

# Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

<https://www.2passeasy.com/dumps/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

In a shared security responsibility model for IaaS, which two layers of the stack does the customer share responsibility for? (Choose two.)

- A. Hardware
- B. Network Security
- C. Storage Encryption
- D. Access Policies
- E. Boot

**Answer: CD**

#### NEW QUESTION 3

While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password. What should you do?

- A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.
- B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.
- C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos-compliant identity provider.
- D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

**Answer: B**

#### NEW QUESTION 4

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 5

You are the Security Admin in your company. You want to synchronize all security groups that have an email address from your LDAP directory in Cloud IAM.

- A. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" as the attribute to facilitate one-way sync.
- B. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" as the attribute to facilitate bidirectional sync.
- C. Use a management tool to sync the subset based on the email address attribute.
- D. Create a group in the Google domain.
- E. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.
- F. Use a management tool to sync the subset based on group object class attribute.
- G. Create a group in the Google domain.
- H. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.

**Answer: C**

#### NEW QUESTION 6

Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised. What should you do?

- A. Enforce 2-factor authentication in GSuite for all users.
- B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
- C. Provision user passwords using GSuite Password Sync.
- D. Configure Cloud VPN between your private network and GCP.

**Answer: D**

#### NEW QUESTION 7

Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway

on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet. What should your team grant to Engineering Group A to meet this requirement?

- A. Compute Network User Role at the host project level.
- B. Compute Network User Role at the subnet level.
- C. Compute Shared VPC Admin Role at the host project level.
- D. Compute Shared VPC Admin Role at the service project level.

**Answer: C**

#### NEW QUESTION 8

Which two implied firewall rules are defined on a VPC network? (Choose two.)

- A. A rule that allows all outbound connections
- B. A rule that denies all inbound connections
- C. A rule that blocks all inbound port 25 connections
- D. A rule that blocks all outbound connections
- E. A rule that allows all inbound port 80 connections

**Answer: AB**

#### NEW QUESTION 9

A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.

Which two approaches can you take to meet the requirements? (Choose two.)

- A. Configure the project with Cloud VPN.
- B. Configure the project with Shared VPC.
- C. Configure the project with Cloud Interconnect.
- D. Configure the project with VPC peering.
- E. Configure all Compute Engine instances with Private Access.

**Answer: DE**

#### NEW QUESTION 10

In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized. Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

- A. App Engine
- B. Cloud Functions
- C. Compute Engine
- D. Google Kubernetes Engine
- E. Cloud Storage

**Answer: AC**

#### NEW QUESTION 10

A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system. How should the customer achieve this using Google Cloud Platform?

- A. Use Cloud Source Repositories, and store secrets in Cloud SQL.
- B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
- C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.
- D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

**Answer: B**

#### NEW QUESTION 11

A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE). How should the DevOps team accomplish this?

- A. Use Puppet or Chef to push out the patch to the running container.
- B. Verify that auto upgrade is enabled; if so, Google will upgrade the nodes in a GKE cluster.
- C. Update the application code or apply a patch, build a new image, and redeploy it.
- D. Configure containers to automatically upgrade when the base image is available in Container Registry.

**Answer: B**

#### NEW QUESTION 13

For compliance reasons, an organization needs to ensure that in-scope PCI Kubernetes Pods reside on "in-scope" Nodes only. These Nodes can only contain the "in-scope" Pods.

How should the organization achieve this objective?

- A. Add a nodeSelector field to the pod configuration to only use the Nodes labeled inscope: true.
- B. Create a node pool with the label inscope: true and a Pod Security Policy that only allows the Pods to run on Nodes with that label.
- C. Place a taint on the Nodes with the label inscope: true and effect NoSchedule and a toleration to match in the Pod configuration.
- D. Run all in-scope Pods in the namespace "in-scope-pci".

Answer: C

#### NEW QUESTION 16

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 17

You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment. How should you prevent and fix this vulnerability?

