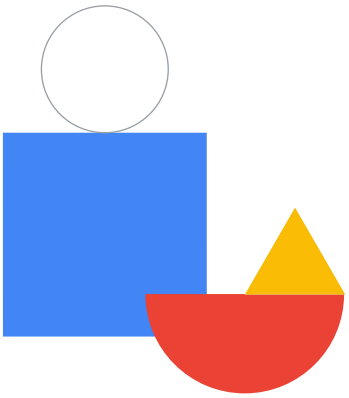
Google Cloud

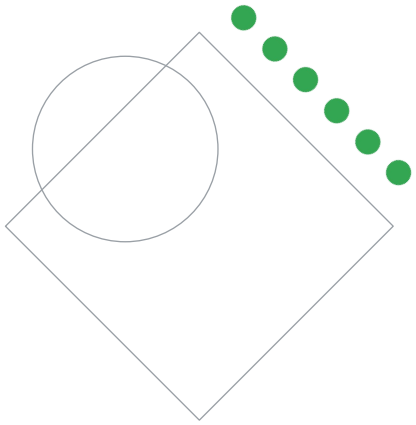


Preparing for Your Professional Cloud Architect Journey

Module 3: Designing for Security and Compliance

Welcome to Module 3: Designing for Security and Compliance.

Review and study planning

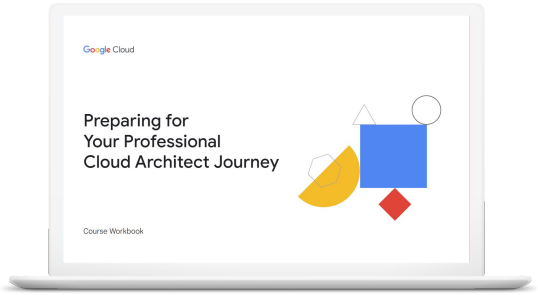


Google Cloud

You'll now review the diagnostic questions and your answers to help you identify what to include in your study plan.

Your study plan:

Designing for security and compliance



3.1 Designing for security

3.2 Designing for compliance

Google Cloud

The diagnostic questions align with these objectives of this exam section. Use the PDF resource that follows to review the questions and how you answered them. Pay specific attention to the rationale for both the correct and incorrect answers. Use the resources detailed under **Where to look** and **Content mapping** to build a study plan that meets your learning needs.

3.1 Designing for security

Considerations include:

- Identity and access management (IAM)
- Resource hierarchy (organizations, folders, projects)
- Data security (key management, encryption, secret management)
- Separation of duties (SoD)
- Security controls (e.g., auditing, VPC Service Controls, context aware access, organization policy)
- Managing customer-managed encryption keys with Cloud Key Management Service
- Remote access

Google Cloud

A Professional Cloud Architect should start the design process with a high-level analysis of how services will be exposed, and how access to those services should be granted. A PCA should be familiar with the best practices around VPC Networks, and all of the products and services they use within Google Cloud, because many best practices are security focused.

Question 1 tested your knowledge of Google-recommended practices for designing secure systems. Question 2 tested your ability to set up Identity and Access Management (IAM) to ensure a secure environment. Question 3 asked you to describe user personas. Question 4 tested your knowledge of using service accounts to manage access and authorization of resources by machines and processes. Question 5 asked you to use organizational policies to simplify cloud governance. Question 6 tested your familiarity with leveraging Google Cloud Armor to help mitigate DDoS attacks. Question 7 assessed your knowledge of ways to securely communicate with VMs that do not have public IP addresses. Question 8 tested your knowledge of securing users with Identity-Aware Proxy. Question 9 tested your knowledge of securing users with custom IAM roles.

3.1 Diagnostic Question 01 Discussion

Your client created an Identity and Access Management (IAM) resource hierarchy with Google Cloud when the company was a startup. Your client has grown and now has **multiple departments and teams**. You want to recommend a resource hierarchy that follows Google-recommended practices.

What should you do?

A. Keep all resources in **one project**, and use a **flat resource hierarchy** to reduce complexity and simplify management.

B. Keep all resources in **one project,** but **change the resource hierarchy** to reflect company organization.

C. Use a **flat resource hierarchy** and **multiple projects** with established trust boundaries.

D. Use **multiple projects** with established trust boundaries, and **change the resource hierarchy** to reflect company organization.

