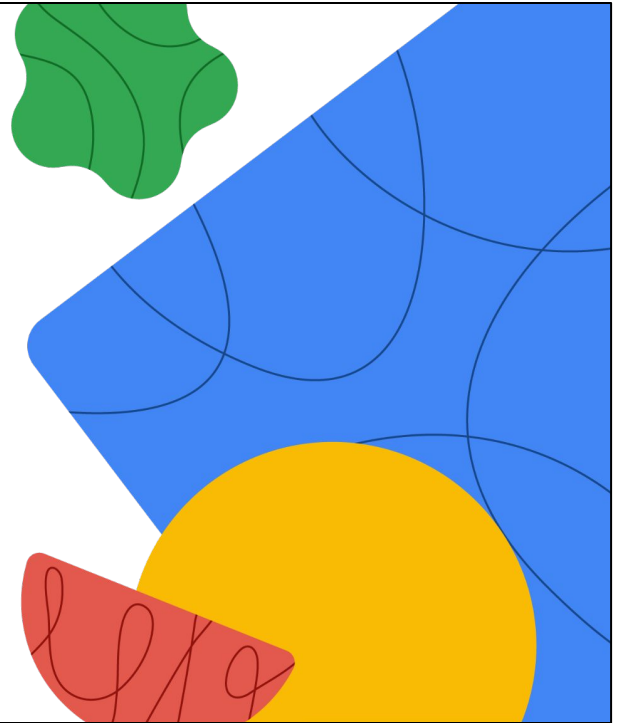





Preparing for your Professional Cloud Security Engineer Journey

Section 5:
Supporting Compliance Requirements



In this module you'll learn about the final area of the Professional Cloud Security Engineer's role at Cymbal Bank. Once the identity and access management, network, data, and operations security have been addressed, the final area of focus is on satisfying and maintaining security regulator compliance with a chosen set of standards. This corresponds to the fifth and final section of the Professional Cloud Security Engineer exam guide.



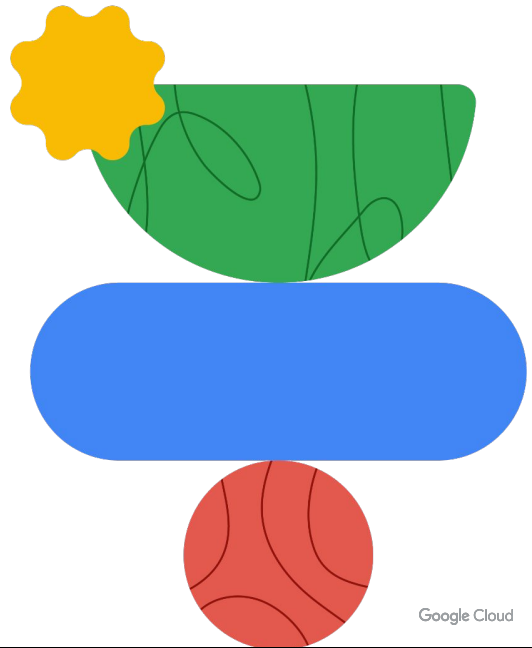
Module agenda

- 01 Cymbal Bank's security regulatory compliance
- 02 Diagnostic questions
- 03 Review and study planning

As in previous modules, we'll begin by exploring what this aspect of your role looks like at Cymbal Bank. Next, you'll assess your skills in this section through 5 diagnostic questions.

Then, we'll review these questions. Based on the areas you need to learn more about, you'll identify resources to include in your study plan.

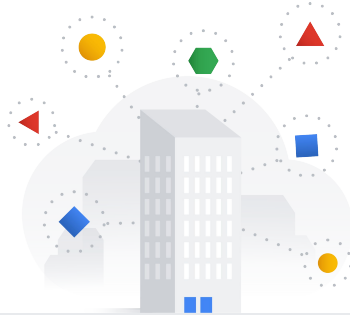
Cymbal Bank's security regulatory compliance



Google Cloud

Let's explore how a Professional Cloud Security Engineer at Cymbal Bank helps ensure security regulatory compliance.

