



# PROFESSIONAL-CLOUD-SECURITY-ENGINEER<sup>Q&As</sup>

Professional Cloud Security Engineer

**Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/professional-cloud-security-engineer.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Google  
Official Exam Center



VCE & PDF

PassApply.com

<https://www.passapply.com/professional-cloud-security-engineer.html>  
2024 Latest passapply PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF  
and VCE dumps Download

---

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

You want to make sure that your organization's Cloud Storage buckets cannot have data publicly available to the internet. You want to enforce this across all Cloud Storage buckets. What should you do?

- A. Remove Owner roles from end users, and configure Cloud Data Loss Prevention.
- B. Remove Owner roles from end users, and enforce domain restricted sharing in an organization policy.
- C. Configure uniform bucket-level access, and enforce domain restricted sharing in an organization policy.
- D. Remove \*.setiamPolicy permissions from all roles, and enforce domain restricted sharing in an organization policy.

Correct Answer: C

-Uniform bucket-level access:

<https://cloud.google.com/storage/docs/uniform-bucket-level-access#should-you-use> -Domain Restricted Sharing:

[https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#public\\_data\\_sharing](https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#public_data_sharing)

---

### QUESTION 2

Your organization is moving virtual machines (VMs) to Google Cloud. You must ensure that operating system images that are used across your projects are trusted and meet your security requirements. What should you do?

- A. Implement an organization policy to enforce that boot disks can only be created from images that come from the trusted image project.
- B. Create a Cloud Function that is automatically triggered when a new virtual machine is created from the trusted image repository. Verify that the image is not deprecated.
- C. Implement an organization policy constraint that enables the Shielded VM service on all projects to enforce the trusted image repository usage.
- D. Automate a security scanner that verifies that no common vulnerabilities and exposures (CVEs) are present in your trusted image repository.

Correct Answer: A

---

### QUESTION 3

Your company is moving to Google Cloud. You plan to sync your users first by using Google Cloud Directory Sync (GCDS). Some employees have already created Google Cloud accounts by using their company email addresses that were created outside of GCDS. You must create your users on Cloud Identity.

What should you do?

- A. Configure GCDS and use GCDS search rules to sync these users.
- B. Use the transfer tool to migrate unmanaged users.



- C. Write a custom script to identify existing Google Cloud users and call the Admin SDK Directory API to transfer their account.
- D. Configure GCDS and use GCDS exclusion rules to ensure users are not suspended.

Correct Answer: B

---

#### QUESTION 4

Your organization wants to be continuously evaluated against CIS Google Cloud Computing Foundations Benchmark v1 3 0 (CIS Google Cloud Foundation 1 3). Some of the controls are irrelevant to your organization and must be disregarded in evaluation. You need to create an automated system or process to ensure that only the relevant controls are evaluated.

What should you do?

- A. Mark all security findings that are irrelevant with a tag and a value that indicates a security exception Select all marked findings and mute them on the console every time they appear Activate Security Command Center (SCC) Premium.
- B. Activate Security Command Center (SCC) Premium Create a rule to mute the security findings in SCC so they are not evaluated.
- C. Download all findings from Security Command Center (SCC) to a CSV file Mark the findings that are part of CIS Google Cloud Foundation 1 3 in the file Ignore the entries that are irrelevant and out of scope for the company.
- D. Ask an external audit company to provide independent reports including needed CIS benchmarks. In the scope of the audit clarify that some of the controls are not needed and must be disregarded.

Correct Answer: B

---

#### QUESTION 5

You are implementing data protection by design and in accordance with GDPR requirements. As part of design reviews, you are told that you need to manage the encryption key for a solution that includes workloads for Compute Engine,

Google Kubernetes Engine, Cloud Storage, BigQuery, and Pub/Sub.

Which option should you choose for this implementation?

- A. Cloud External Key Manager
- B. Customer-managed encryption keys
- C. Customer-supplied encryption keys
- D. Google default encryption

Correct Answer: A

---

[PROFESSIONAL-CLOUD-](#) [PROFESSIONAL-CLOUD-](#) [PROFESSIONAL-CLOUD-](#)



VCE & PDF

PassApply.com

<https://www.passapply.com/professional-cloud-security-engineer.html>  
2024 Latest passapply PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF  
and VCE dumps Download

---

[SECURITY-ENGINEER  
VCE Dumps](#)

[SECURITY-ENGINEER  
Practice Test](#)

[SECURITY-ENGINEER  
Exam Questions](#)