ Your answer)
- ○ ○ ○ ROI
- ○ ○ ○ RPO

☑ You correctly answered this question.

▶ Recovery time objective (RTO) specifies a point in time to which systems and data must be recovered after a disaster has occurred.

- 👆 ○ ➖ True (✖ Your answer)
- ○ ✔ 👎 False (✖ Missed)

➖ Your answer to this question is incorrect.

▶ An agreement between a service provider and the user(s) defining the nature, availability, quality, and scope of the service to be provided is known as:

- ○ ○ ○ SLE
- ○ ○ ○ BPA
- 👆 ✔ ☑ SLA (☑ Your answer)
- ○ ○ ○ DLP

☑ You correctly answered this question.

▶ Which of the following answers refers to a key document governing the relationship between two business organisations?

- ○ ○ ○ ISA
- ○ ○ ○ ALE
- 👆 ○ ➖ SLA (✖ Your answer)
- ○ ✔ 👎 BPA (✖ Missed)

➖ Your answer to this question is incorrect.

▶ A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission is known as:

- ○ ○ ○ BPA

- 👍 ✔ ☑ MOU (☑ Your answer)
- ○ ○ ○ SLE
- ○ ○ ○ ISA

☑ You correctly answered this question.

▶ Which of the answers listed below refers to an agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection?

- 👍 ✔ ☑ ISA (☑ Your answer)
- ○ ○ ○ ALE
- ○ ○ ○ MOU
- ○ ○ ○ BPA

☑ You correctly answered this question.

▶ Which of the following functionalities allows a DLP system to fulfil its role?

- ○ ○ ○ Motion detection
- ○ ○ ○ Environmental monitoring
- 👍 ✔ ☑ Content inspection (☑ Your answer)
- ○ ○ ○ Loop protection

☑ You correctly answered this question.

▶ In forensic procedures, a sequence of steps in which different types of evidence should be collected is known as:

- ○ ✔ 👎 Order of volatility (✖ Missed)
- ○ ○ ○ Layered security
- 👍 ○ ◼ Chain of custody (✖ Your answer)
- ○ ○ ○ Transitive access

◼ Your answer to this question is incorrect.

▶ In forensic procedures, a chronological record outlining persons in possession of an evidence is referred to as:

- ○ ○ ○ Proxy list
- ○ ○ ○ Order of volatility
- ○ ○ ○ Access log
- 👍 ✔ ☑ Chain of custody (☑ Your answer)

☑ You correctly answered this question.

Try Again (/component/communityquiz/quiz/10-comptia-security-plus-certification/57-comptia-security-plus-certification-practice-test-5-exam-sy0-401?Itemid=101)