

Preparing for Your Professional Cloud Architect Journey

Module 3: Designing for Security and Compliance

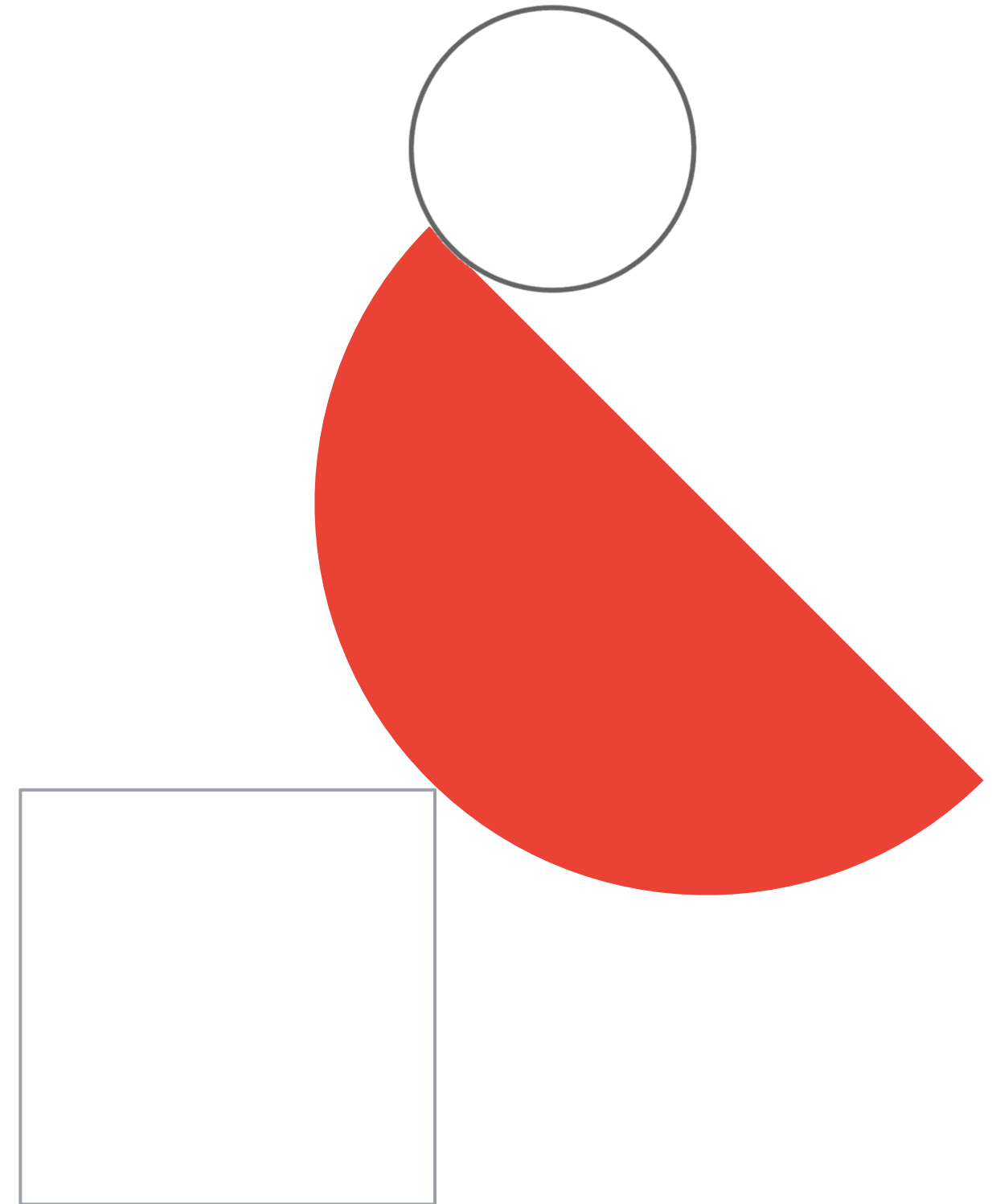


Module agenda

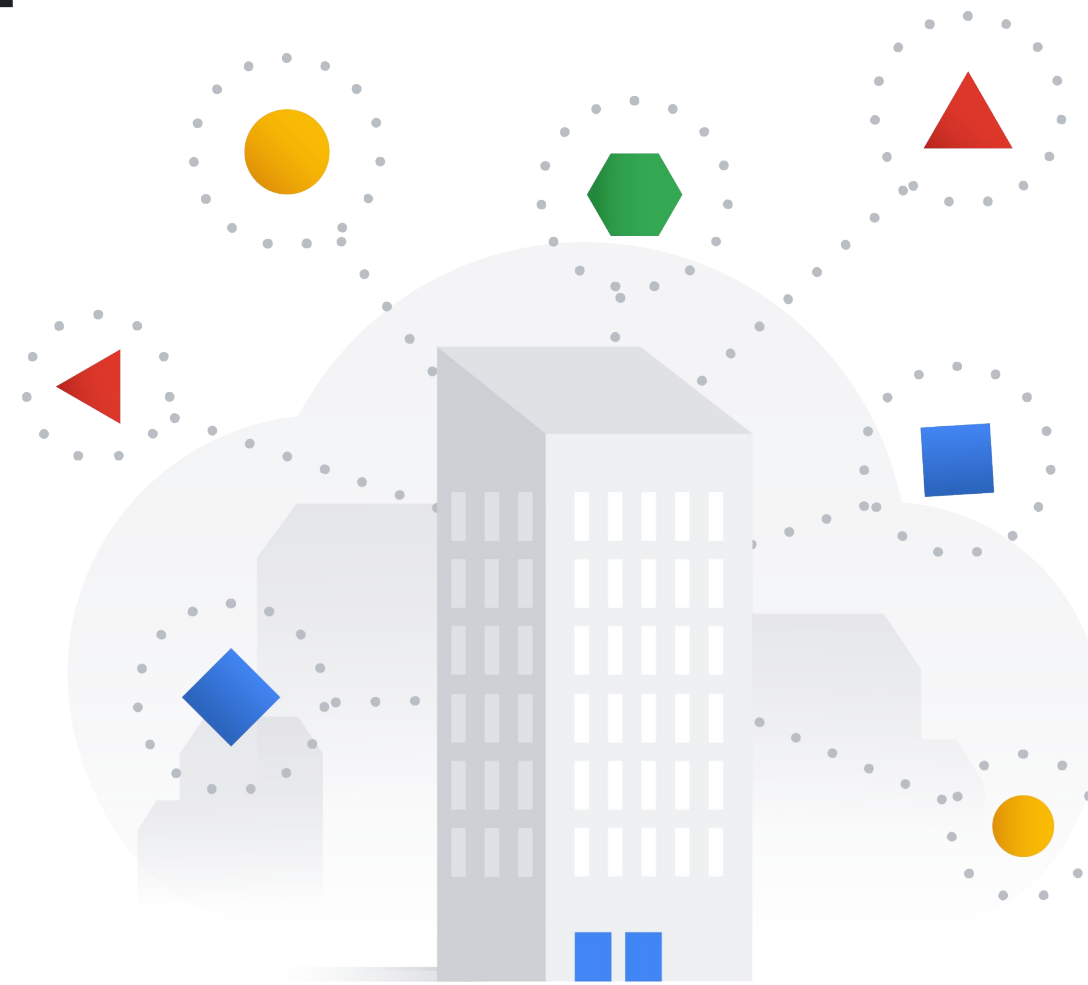
- 01 Designing for security and compliance with Cymbal Direct's cloud solution
- 02 Diagnostic questions
- 03 Review and study planning