Google Cloud

Feedback:
A. Incorrect. Mirror your Google Cloud resource hierarchy structure to match your organization structure. Use projects to group resources that share the same trust boundary.
B. Incorrect. Use projects to group resources that share the same trust boundary.
C. Incorrect. Mirror your Google Cloud resource hierarchy structure to match your organization structure.
D. Correct! Because the environment has evolved, update the IAM resource hierarchy to reflect the changes. Use projects to group resources that share the same trust boundary.

Where to look:
https://cloud.google.com/iam/docs/resource-hierarchy-access-control
https://cloud.google.com/iam/docs/resource-hierarchy-access-control#best_practices

Content mapping:
- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security
- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M8 Security

Summary:
Best practices are incredibly important for Identity and Access Management (IAM).

You encountered two best-practice rules in this question, but you should be familiar with the rest. Look at the best practices in more detail in Google documentation.

3.1 Diagnostic Question 02 Discussion

Cymbal Direct's social media app must run in a **separate project** from its APIs and web store. You want to use **Identity and Access Management (IAM)** to ensure a **secure environment.**

How should you set up IAM?

A. Use **separate** service accounts for each component (social media app, APIs, and web store) with **basic** roles to grant access.

B. Use **one** service account for all components (social media app, APIs, and web store) with **basic** roles to grant access.

C. Use **separate** service accounts for each component (social media app, APIs, and web store) with **predefined or custom** roles to grant access.

D. Use **one** service account for all components (social media app, APIs, and web store) with **predefined or custom** roles to grant access.

Google Cloud

Feedback:
A. Incorrect. Basic roles include thousands of permissions across all Google Cloud services. In production environments, do not grant basic roles unless there is no alternative.
B. Incorrect. Treat each component of your application as a separate trust boundary. If multiple services require different permissions, create a separate service account for each service, and then grant only the required permissions to each service account. Basic roles include thousands of permissions across all Google Cloud services. In production environments, do not grant basic roles unless there is no alternative.
C. Correct! Using separate service accounts for each component allows you to grant only the access needed to each service account with either a predefined or custom role.
D. Incorrect. Treat each component of your application as a separate trust boundary. If multiple services require different permissions, create a separate service account for each service, and then grant only the required permissions to each service account.

Where to look:
https://cloud.google.com/blog/products/identity-security/iam-best-practice-guides-available-now

Content mapping:
- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security

- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
    - M8 Security

Summary:
Using IAM and designing the best environmental approach largely relies on abiding by the “principle of least privilege.” This question included some of the recommended practices. Treat each component of your application as a separate trust boundary. If multiple services require different permissions, create a separate service account for each service, and then grant each the least permissions possible. Basic roles include thousands of permissions across all Google Cloud services, so using them probably provides more abilities than necessary. In production environments, do not grant basic roles unless there is no alternative. A checklist you can use to ensure best practices is available here: https://cloud.google.com/iam/docs/using-iam-securely

3.1 Diagnostic Question 03 Discussion

Michael is the owner/operator of "Zneeks," a retail shoe store that caters to sneaker aficionados. He regularly works with customers who order small batches of custom shoes. Michael is interested in **using Cymbal Direct to manufacture and ship custom batches of shoes to these customers**. Reasonably tech-savvy but not a developer, Michael likes using Cymbal Direct's **partner purchase portal but wants the process to be easy**.

What is an example of a user story that could describe Michael's persona?

A. As a shoe retailer, Michael wants to **send Cymbal Direct custom purchase orders so that batches of custom shoes are sent to his customers.**

B. Michael is a **tech-savvy owner/operator** of a small business.

C. Zneeks is a **retail shoe store** that **caters to sneaker aficionados**.

D. Michael is reasonably tech-savvy but **needs Cymbal Direct's partner purchase portal to be easy.**

Google Cloud

Feedback:
A. Correct! "As a [type of user], I want to [do something] so that I can [get some benefit]" is the standard format for a user story.
B. Incorrect. This describes aspects of the user but not what they want to do or the benefit the user would receive.
C. Incorrect. This does not describe the user, what they want to do, or the benefit the user would receive.
D. Incorrect. This does not describe what he wants to do with the partner portal.

