Risk in the Workplace

Users

Incident Handling

Graded Assessments

Video: Final Assessment
22 sec

Quiz: Creating a Company Culture for Security
10 questions

Quiz: Creating a Company Culture for Security - Design Document
1 question

Reading: Final Project - Sample Submission
10 min

Discussion Prompt: Connect with Google IT Support Certificate graduates
10 min

Course Wrap Up

Congratulations! You passed!

Grade received 92.50%

Latest Submission Grade 92.50%

To pass 80% or higher

Retake the assignment in **23h 59m**

Go to next item

Creating a Company Culture for Security

Quiz • 55 min

Submit your assignment

Due Jul 2, 11:59 PM +08 **Attempts** 3 every 24 hours

Receive grade

Your grade
92.50%

We keep your highest score

Try again

Retake the quiz in **23h 56m**

View Feedback

1. In the Payment Card Industry Data Security Standard (PCI DSS), what are the requirements for the "regularly monitor and test networks" objective? Select all that apply

1 / 1 point

- [ ] Develop and maintain secure systems and applications
- [x] Regularly test security systems and processes

  Correct
- [x] Track and monitor all access to network resources and cardholder data

  Correct

  Like **Dislike** **Report an issue**
- [ ] Encrypt the transmission of cardholder data across open public networks

2. What characteristics are used to assess the severity of found vulnerabilities? Select all that apply.

1 / 1 point

- [ ] Use of encryption or not
- [x] Remotely exploitable or not

  Correct
- [x] Type of access gained

  Correct
- [x] Chance of exploitation

  Correct

3. _____ is the practice of attempting to break into a system or network for the purpose of verifying the systems in place.

1 / 1 point

- (•) Penetration testing
- ( ) Vulnerability scanning
- ( ) Network probing
- ( ) Security assessment

Correct

4. Which of the following should be part of an access data request? Select all that apply.

0.75 / 1 point

- [ ] Time limit
- [x] Provide justification

  Correct
- [ ] A second signature
- [x] Specify exact data needed

  Correct

You didn't select all the correct answers

5. Consider the following scenario:

A co-worker needs to share a sensitive file with you, but it is too large to send via an encrypted email. The co-worker works out of a remote office. You work at headquarters. Which of these options would most likely be approved by the company's security policies? Select all that apply.

1 / 1 point

- [x] Upload to company secure cloud storage

  Correct
- [x] Put on a company file server that you both have access to

  Correct
- [ ] Upload to a personal OneDrive
- [ ] Upload to a personal Google drive

6. Which of the following are ways to prevent email phishing attacks against user passwords? Select all that apply.

1 / 1 point

- [x] User education

  Correct
- [ ] Virtual private network
- [ ] Cloud email
- [x] Spam filters

  Correct

7. Which of the following actions should be included when conducting a vendor risk review? Select all that apply.

0.5 / 1 point

- [ ] Ask the vendor for a cost comparison
- [x] Ask the vendor to fill out a security questionnaire

  Correct
- [ ] Test the vendor's hardware or software
- [x] Talk to the vendor's employees

  This should not be selected
  Please review the video about third-party security

8. Google provides free _____, which is a good starting point when assessing third-party vendors.

1 / 1 point

- ( ) mobile phone services
- ( ) cloud storage
- (•) vendor security assessment questionnaires
- ( ) business apps

Correct

9. Periodic mandatory security training courses can be given to employees in what way? Select all that apply.

1 / 1 point

- [x] Short video

  Correct
- [ ] Interoffice memos
- [ ] One-on-one interviews
- [x] Brief quiz

  Correct

10. Once the scope of the incident is determined, the next step would be _____.

1 / 1 point

- ( ) remediation
- (•) containment
- ( ) escalation
- ( ) documentation

Correct