Designing for security and compliance with Cymbal Direct's cloud solution



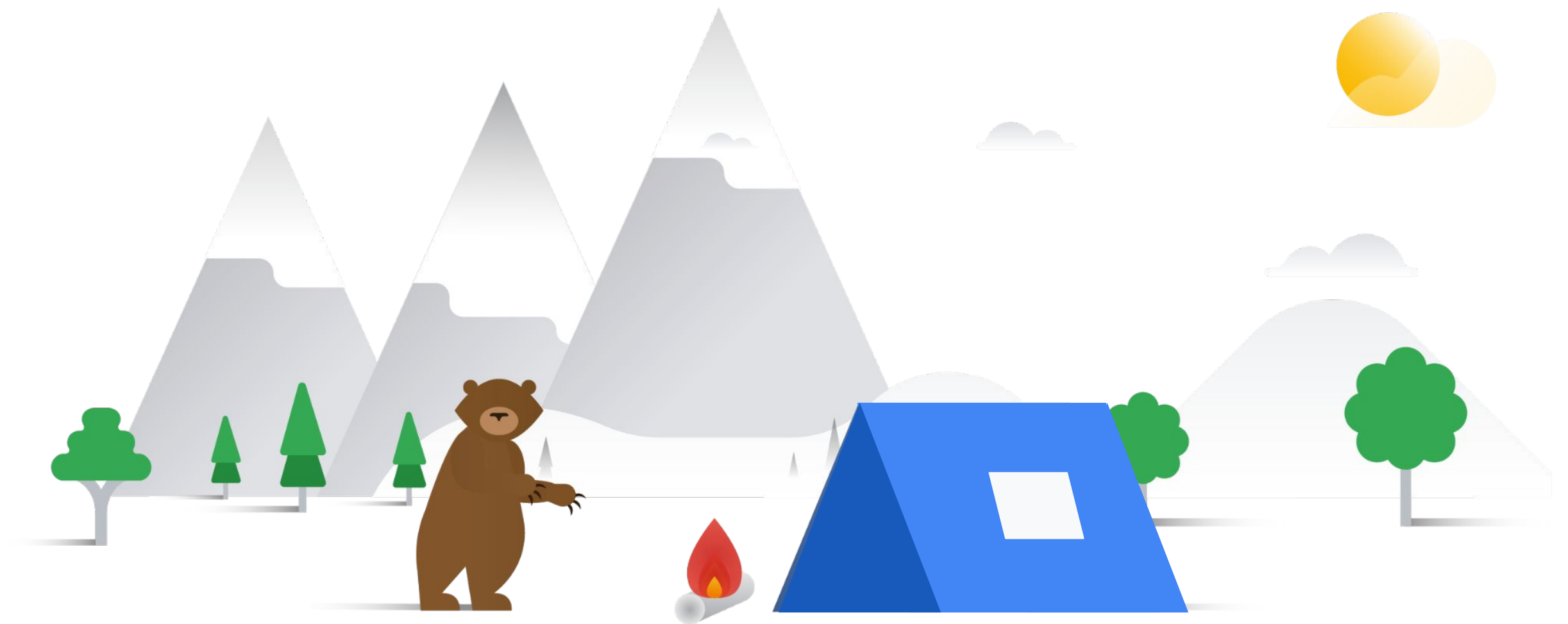
Your role in architecting a secure and compliant cloud solution