Where to look:
https://sre.google/workbook/engagement-model/

Content mapping:
- Architecting with Google Cloud: Design and Process (ILT)
  - M1 Defining Services
- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M1 Defining Services

Summary:
User stories describe one thing a user wants the system to do. Stories are written in a simple structure, typically using the format: *"As a [type of user], I want to [do something] so that I can [get some benefit]."* Stories should be simple, small, and testable and represent something that actually has value. A user can have multiple

stories associated with them, but the stories should be atomic so no story depends on another.

3.1 Diagnostic Question 04 Discussion

Cymbal Direct has an application running on a Compute Engine instance. You need to **give the application access** to several Google Cloud services. You **do not want to keep any credentials on the VM** instance itself.

What should you do?

A. Create a service account **for each of the services** the VM needs to access. Associate the service accounts with the Compute Engine instance.

B. Create a service account and **assign it the project owner role**, which enables access to any needed service.

C. Create a service account for the instance. Use **Access scopes** to enable access to the required services.

D. Create a service account with one or more **predefined or custom roles**, which give access to the required services.

Google Cloud

Feedback:
A. Incorrect. A Compute Engine instance is associated with only one service account.
B. Incorrect. This violates the "principle of least privilege" because assigning the project owner role gives access to unnecessary services.
C. Incorrect. Access scopes are used with the Compute Engine default service account.
D. Correct! This gives the flexibility and granularity needed to allow access to multiple services, without giving access to unnecessary services.

Where to look:
https://cloud.google.com/compute/docs/access/service-accounts

Content mapping:

- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security

- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M8 Security

Summary:
A service account is a special kind of account used by an application, service, or a virtual machine (VM) instance, not a person. Applications or services use service accounts to authenticate and make authorized API calls. To give access to a service or resources, the relevant IAM role must be granted to the service account. Another

aspect should also be considered: controlling who uses the service account. Assign the ServiceAccountUser role to the users you trust to use the service account.

3.1 Diagnostic Question 05 Discussion

Cymbal Direct wants to use Identity and Access Management (IAM) to allow employees to have **access to Google Cloud resources and services based on their job roles. Several employees are project managers and want to have some level of access** to see what has been deployed. The security team wants to ensure that securing the environment and managing resources is simple so that it will **scale.**

What approach should you use?

A. Grant access by assigning **custom** roles to groups. Use multiple groups for better control. Give access as low in the hierarchy as possible to prevent the inheritance of too many abilities from a higher level.

B. Grant access by assigning **predefined roles to groups.** Use multiple groups for better control. Give access as **low in the hierarchy as possible** to prevent the inheritance of too many abilities from a higher level.

C. Give access directly to each **individual** for more granular control. Give access as low in the hierarchy as possible to prevent the inheritance of too many abilities from a higher level.

D. Grant access by assigning **predefined roles to groups**. Use multiple groups for better control. Make sure you **give out access to all the children** in a hierarchy under the level needed, because child resources will not automatically inherit abilities.

Google Cloud

Feedback:
A. Incorrect. Unless there is a specific need for a custom role, you should use predefined ones.
B. Correct! This follows recommended practices regarding organizational policies.
C. Incorrect. Whenever possible, use groups to manage access. It is much easier to add or remove individuals from groups than manage permissions at the individual level.
D. Incorrect. Access is inherited by the descendants of a resource like a project or folder. You can give out more access at a lower level but cannot restrict access inherited from a parent.

Where to look:
https://cloud.google.com/iam/docs/resource-hierarchy-access-control

Content mapping:

- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security

- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M8 Security

Summary:
Select policies at the organization and project level. As new resources are added, they will automatically inherit the policies of their parents. This simplifies managing

policies and keeps permissions consistent. When adding a policy on a child resource, consider the access granted by the parent. Children inherit abilities and cannot restrict them. The principle of least privilege should always be applied, thus giving minimal access to roles and avoiding the use of owner and editor roles. The predefined roles have been designed to cover all use cases for resources. Custom roles should only be used where you need to make an exception and no predefined role meets your use case.

3.1 Diagnostic Question 06 Discussion

You have several Compute Engine instances running NGINX and Tomcat for a web application. In your web server logs, **many login failures come from a single IP address,** which looks like a brute force attack.

How can you block this traffic?

A. **Edit the Compute Engine instances** running your web application, and **enable Google Cloud Armor.** Create a Google Cloud Armor policy with a default rule action of "Allow." Add a new rule that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000).

