

# Google

## Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer



#### NEW QUESTION 1

You want to evaluate GCP for PCI compliance. You need to identify Google's inherent controls. Which document should you review to find the information?

- A. Google Cloud Platform: Customer Responsibility Matrix
- B. PCI DSS Requirements and Security Assessment Procedures
- C. PCI SSC Cloud Computing Guidelines
- D. Product documentation for Compute Engine

**Answer: C**

#### NEW QUESTION 2

A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.

What should they do?

- A. Use Cloud Build to build the container images.
- B. Build small containers using small base images.
- C. Delete non-used versions from Container Registry.
- D. Use a Continuous Delivery tool to deploy the application.

**Answer: D**

#### NEW QUESTION 3

You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually. You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.

What should you do?

- A. Set up an ACL with OWNER permission to a scope of allUsers.
- B. Set up an ACL with READER permission to a scope of allUsers.
- C. Set up a default bucket ACL and manage access for users using IAM.
- D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

**Answer: A**

#### NEW QUESTION 4

A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location.

Which solution will restrict access to the in-progress sites?

- A. Upload an .htaccess file containing the customer and employee user accounts to App Engine.
- B. Create an App Engine firewall rule that allows access from the customer and employee networks and denies all other traffic.
- C. Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.
- D. Use Cloud VPN to create a VPN connection between the relevant on-premises networks and the company's GCP Virtual Private Cloud (VPC) network.

**Answer: C**

#### NEW QUESTION 5

A customer has an analytics workload running on Compute Engine that should have limited internet access. Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet.

The Compute Engine instances now need to reach out to the public repository to get security updates. What should your team do?

- A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.
- B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
- C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.
- D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

**Answer: C**

#### NEW QUESTION 6

An organization is evaluating the use of Google Cloud Platform (GCP) for certain IT workloads. A well-established directory service is used to manage user identities and lifecycle management. This directory service must continue for the organization to use as the "source of truth" directory for identities.

Which solution meets the organization's requirements?

- A. Google Cloud Directory Sync (GCDS)
- B. Cloud Identity
- C. Security Assertion Markup Language (SAML)
- D. Pub/Sub

**Answer: B**

#### NEW QUESTION 7

You will create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices. What should you do?

- A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
- B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.
- C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
- D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

**Answer:** A

#### NEW QUESTION 8

Your team wants to limit users with administrative privileges at the organization level. Which two roles should your team restrict? (Choose two.)

- A. Organization Administrator
- B. Super Admin
- C. GKE Cluster Admin
- D. Compute Admin
- E. Organization Role Viewer

**Answer:** AB

#### NEW QUESTION 9

When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)

- A. Ensure that the app does not run as PID 1.
- B. Package a single app as a container.
- C. Remove any unnecessary tools not needed by the app.
- D. Use public container images as a base image for the app.
- E. Use many container image layers to hide sensitive information.

**Answer:** BC

#### NEW QUESTION 10

A company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery. What should you do?

- A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.
- B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.
- C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.
- D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

**Answer:** D

#### NEW QUESTION 10

Your company runs a website that will store PII on Google Cloud Platform. To comply with data privacy regulations, this data can only be stored for a specific amount of time and must be fully deleted after this specific period. Data that has not yet reached the time period should not be deleted. You want to automate the process of complying with this regulation. What should you do?

- A. Store the data in a single Persistent Disk, and delete the disk at expiration time.
- B. Store the data in a single BigQuery table and set the appropriate table expiration time.
- C. Store the data in a single Cloud Storage bucket and configure the bucket's Time to Live.
- D. Store the data in a single BigTable table and set an expiration time on the column families.

**Answer:** B

#### NEW QUESTION 13

You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer. What should you do?

- A. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryptionkey (KEK) in Cloud KMS to encrypt the DE
- B. Store both the encrypted data and the encrypted DEK.
- C. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DE
- D. Store both the encrypted data and the KEK.
- E. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the ke
- F. Store both the encrypted data and the encrypted DEK.
- G. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the ke
- H. Store both the encrypted data and the KEK.