- Designing for security
- Designing for compliance

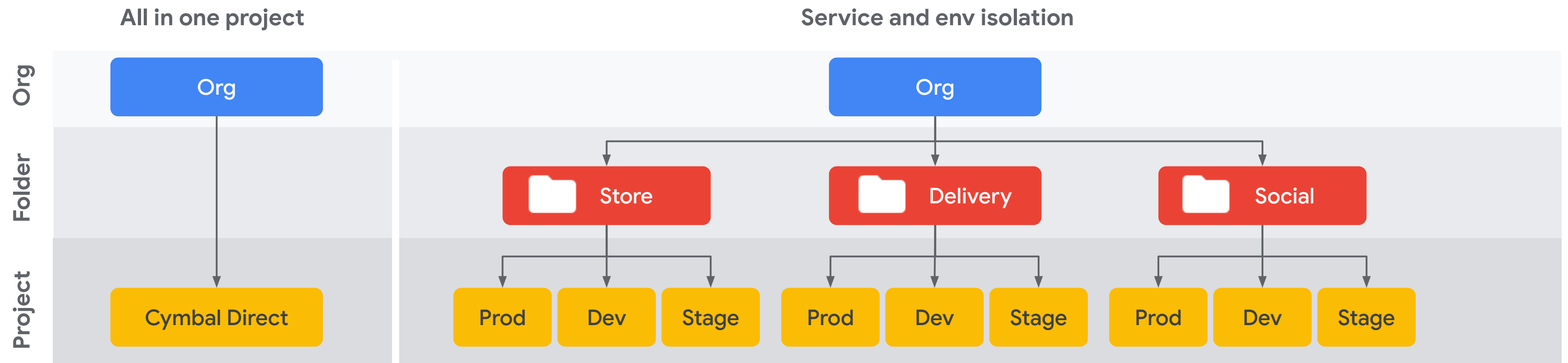


The parable of the campers and the bear



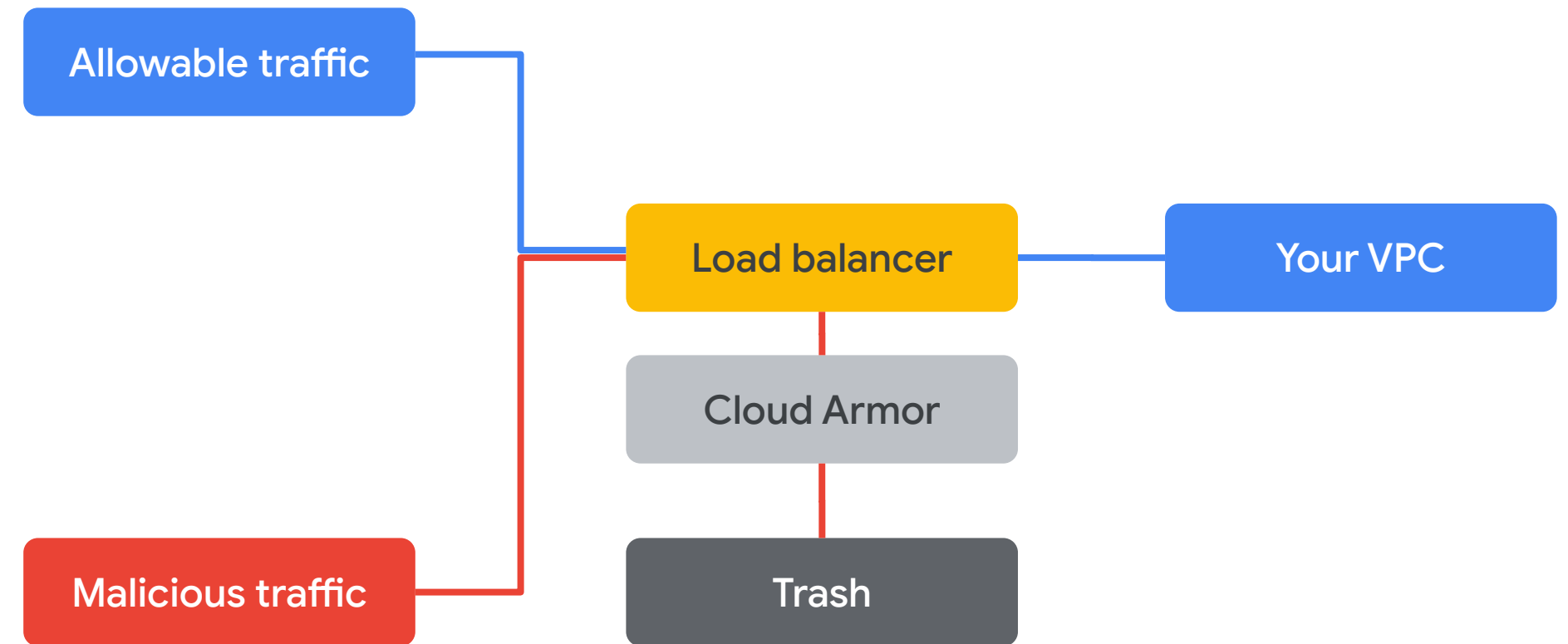
Projects

- Projects limit access.
- Projects limit the scope of damage.
- Projects are in your resource hierarchy.



Security is woven into everything

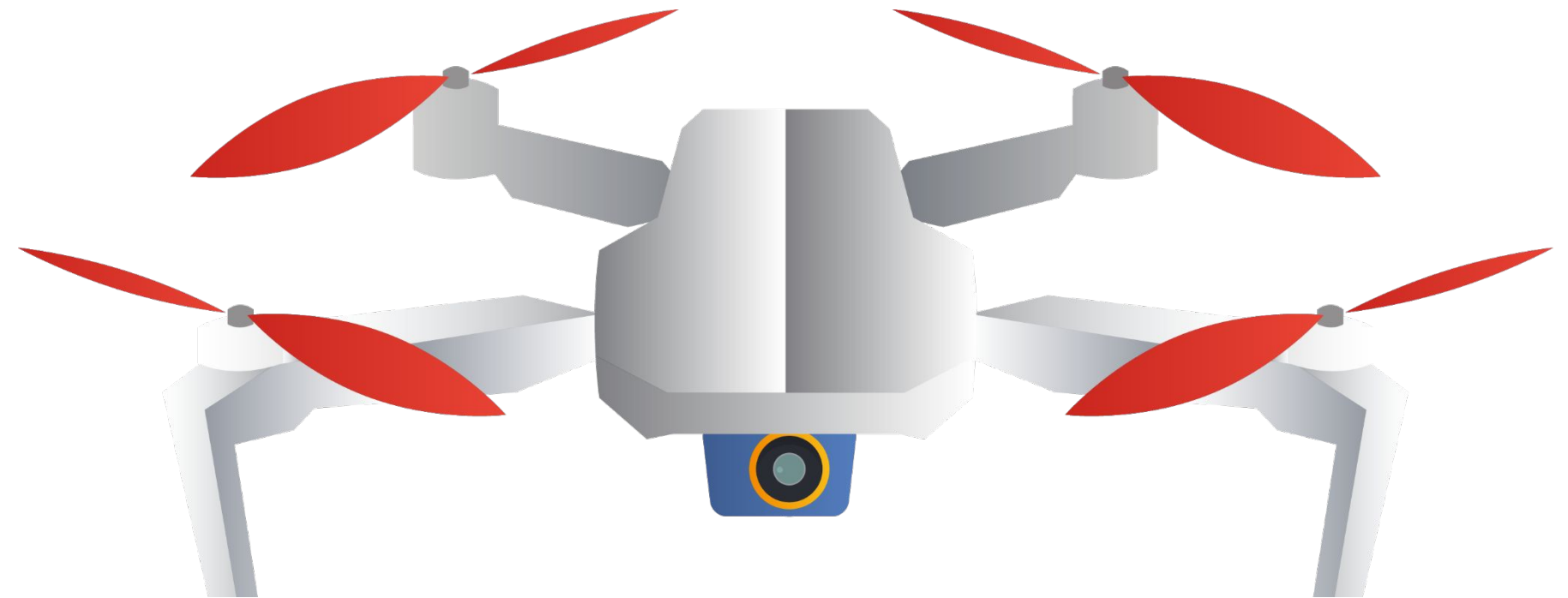
- Projects aren't just for security
- Virtually all services and tools in Google Cloud have security options