B. Ensure that an HTTP(S) load balancer is configured to send traffic to the backend Compute Engine instances running your web server. Create a Google Cloud Armor policy with a **default rule action of "Deny."** Add a new rule that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000). Add the load balancer backend service's HTTP-backend as the target.

C. Ensure that an HTTP(S) load balancer is configured to send traffic to the backend Compute Engine instances running your web server. Create a Google Cloud Armor policy with a default rule action of "Allow." **Add a new rule that specifies the IP address causing the login failures** as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000). Add the load balancer backend service's HTTP-backend as the target.

D. Ensure that an HTTP(S) load balancer is configured to send traffic to your backend Compute Engine instances running your web server. Create a Google Cloud Armor policy **using the instance's local firewall** with a default rule action of "Allow." **Add a new local firewall rule** that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000).

Google Cloud

Feedback:
A. Incorrect. Google Cloud Armor can't be associated directly with a Compute Engine instance and instead is applied at the edge via a load balancer or a Cloud CDN.
B. Incorrect. A default rule action of "deny" would block all access. The additional rule is redundant.
C. Correct! Configuring a Google Cloud Armor rule to prevent that IP address from accessing the HTTP-backend on the load balancer will prevent access.
D. Incorrect. Google Cloud Armor allows you to block traffic outside your VPC, which prevents load on your systems.

Where to look:
https://cloud.google.com/armor/docs/cloud-armor-overview

Content mapping:
- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security
- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M8 Security

Summary:
Google Cloud Armor offers built-in DDoS protection and protection against application-aware attacks such as cross-site scripting and SQL injection. Google Cloud Armor is integrated into global HTTP(S) load balancing. Google Cloud Armor is

based on the same technologies and global infrastructure used to protect Google's own services. Google Cloud Armor's security policies enable the access or denial of requests at the load balancers. Google Cloud Armor blocks unwelcome traffic before it gets to your VPC networks and incurs costs.

3.1 Diagnostic Question 07 Discussion

Cymbal Direct needs to make sure its new social media integration service **can't be accessed directly from the public internet.** You want to **allow access only through the web frontend store**.

How can you prevent access to the social media integration service from the outside world, but still **allow access to the APIs** of social media services?

A. **Remove external IP addresses** from the VM instances running the social media service and place them in a private VPC behind **Cloud NAT**. Any SSH connection for management should be done with **Identity-Aware Proxy (IAP)** or a **bastion host (jump box)** after allowing SSH access from IAP or a corporate network.

B. **Limit access to the external IP addresses** of the VM instances using firewall rules and place them in a private VPC behind Cloud NAT. Any SSH connection for management should be done with Identity-Aware Proxy (IAP) or a bastion host (jump box) after allowing SSH access from IAP or a corporate network.

C. **Limit access to the external IP addresses** of the VM instances using a firewall rule to block all outbound traffic. Any SSH connection for management should be done with Identity-Aware Proxy (IAP) or a bastion host (jump box) after allowing SSH access from IAP or a corporate network.

D. **Remove external IP addresses** from the VM instances running the social media service and place them in a private VPC behind **Cloud NAT**. Any SSH connection for management should be restricted to corporate network IP addresses by Google Cloud Armor.

Google Cloud

Feedback:
A. Correct! Using Cloud NAT will prevent inbound access from the outside world but will allow connecting to social media APIs outside of the VPC. Using IAP or a bastion host allows for management by SSH, but without the complexity of using VPNs for user access.
B. Incorrect. If VMs do not need to be accessed by the outside world, they should not have external IP addresses.
C. Incorrect. If VMs do not need to be accessed by the outside world, they should not have external IP addresses, and denying all outbound traffic would prevent connecting to external social media APIs.
D. Incorrect. Without using IAP or a bastion host, the corporate network would have no way of connecting to the VMs, because VMs have no external IP addresses.

Where to look:
https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept

Content mapping:
- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security
- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M8 Security

Summary:

Several options are available for securely communicating with VMs that do not have public IP addresses. These services do not have a public IP address normally because the VMs are deployed in order to be consumed by other instances in the project or through Dedicated Interconnect options. However, for those instances without an external IP address, it can be a requirement to gain external access; for example, for updates or patches to be applied. In this question, the VMs need to access social media APIs. Cloud NAT can allow for outbound access, and IAP or a bastion host can allow SSH access.