Ensuring security regulatory compliance at Cymbal Bank



- Adhering to regulatory and industry standards requirements for the cloud



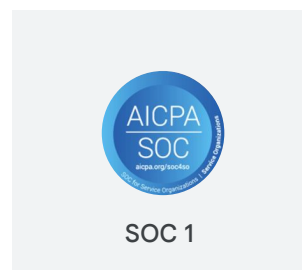
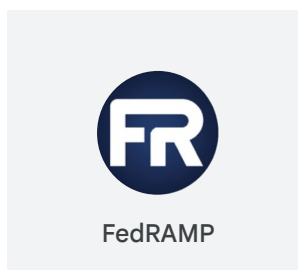
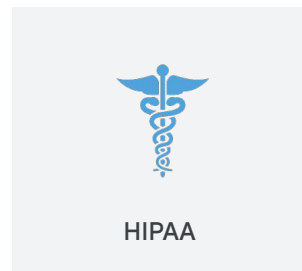
The final area of concern for the Professional Cloud Security Engineer is ensuring compliance with a chosen set of security standards. An organization's standards depend on the business and competitive landscape, and can include such standards as HIPAA, PCI-DSS, The ISO 27000 Series, The NIST cybersecurity framework, CIS critical security controls, FedRAMP, SOC1 and SOC2, and many others.

These standards typically specify requirements related to:

- How authentication, authorization, and access control can be performed;
- How data is encrypted and otherwise secured;
- How key management is performed; and,
- How networks, computing, and storage resources are monitored, secured, and maintained.

Google Cloud meets many third-party and government compliance standards worldwide

- Google Cloud has been certified as secure, but that does not mean that applications built on Google Cloud are automatically certified.
- Cymbal Bank does not need to worry about getting Google Cloud tools and services certified, only those services you build on top of Google Cloud.



Google Cloud

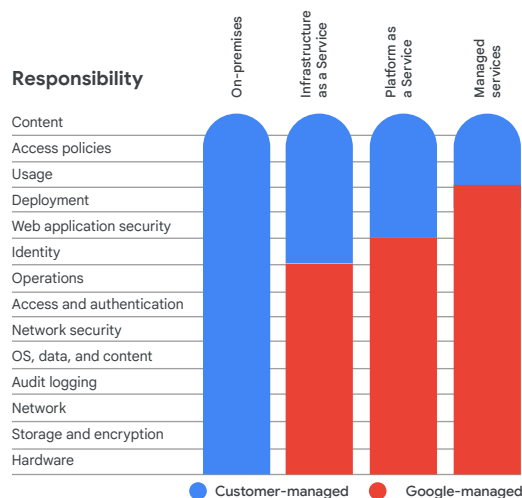
Google Cloud meets many third-party and government compliance standards worldwide. Cymbal Bank will be building on top of Google Cloud, and can leverage the compliance built into the infrastructure of Google Cloud. However, as a Professional Cloud Security Engineer, you will need to help ensure that the applications and services Cymbal Bank builds on top of this infrastructure are also compliant with your chosen standards. Google Cloud has been certified as secure, but that does not mean that applications built on Google Cloud are automatically certified.

Google products undergo regular independent verification of security privacy and compliance controls. To help customers with compliance and reporting, Google shares information and best practices, and provides access to documentation. ISO/IEC 27001, HIPAA, FedRAMP, and SOC 1 are just a sample of the compliance offerings of Google Cloud. For the full set, visit <https://cloud.google.com/security/compliance/offerings/#/>.

Cymbal Bank does not need to worry about getting Google Cloud tools and services certified, only those services you build on top of Google Cloud. It is important to note that when deploying services on Google Cloud, it is still necessary to ensure that you follow applicable standards. Guidelines are provided by Google for some standards. For example, for Google provides you with documentation on how to set up a HIPAA-aligned project. See the link for more details: <https://cloud.google.com/solutions/setting-up-a-hipaa-aligned-project>.

Cymbal Bank collaborates with Google Cloud to ensure security compliance

- Google is responsible for managing its infrastructure security.
- You are responsible for securing your virtual infrastructure, workloads and data.
- Google helps you with best practices, templates, products, and solutions.



Google Cloud

In the cloud, an important concept is the shared responsibility model. The cloud provider (Google) is responsible for the shared physical infrastructure and managing its security. When working in an infrastructure as a service model, the customer (in this case, Cymbal Bank) is responsible for securing the virtual infrastructure built over top of the physical infrastructure, the workloads running in that virtual infrastructure, and data. When working in other more managed approaches Google can take over more responsibility for the virtual infrastructure and its security.