- A. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- C. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

Answer: D

#### NEW QUESTION 20

An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters. Which Cloud Identity password guidelines can the organization use to inform their new requirements?

- A. Set the minimum length for passwords to be 8 characters.
- B. Set the minimum length for passwords to be 10 characters.
- C. Set the minimum length for passwords to be 12 characters.
- D. Set the minimum length for passwords to be 6 characters.

Answer: C

#### NEW QUESTION 22

A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means. Which connectivity option should be implemented?

- A. VPC peering
- B. Cloud VPN
- C. Cloud Interconnect
- D. Shared VPC

Answer: B

#### NEW QUESTION 23

Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network. How should your team design this network?

- A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.
- B. Create a different subnet for the frontend application and database to ensure network isolation.
- C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.
- D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

Answer: A

#### NEW QUESTION 24

Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer. What type of Load Balancing should you use?

- A. Network Load Balancing
- B. HTTP(S) Load Balancing
- C. TCP Proxy Load Balancing
- D. SSL Proxy Load Balancing

Answer: D

#### NEW QUESTION 27

A company's application is deployed with a user-managed Service Account key. You want to use Google- recommended practices to rotate the key. What should you do?

- A. Open Cloud Shell and run `gcloud iam service-accounts enable-auto-rotate --iam- account=IAM_ACCOUNT`.
- B. Open Cloud Shell and run `gcloud iam service-accounts keys rotate --iam- account=IAM_ACCOUNT--key=NEW_KEY`.
- C. Create a new key, and use the new key in the applicatio
- D. Delete the old key from the Service Account.
- E. Create a new key, and use the new key in the applicatio
- F. Store the old key on the system as a backup key.

**Answer: C**

#### NEW QUESTION 32

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 37

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 42

As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name. Which cost reduction options should you recommend?

- A. Set appropriate `rowsLimit` value on BigQuery data hosted outside the US and set appropriate `bytesLimitPerFile` value on multiregional Cloud Storage buckets.
- B. Set appropriate `rowsLimit` value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.
- C. Use `rowsLimit` and `bytesLimitPerFile` to sample data and use `CloudStorageRegexFileSet` to limit scans.
- D. Use `FindingLimits` and `TimespanContfig` to sample data and minimize transformation units.

**Answer: C**

#### NEW QUESTION 44

An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented. Which GCP solution should the organization use?

- A. BigQuery using a data pipeline job with continuous updates via Cloud VPN
- B. Cloud Storage using a scheduled task and `gsutil` via Cloud Interconnect
- C. Compute Engines Virtual Machines using Persistent Disk via Cloud Interconnect
- D. Cloud Datastore using regularly scheduled batch upload jobs via Cloud VPN

**Answer: B**

#### NEW QUESTION 49

Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written to BigQuery was done using the App Engine Default Service Account. What should you do?

- A. \* 1. Use StackDriver Logging and filter on BigQuery Insert Jobs.\* 2. Click on the email address in line with the App Engine Default Service Account in the authentication field.\* 3. Click Hide Matching Entry
- B. \* 4. Make sure the resulting list is empty.
- C. \* 1. Use StackDriver Logging and filter on BigQuery Insert Jobs.\* 2. Click on the email address in line with the App Engine Default Service Account in the authentication field.\* 3. Click Show Matching Entry
- D. \* 4. Make sure the resulting list is empty.
- E. \* 1. In BigQuery, select the related dataset.\* 2. Make sure the App Engine Default Service Account is the only account that can write to the dataset.
- F. \* 1. Go to the IAM section on the project.\* 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

Answer: C

#### NEW QUESTION 50

Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?

- A. ISO 27001
- B. ISO 27002
- C. ISO 27017
- D. ISO 27018

Answer: C

#### Explanation:

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.

#### NEW QUESTION 54

You are the security admin of your company. Your development team creates multiple GCP projects under the "implementation" folder for several dev, staging, and production workloads. You want to prevent data exfiltration by malicious insiders or compromised code by setting up a security perimeter. However, you do not want to restrict communication between the projects.