3.1 Diagnostic Question 08 Discussion

Cymbal Direct is experiencing success using Google Cloud and you want to leverage tools to make your solutions more efficient. Erik, one of the original web developers, currently adds new products to your application manually. Erik has many responsibilities and requires a long lead time to add new products. You need to create a Cloud Functions application to l**et Cymbal Direct employees add new products** instead of waiting for Erik. However, you want to make sure that **only authorized employees** can use the application.

What should you do?

A. Set up Cloud VPN between the corporate network and the Google Cloud project's VPC network. Allow **users** to connect to the Cloud Functions instance.

B. Use Google Cloud Armor to restrict access to the corporate network's external IP address. Configure firewall rules to allow only HTTP(S) access.

C. Create a **Google group** and add authorized employees to it. Configure Identity-Aware Proxy (IAP) to the Cloud Functions application as a HTTP-resource. Add the group as a principle with the role **"Project Owner."**

D. Create a **Google group** and add authorized employees to it. Configure Identity-Aware Proxy (IAP) to the Cloud Functions application as a HTTP-resource. Add the group as a principle with the role **"IAP-secured Web App User."**

Google Cloud

Feedback:
A. Incorrect. Although this solution restricts access to just the corporate network, it doesn't restrict the application to authorized users.
B. Incorrect. Although this solution permits access to only the corporate network's public IP address, it doesn't restrict the application to authorized users. HTTP(S) is always recommended, especially when the traffic uses the internet, but doesn't address the real problem.
C. Incorrect. Project Owner gives out much more access than necessary and doesn't adhere to the "Principle of Least Privilege." This solution also doesn't allow access to the Cloud Function.
D. Correct! You could use individual accounts to give out access instead of a group, and by doing so you make access more manageable. Identity-Aware Proxy is a great tool for exactly this kind of issue.

Where to look:
https://cloud.google.com/iap/docs/App Engine-quickstart
https://cloud.google.com/functions/docs/quickstarts

Content mapping:
- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security
- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M8 Security

Summary:
IAP lets you require that users be signed in to Google accounts (groups, service accounts, and Workspace domains are fine, too). You can authorize users' access to individual applications without having to write code.

3.1 Diagnostic Question 09 Discussion

You've recently created an internal Cloud Run application for developers in your organization. The application lets **developers clone production Cloud SQL databases into a project specifically created to test code and deployments**. Your previous process was to export a database to a Cloud Storage bucket, and then import the SQL dump into a legacy on-premises testing environment database with connectivity to Google Cloud via Cloud VPN. Management wants to **incentivize using the new process with Cloud SQL** for rapid testing and track how frequently rapid testing occurs.

How can you ensure that the developers use the new process?

A. **Use an ACL on the Cloud Storage bucket.** Create a read-only group that only has viewer privileges, and ensure that the developers are in that group.

B. Leave the ACLs on the Cloud Storage bucket as-is. **Disable Cloud VPN**, and have developers use Identity-Aware Proxy (IAP) to connect. Create an organization policy to enforce public access protection.

C. Use **predefined roles to restrict access** to what the developers are allowed to do. Create a group for the developers, and associate the group with the Cloud SQL Viewer role. Remove the "cloudsql.instances.export" ability from the role.

D. Create a **custom role to restrict access** to what developers are allowed to do. Create a group for the developers, and associate the group with your custom role. Ensure that the custom role does not have "cloudsql.instances.export."

Google Cloud

Feedback:
A. Incorrect. This only prevents developers from writing to that bucket. Depending on their other roles, they may be able to create new buckets to use as a workaround. If the developers are testing deployments, they probably have this ability.
B. Incorrect. Disabling Cloud VPN may have other effects and could cause problems. You would use IAP more often for serverless instances, or endpoints, and for ensuring authentication. The organization policy would prohibit sharing data to accounts outside your organization.
C. Incorrect. You cannot add or remove abilities to a predefined role. Predefined roles are managed by Google.
D. Correct! In this scenario, using a predefined role is inappropriate because the most appropriate predefined role, Cloud SQL Viewer, contains the cloudsql.instances.export capability, which would allow the database to be exported.

Where to look:
https://cloud.google.com/iam/docs/understanding-custom-roles

Content mapping:
- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security
- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M8 Security

Summary:
Custom roles are user-defined and allow bundling one or more supported permissions to meet your specific needs. Custom roles are not maintained by Google; when new permissions, features, or services are added to Google Cloud, your custom roles will not be updated automatically.