Depending on how a customer works in the cloud, this can involve more or less security responsibility and effort to ensure security compliance. Google helps you by providing best practices, templates, products, and solutions.

Encryption in the context of security compliance

- Default at rest encryption provided by Google Cloud
- Options for encryption at rest with varying degrees of control over keys and key storage
- Optional hardened hardware-based key storage with Cloud HSM
- Default encryption in motion when data is transferred across physical boundaries controlled by Google Cloud
- Optional application layer encryption in motion for auditable end-to-end encryption



Google Cloud

Cymbal Bank will use Google Cloud's default encryption at rest where compliance does not require conflicting key control or storage requirements.

Where there is such conflict, you can leverage customer managed encryption keys (CMEK), customer supplied encryption keys (CSEK), or externally managed keys (EKM). These options provide encryption at rest with varying degrees of control over keys and key storage.

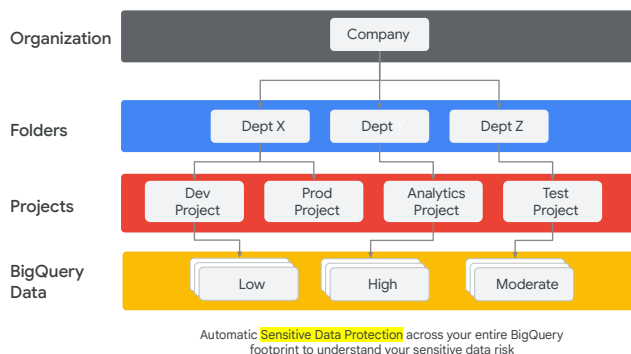
Where compliance requirements dictate, you can also store keys in hardware-based hardened key storage appliances via Cloud HSM.

Cymbal Bank will use Google Cloud's default encryption in motion for managed services or when data is transferred across physical boundaries controlled by Google Cloud.

Where there are compliance requirements for auditable end-to-end encryption or encryption using a particular set of ciphers or protocols, you will help Cymbal Bank apply application layer encryption using TLS or similar protocols.

Sensitive Data Protection and granular access control for data security compliance

- Use Sensitive Data Protection to scan, classify, and label data with metadata indicating sensitivity
- Transform sensitive data to allow processing while preventing exposure
- Apply granular access control to data to ensure correct access based on sensitivity



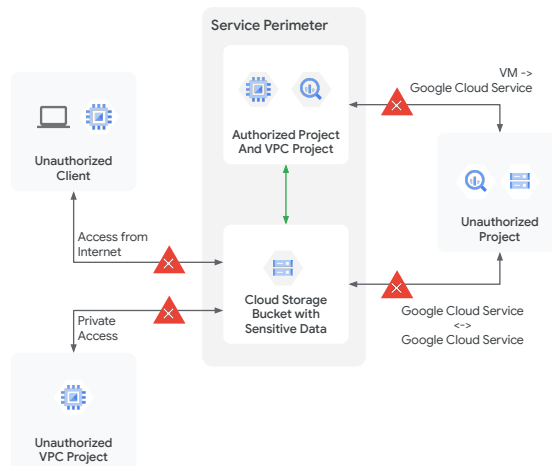
Google Cloud

Cymbal Bank will use Sensitive Data Protection to scan and classify data. You will have metadata applied to indicate sensitive data or data that requires special treatment, and optionally transform that data to allow it to be used without risk of exposure. Using this Sensitive Data Protection process will help Cymbal Bank satisfy compliance requirements related to dealing appropriately with sensitive data.

The metadata that is applied as part of the Sensitive Data Protection scanning process can then be used to determine whether or not to grant access to data based on the sensitivity indicated by the metadata. You can apply granular access control to data to ensure correct access based on sensitivity.

VPC service controls for data residency and location-based access requirements

- Coupled with isolated VPC networks, services and data can be locked down to be accessible only from fixed hardened endpoints
- VPCs can be configured with subnets in only certain regions which when combined with VPC service controls can constrain access to data from only those locations



Google Cloud

Cymbal Bank has compliance requirements related to data residency and from where and how data can be accessed. As a Professional Cloud Security Engineer, you help Cymbal Bank leverage VPC service controls to enforce data residency and location-based access requirements by limiting access to the data from specific VPCs that are located in approved locations.