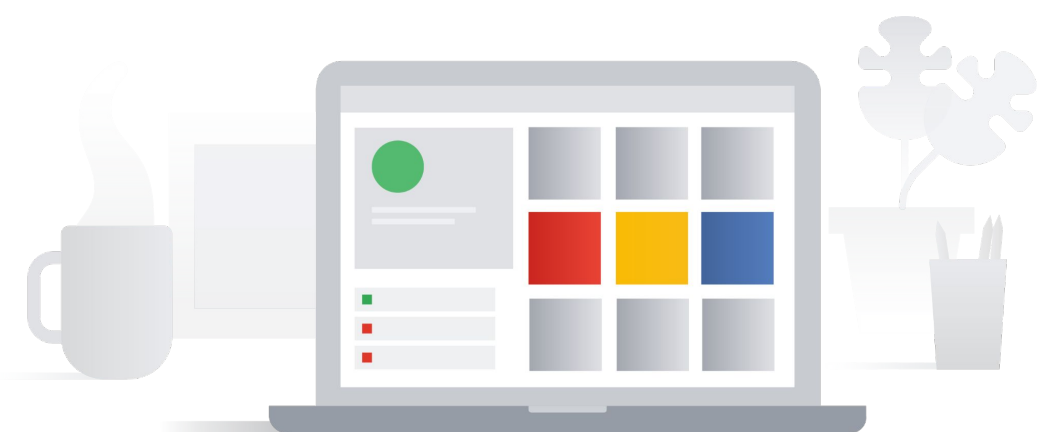
Considering potential compliance issues for Cymbal Direct

What happens if...

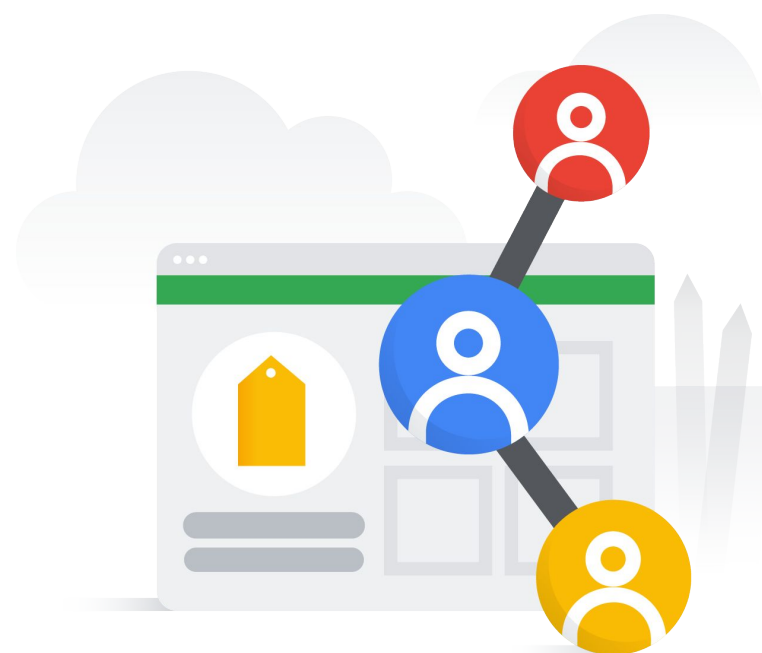
- A drone records video of PII?
- Inappropriate social media content is imported?