What should you do?

- A. Use a Shared VPC to enable communication between all projects, and use firewall rules to prevent data exfiltration.
- B. Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.
- C. Use an infrastructure-as-code software tool to set up a single service perimeter and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Su
- D. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the associated perimeter.
- E. Use an infrastructure-as-code software tool to set up three different service perimeters for dev, staging, and prod and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Su
- F. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the respective perimeter.

Answer: B

#### NEW QUESTION 56

Your team uses a service account to authenticate data transfers from a given Compute Engine virtual machine instance of to a specified Cloud Storage bucket. An engineer accidentally deletes the service account, which breaks application functionality. You want to recover the application as quickly as possible without compromising security.

What should you do?

- A. Temporarily disable authentication on the Cloud Storage bucket.
- B. Use the undelete command to recover the deleted service account.
- C. Create a new service account with the same name as the deleted service account.
- D. Update the permissions of another existing service account and supply those credentials to the applications.

Answer: B

#### NEW QUESTION 60

A customer deploys an application to App Engine and needs to check for Open Web Application Security Project (OWASP) vulnerabilities. Which service should be used to accomplish this?

- A. Cloud Armor
- B. Google Cloud Audit Logs
- C. Cloud Security Scanner
- D. Forseti Security

Answer: C

#### NEW QUESTION 65

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 AP
- 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 70

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 72

An organization receives an increasing number of phishing emails.  
Which method should be used to protect employee credentials in this situation?

- A. Multifactor Authentication
- B. A strict password policy
- C. Captcha on login pages
- D. Encrypted emails

**Answer:** D

#### NEW QUESTION 73

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 77

A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing.  
How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

- A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.
- B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.
- C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).
- D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

**Answer:** D

#### NEW QUESTION 79

A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on Compute Engine. Their security team wants to add a security layer so that the ERP systems only accept traffic from Cloud Identity-Aware Proxy.  
What should the customer do to meet these requirements?

- A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
- B. Make sure that the ERP system can validate the identity headers in the HTTP requests.
- C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
- D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

**Answer:** A

#### NEW QUESTION 81

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 82

An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege.  
Which option meets the requirement of your team?

- A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance's IP address and allows the application to read from the bucket without credentials.
- B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.
- C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.

D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

**Answer:** C

#### NEW QUESTION 85

What are the steps to encrypt data using envelope encryption?

- A. Generate a data encryption key (DEK) locally. Use a key encryption key (KEK) to wrap the DE
- B. Encrypt data with the KE
- C. Store the encrypted data and the wrapped KEK.
- D. Generate a key encryption key (KEK) locally. Use the KEK to generate a data encryption key (DEK). Encrypt data with the DE
- E. Store the encrypted data and the wrapped DEK.
- F. Generate a data encryption key (DEK) locally. Encrypt data with the DEK. Use a key encryption key (KEK) to wrap the DE
- G. Store the encrypted data and the wrapped DEK.
- H. Generate a key encryption key (KEK) locally. Generate a data encryption key (DEK) locally
- I. Encrypt data with the KE
- J. Store the encrypted data and the wrapped DEK.

**Answer:** C

#### NEW QUESTION 90

An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its current data backup and disaster recovery solutions to GCP for later analysis. The organization's production environment will remain on-premises for an indefinite time. The organization wants a scalable and cost-efficient solution. Which GCP solution should the organization use?

- A. BigQuery using a data pipeline job with continuous updates
- B. Cloud Storage using a scheduled task and gsutil
- C. Compute Engine Virtual Machines using Persistent Disk
- D. Cloud Datastore using regularly scheduled batch upload jobs

**Answer:** A

#### NEW QUESTION 92

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Professional-Cloud-Security-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Professional-Cloud-Security-Engineer Product From:

<https://www.2passeasy.com/dumps/Professional-Cloud-Security-Engineer/>

### Money Back Guarantee

#### **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