**Answer:** A

#### NEW QUESTION 17

A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage. Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet. Which two strategies should your team use to meet these requirements? (Choose two.)

- A. Configure Private Google Access on the Compute Engine subnet
- B. Avoid assigning public IP addresses to the Compute Engine cluster.
- C. Make sure that the Compute Engine cluster is running on a separate subnet.

- D. Turn off IP forwarding on the Compute Engine instances in the cluster.
- E. Configure a Cloud NAT gateway.

**Answer:** BE

#### NEW QUESTION 20

When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for

review by internal or external analysts for customer service trend analysis.

Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

- A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.
- B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.
- C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.
- D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

**Answer:** D

#### Explanation:

Reference; <https://cloud.google.com/dlp/docs/deidentify-sensitive-data>

#### NEW QUESTION 24

How should a customer reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

- A. Send all logs to the SIEM system via an existing protocol such as syslog.
- B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.
- C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.
- D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

**Answer:** C

#### NEW QUESTION 28

A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects.

Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources.

Which type of access should your team grant to meet this requirement?

- A. Organization Administrator
- B. Security Reviewer
- C. Organization Role Administrator
- D. Organization Policy Administrator

**Answer:** C

#### NEW QUESTION 33

In an effort for your company messaging app to comply with FIPS 140-2, a decision was made to use GCP compute and network services. The messaging app architecture includes a Managed Instance Group (MIG) that controls a cluster of Compute Engine instances. The instances use Local SSDs for data caching and UDP for instance-to-instance communications. The app development team is willing to make any changes necessary to comply with the standard

Which options should you recommend to meet the requirements?

- A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.
- B. Set Disk Encryption on the Instance Template used by the MIG to customer-managed key and use BoringSSL for all data transit between instances.
- C. Change the app instance-to-instance communications from UDP to TCP and enable BoringSSL on clients' TLS connections.
- D. Set Disk Encryption on the Instance Template used by the MIG to Google-managed Key and use BoringSSL library on all instance-to-instance communications.

**Answer:** D

#### NEW QUESTION 34

A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.

What technique should the institution use?

- A. Use Cloud Storage as a federated Data Source.
- B. Use a Cloud Hardware Security Module (Cloud HSM).
- C. Customer-managed encryption keys (CMEK).
- D. Customer-supplied encryption keys (CSEK).

**Answer:** C

#### NEW QUESTION 39

You need to provide a corporate user account in Google Cloud for each of your developers and operational staff who need direct access to GCP resources.

Corporate policy requires you to maintain the user identity in a third-party identity management provider and leverage single sign-on. You learn that a significant number of users are using their corporate domain email addresses for personal Google accounts, and you need to follow Google recommended practices to convert existing unmanaged users to managed accounts.

Which two actions should you take? (Choose two.)

- A. Use Google Cloud Directory Sync to synchronize your local identity management system to Cloud Identity.
- B. Use the Google Admin console to view which managed users are using a personal account for their recovery email.
- C. Add users to your managed Google account and force users to change the email addresses associated with their personal accounts.
- D. Use the Transfer Tool for Unmanaged Users (TTUU) to find users with conflicting accounts and ask them to transfer their personal Google accounts.
- E. Send an email to all of your employees and ask those users with corporate email addresses for personal Google accounts to delete the personal accounts immediately.

**Answer:** BE

#### NEW QUESTION 40

A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack. Which solution should this customer use?

- A. VPC Flow Logs
- B. Cloud Armor
- C. DNS Security Extensions
- D. Cloud Identity-Aware Proxy

**Answer:** C

#### NEW QUESTION 43

A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK). How should the team complete this task?

- A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.
- B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.
- C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.
- D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

**Answer:** D

#### NEW QUESTION 44

A company is backing up application logs to a Cloud Storage bucket shared with both analysts and the administrator. Analysts should only have access to logs that do not contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible by the administrator. What should you do?