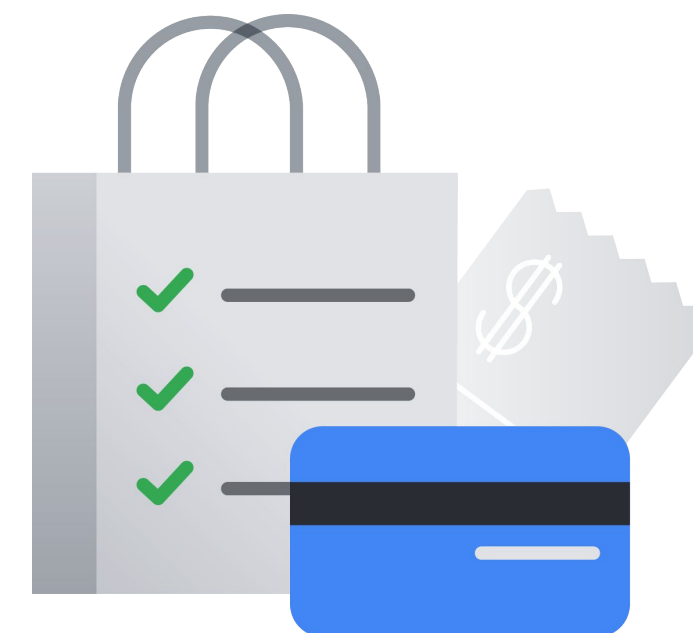
Compliance



Drones &
Social Media

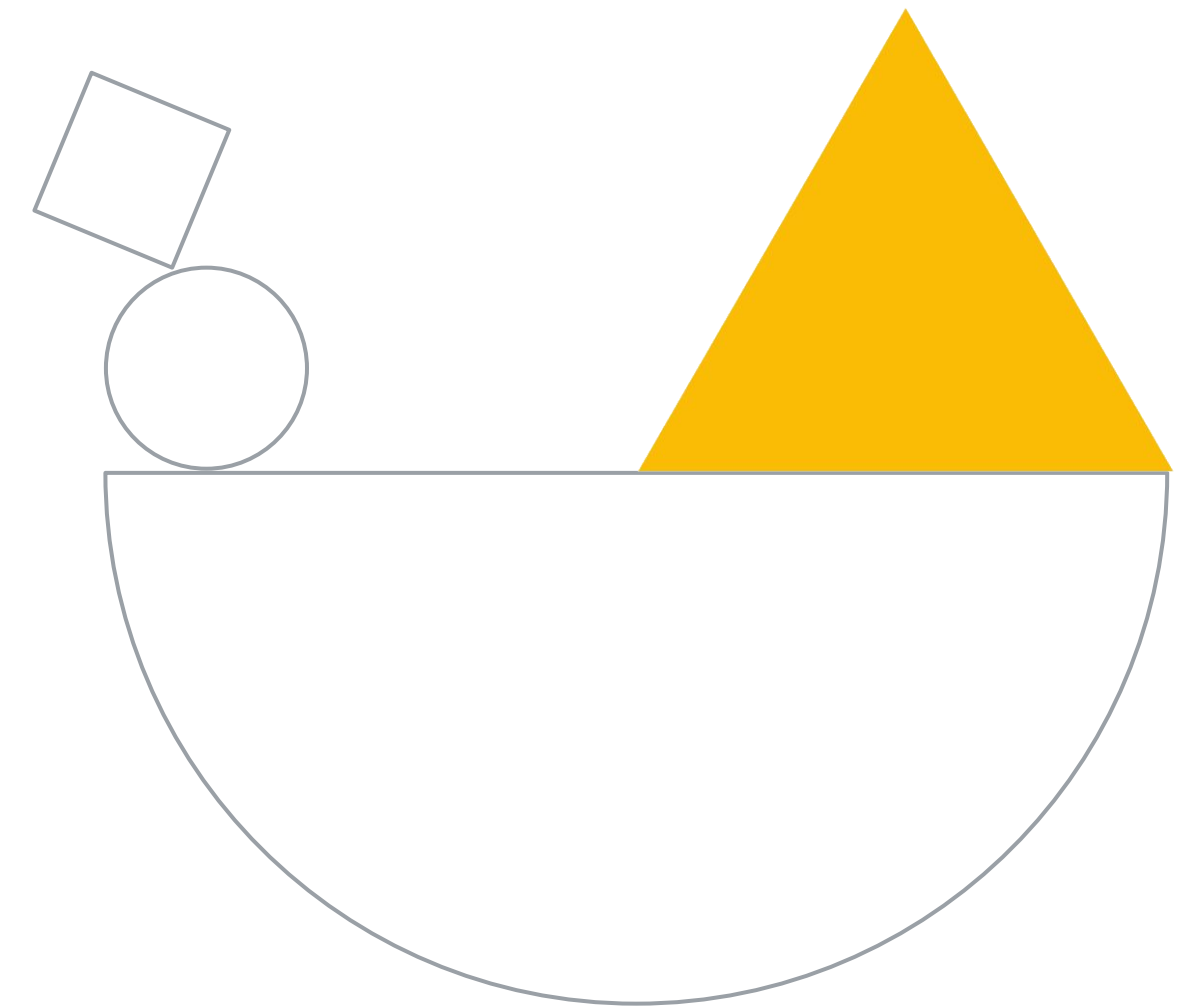


Retention



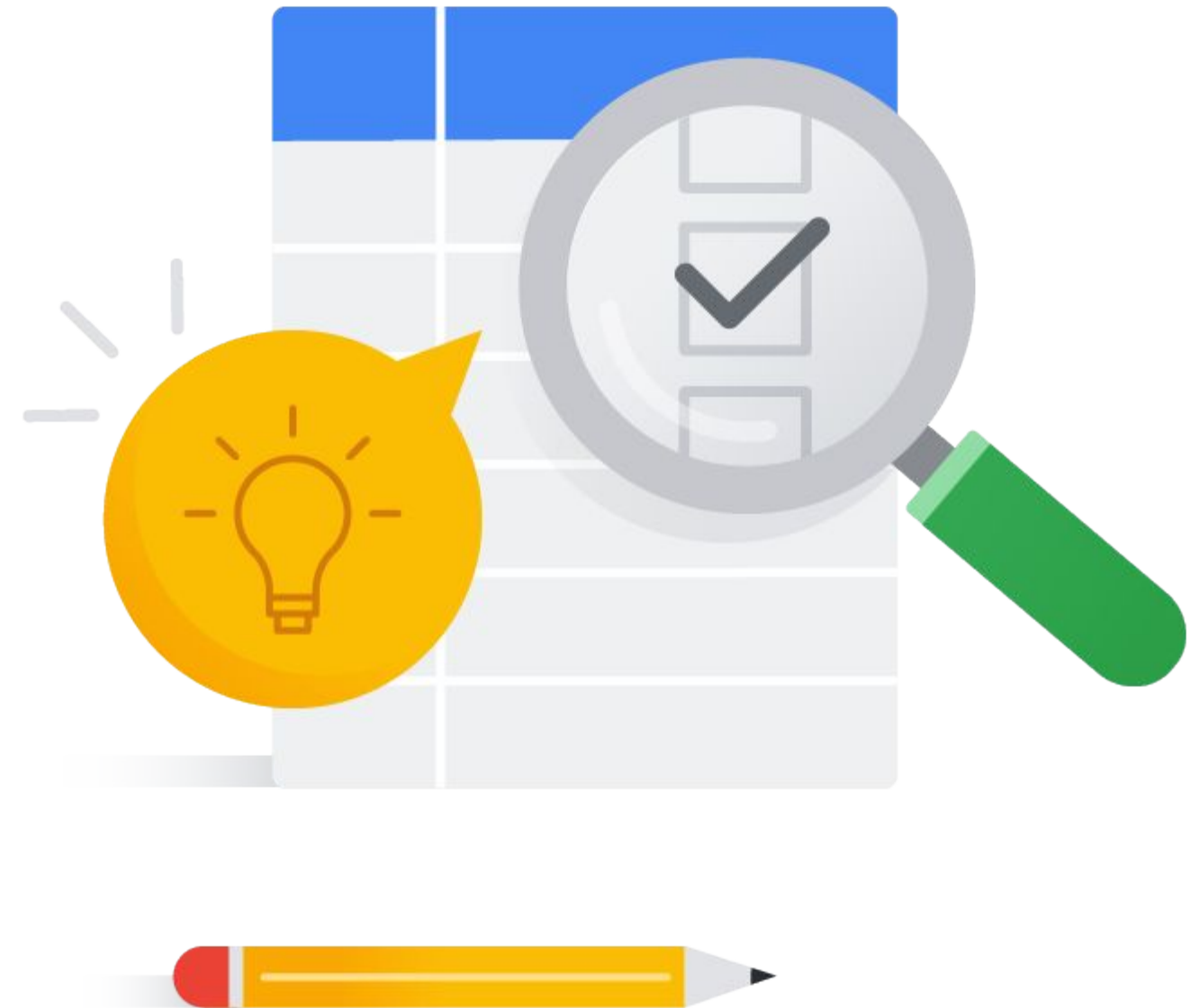
Credit