3.1 Designing for security

Resources to start your journey

Google Cloud Architecture Framework: Security, privacy, and compliance

IAM best practice guides available now | Google Cloud Blog

Using resource hierarchy for access control | IAM Documentation | Google Cloud

Chapter 18 - SRE Engagement Model

Service accounts | Compute Engine Documentation | Google Cloud

Google Cloud Armor overview

Private clusters | Kubernetes Engine Documentation | Google Cloud

Understanding IAM custom roles | IAM Documentation | Google Cloud

Google Cloud

You just reviewed several diagnostic questions that addressed different aspects of designing for security. These are some links to learn more about the concepts in these questions. They provide a starting point to explore Google-recommended practices in designing for security.

https://cloud.google.com/architecture/framework/security
https://cloud.google.com/iam/docs/resource-hierarchy-access-control
https://cloud.google.com/blog/products/identity-security/iam-best-practice-guides-available-now
https://sre.google/workbook/engagement-model
https://cloud.google.com/compute/docs/access/service-accounts
https://cloud.google.com/armor/docs/cloud-armor-overview
https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept
https://cloud.google.com/iam/docs/understanding-custom-roles

3.2 Designing for compliance

Considerations include:

- Legislation (e.g., health record privacy, children's privacy, data privacy, and ownership)
- Commercial (e.g., sensitive data such as credit card information handling, personally identifiable information [PII])
- Industry certifications (e.g., SOC 2)
- Audits (including logs)

Google Cloud

As a Professional Cloud Architect, you need to be aware of any compliance requirements for your cloud solutions, such as privacy legislation, PII, industry certifications, or audits. After you've identified potential areas of concern, look into laws governing the management of that kind of data. Review Google's documentation on compliance, and make sure you are familiar with where you can leverage the shared responsibility model.

Question 10 tested your knowledge of using Security Command Center to help identify vulnerabilities.

3.2 Diagnostic Question 10 Discussion

Your client is legally required to comply with the Payment Card Industry Data Security Standard (PCI-DSS). The client has formal audits already, but the audits are only done periodically. The client needs to **monitor for common violations** to meet those requirements more easily. The client does not want to replace audits but wants to engage in **continuous compliance** and catch violations early.

What would you recommend that this client do?

A. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Premium tier**. Export or view the PCI-DSS Report from the SCC dashboard's **Compliance tab**.

B. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Standard tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Compliance tab.**

C. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Premium tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Vulnerabilities tab**.

D. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Standard tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Vulnerabilities tab.**

Google Cloud

Feedback:
A. Correct! The reports relating to compliance vulnerabilities are on the Compliance tab. To use the Security Health Analytics that scan for common compliance vulnerabilities, you must use the Premium tier.
B. Incorrect. To use the Security Health Analytics that scan for common compliance vulnerabilities, you must use the Premium tier.
C. Incorrect. The reports relating to compliance vulnerabilities are on the Compliance tab.
D. Incorrect. The reports relating to compliance vulnerabilities are on the Compliance tab. To use the Security Health Analytics that scan for common compliance vulnerabilities, you must use the Premium tier.

Where to look:
https://cloud.google.com/security-command-center/

Content mapping:
- Architecting with Google Cloud: Design and Process (ILT)
  - M8 Security
- Reliable Google Cloud Infrastructure: Design and Process (On-demand)
  - M8 Security

Summary:
You can use the Security Command Center to detect many well-known vulnerabilities

in your applications and instances. The Standard tier is available at no cost, but is more limited in what it can detect. For customers who have compliance requirements to meet, it is worth considering the Premium tier option, but it's important to realize that it is not a replacement for audits, but is simply a tool to make compliance easier.

3.2 Designing for compliance

Resources to start your journey

Manage compliance obligations | Architecture Framework | Google Cloud
Cloud Compliance & Regulations Resources
Assuring Compliance in the Cloud
Security Command Center | Google Cloud

Google Cloud

The diagnostic question we just reviewed covers one scenario where you would need to address compliance considerations in your solution design. These links provide a starting point to learn more about ensuring compliance in Google Cloud solutions.

https://cloud.google.com/architecture/framework/security/compliance
https://cloud.google.com/security/compliance
https://services.google.com/fh/files/misc/assuringcompliance_in_the_cloud.pdf
https://cloud.google.com/security-command-center/