- A. Use Cloud Pub/Sub and Cloud Functions to trigger a Data Loss Prevention scan every time a file is uploaded to the shared bucket.
- B. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.
- C. Upload the logs to both the shared bucket and the bucket only accessible by the administrator.
- D. Create a job trigger using the Cloud Data Loss Prevention API.
- E. Configure the trigger to delete any files from the shared bucket that contain PII.
- F. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.
- G. On the bucket shared with both the analysts and the administrator, configure a Cloud Storage Trigger that is only triggered when PII data is uploaded.
- H. Use Cloud Functions to capture the trigger and delete such files.

**Answer:** C

#### NEW QUESTION 45

A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection. Which product should be used to meet these requirements?

- A. Cloud Armor
- B. VPC Firewall Rules
- C. Cloud Identity and Access Management
- D. Cloud CDN

**Answer:** A

#### NEW QUESTION 50

An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud. What solution would help meet the requirements?

- A. Ensure that firewall rules are in place to meet the required controls.
- B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.
- C. Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite.
- D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

**Answer:** B

#### NEW QUESTION 55

You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual



machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow the application frontend to access the data in the application's mysql instance on port 3306. What should you do?

- A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag "data-tag" that is applied to the mysql Compute Engine VM on port 3306.
- B. Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique service account of the mysql Compute Engine VM on port 3306.
- C. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B.
- D. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged with fe-tag.
- E. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B.
- F. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

**Answer: B**

#### NEW QUESTION 56

You are part of a security team that wants to ensure that a Cloud Storage bucket in Project A can only be readable from Project B. You also want to ensure that data in the Cloud Storage bucket cannot be accessed from or copied to Cloud Storage buckets outside the network, even if the user has the correct credentials. What should you do?

- A. Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.
- B. Enable Domain Restricted Sharing Organization Policy and Bucket Policy Only on the Cloud Storage bucket.
- C. Enable Private Access in Project A and B networks with strict firewall rules to allow communication between the networks.
- D. Enable VPC Peering between Project A and B networks with strict firewall rules to allow communication between the networks.

**Answer: B**

#### NEW QUESTION 58

Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud. What should you do?

- A. Use the Cloud Key Management Service to manage the data encryption key (DEK).
- B. Use the Cloud Key Management Service to manage the key encryption key (KEK).
- C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
- D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

**Answer: A**

#### NEW QUESTION 63

A manager wants to start retaining security event logs for 2 years while minimizing costs. You write a filter to select the appropriate log entries. Where should you export the logs?

- A. BigQuery datasets
- B. Cloud Storage buckets
- C. StackDriver logging
- D. Cloud Pub/Sub topics

**Answer: C**

#### NEW QUESTION 68

A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published. Which Google Cloud Service should be used to achieve this?

- A. Cloud Key Management Service
- B. Cloud Data Loss Prevention API
- C. BigQuery
- D. Cloud Security Scanner

**Answer: D**

#### NEW QUESTION 71

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys. What should you do?

- A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing.
- B. Manage the IAM permissions at the Key level.
- C. Create a single KeyRing for all persistent disks and all Keys in this KeyRing.
- D. Manage the IAM permissions at the KeyRing level.
- E. Create a KeyRing per persistent disk, with each KeyRing containing a single Key.
- F. Manage the IAM permissions at the Key level.
- G. Create a KeyRing per persistent disk, with each KeyRing containing a single Key.
- H. Manage the IAM permissions at the KeyRing level.

**Answer:** C

**NEW QUESTION 72**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### Professional-Cloud-Security-Engineer Practice Exam Features:

- \* Professional-Cloud-Security-Engineer Questions and Answers Updated Frequently
- \* Professional-Cloud-Security-Engineer Practice Questions Verified by Expert Senior Certified Staff
- \* Professional-Cloud-Security-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* Professional-Cloud-Security-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The Professional-Cloud-Security-Engineer Practice Test Here](#)**