Cards

Diagnostic questions

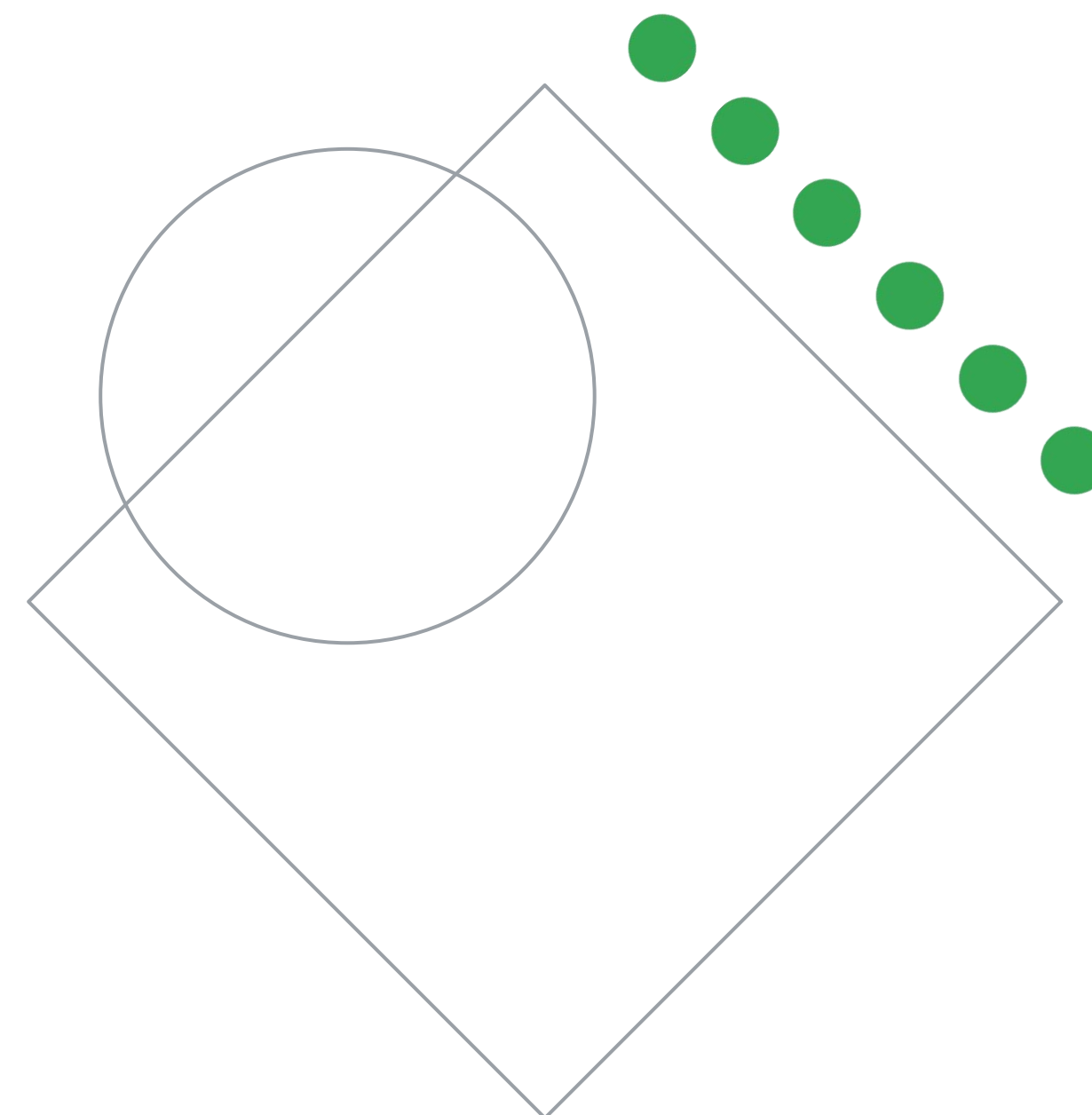


Please complete the diagnostic questions now

- The diagnostic questions are available in the workbook.

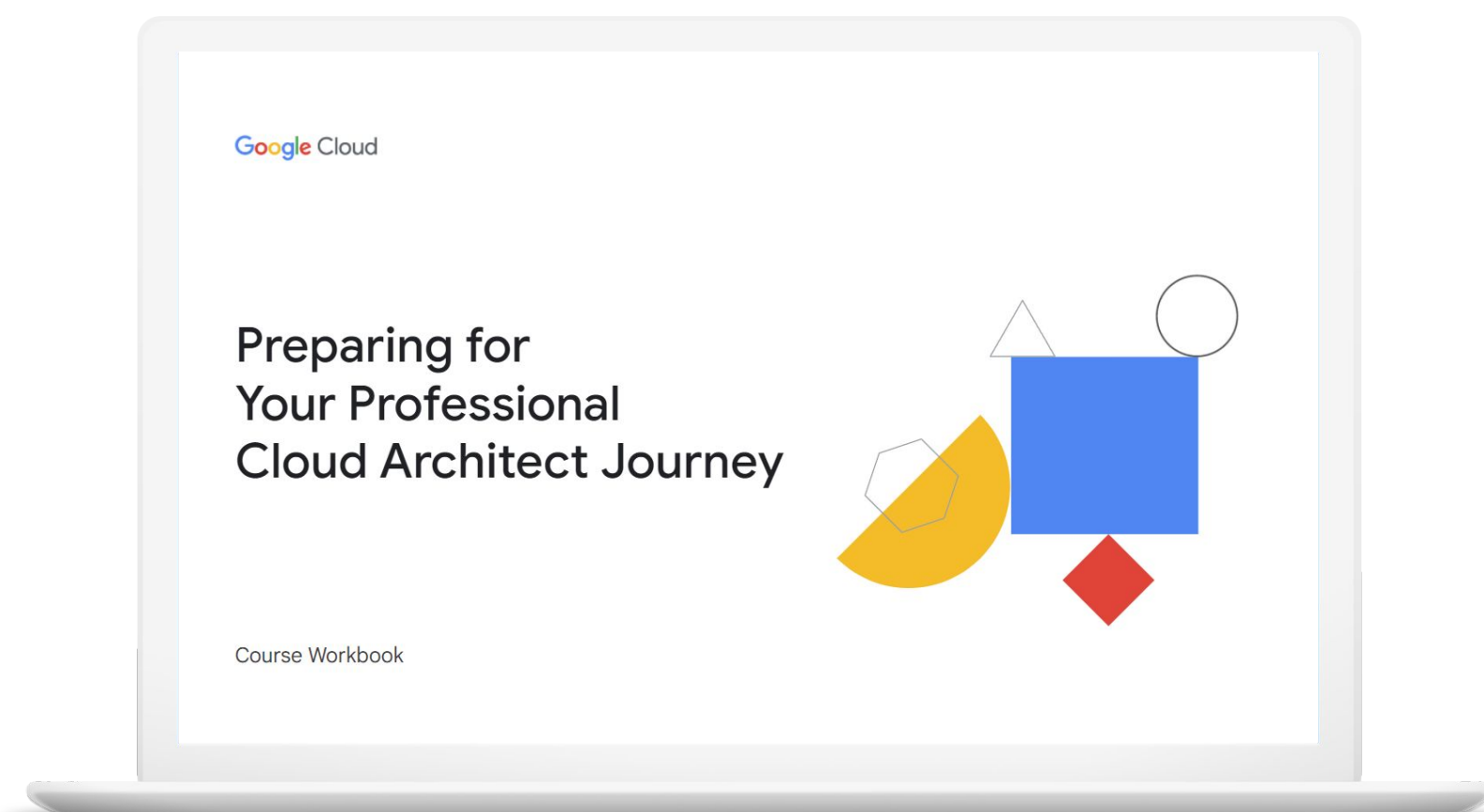


Review and study planning



Your study plan:

Designing for security and compliance



3.1

Designing for security

3.2

Designing for compliance

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

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.

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.

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.

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.

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.**

- 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.**

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

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.**

- 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.**

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

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.

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.

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.



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.



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).



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).



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.



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.



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 **let 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.**"



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 **let 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.**"



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."



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."



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](#)

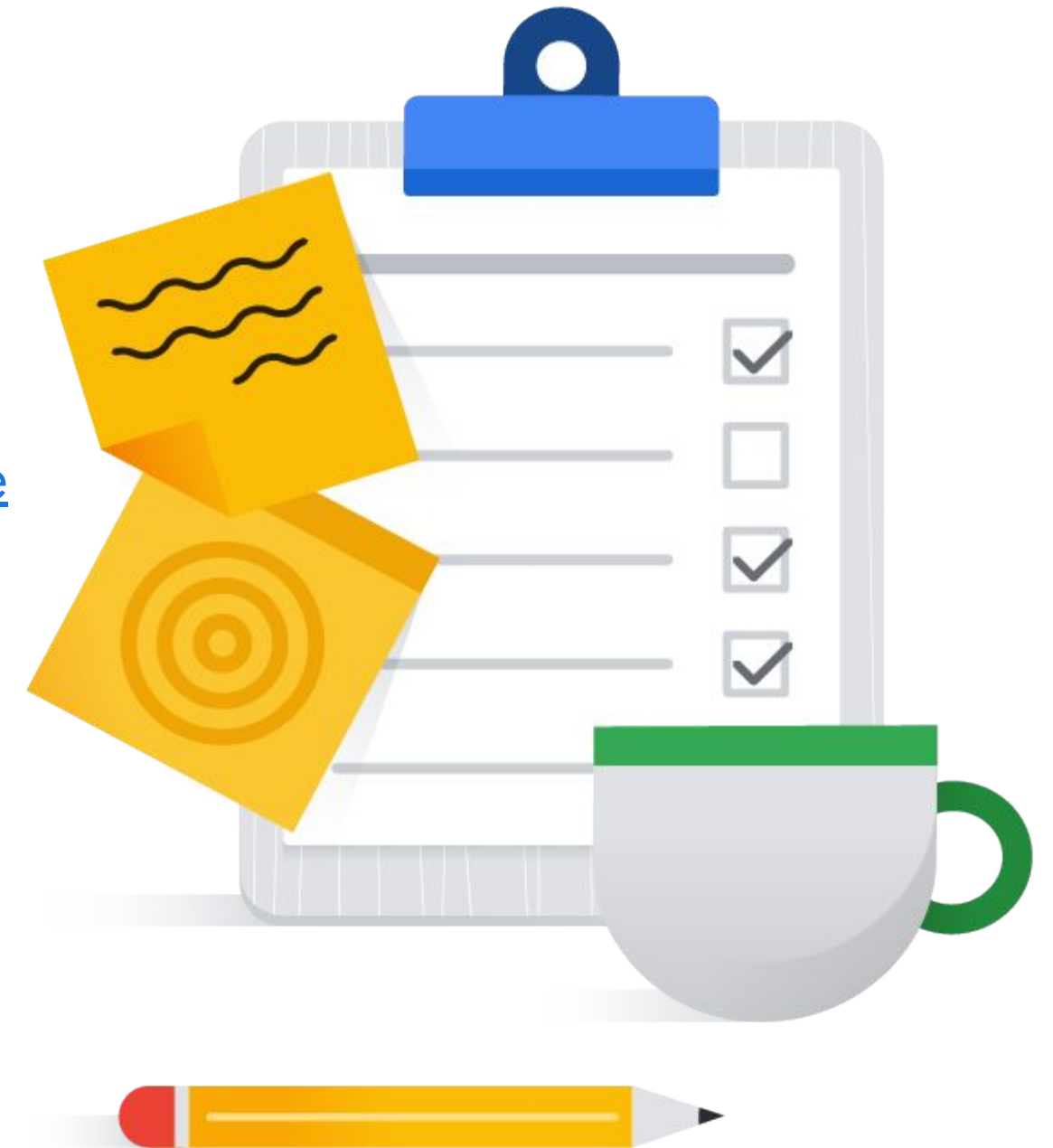
[Chapter 18 - SRE Engagement Model](#)

[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](#)



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)

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**.

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**.

32 | Designing for compliance

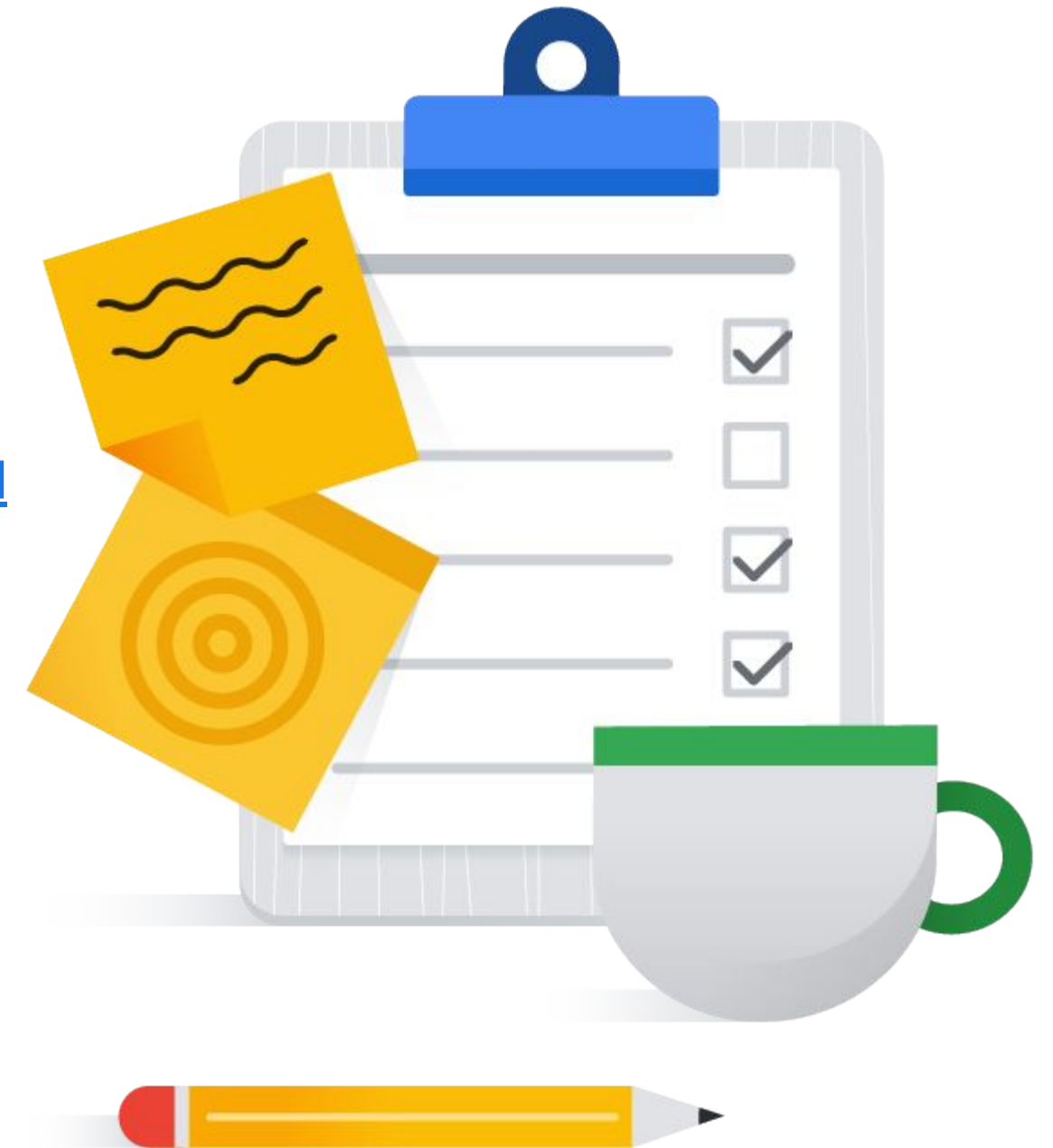
Resources to start your journey

[Manage compliance obligations | Architecture Framework | Google Cloud](#)

[Cloud Compliance & Regulations Resources](#)

[Assuring Compliance in the Cloud](#)

[Security Command Center | Google Cloud](#)



Knowledge Check 1

Cymbal Direct has chosen to use multiple projects for their environment. How do you describe this choice?

- A. Unnecessary. Using multiple projects adds little to no benefits.
- B. Using multiple projects only adds security benefits.
- C. Using multiple projects adds both security and other benefits.
- D. Using multiple projects requires creating separate IAM policies at each project level



Knowledge Check 1

Cymbal Direct has chosen to use multiple projects for their environment. How do you describe this choice?

- A. Unnecessary. Using multiple projects adds little to no benefits.
- B. Using multiple projects only adds security benefits.
- C. Using multiple projects adds both security and other benefits.
- D. Using multiple projects requires creating separate IAM policies at each project level



Knowledge Check 2

What type of data might be inadvertently picked up by a drone during a delivery?

- A. Healthcare data regulated by privacy laws
- B. Financial data regulated by banking laws
- C. Classified government data
- D. Video of private property



Knowledge Check 2

What type of data might be inadvertently picked up by a drone during a delivery?

- A. Healthcare data regulated by privacy laws
- B. Financial data regulated by banking laws
- C. Classified government data
- D. Video of private property