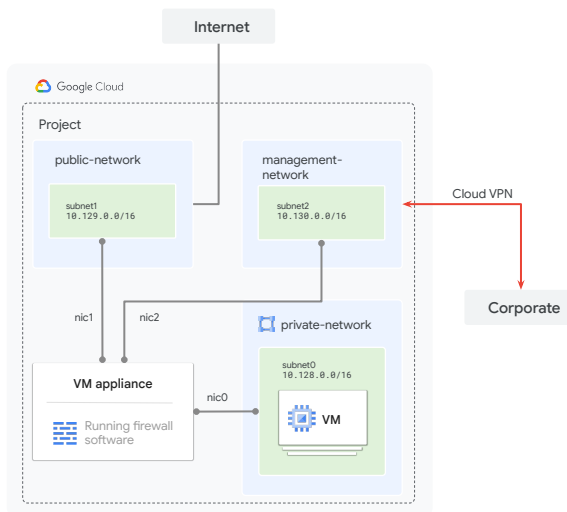
Cymbal Bank can limit access to only VMs in those VPCs that are hardened and have necessary software installed to ensure correct and secure processing of the data.

VPCs can be configured with subnets in only certain regions, which when combined with VPC service controls can constrain access to data from only those locations.

Network isolation to support regulatory compliance

Separate isolated VPCs can:

- Guarantee better workload isolation.
- Help satisfy compliance requirements that depend on workload isolation.
- Facilitate meeting location-based requirements when combined with VPC service controls.



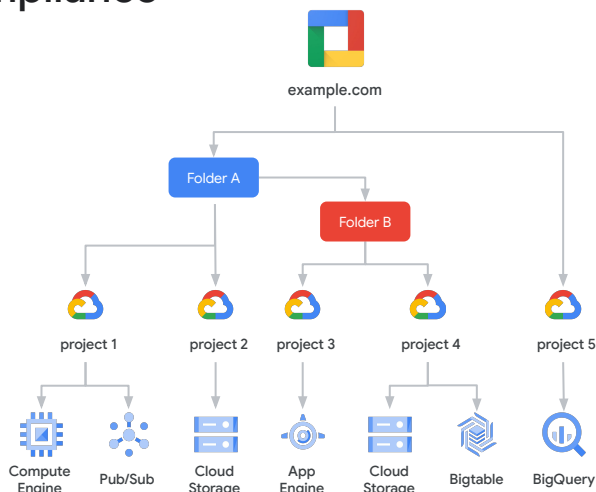
Google Cloud

Cymbal Bank has compliance requirements that require you to classify networks by trust level. The highest trust networks have no direct connectivity to the internet and satisfy strict requirements about when and how they can be used, what sort of traffic can flow into them, and how that traffic is scanned.

Cymbal Bank will use many isolated VPCs for different workloads to help satisfy such requirements. Having different VPCs for different workloads can also facilitate location-based access requirements when combined with VPC service controls.

Setting policy to ensure compliance

- Organization policy constraints can be applied to the organization or any folder or project and restrict how Google Cloud can be used.
- Compliance may require auditable least privilege and separation of duties in access control policies

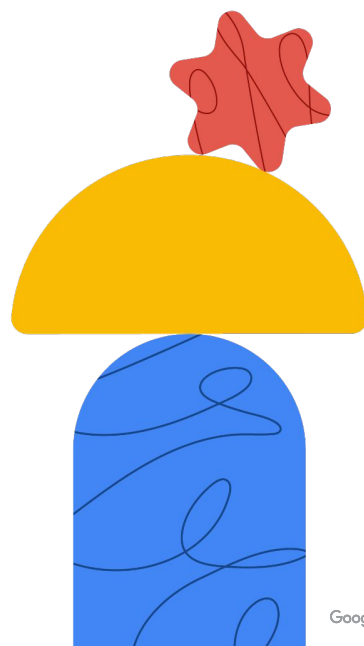


Google Cloud

Cymbal Bank has compliance requirements which mandate policies that define, lock-down, and restrict what can be done in cloud environments to prevent unauthorized activity. Organization policy constraints can be applied to the organization, or any folder or project, and restrict how Google Cloud can be used. This lets you specify which Google Cloud services can be used in which projects, and the parameters of that usage.

The principles of least privilege and separation of duties are commonly expressed in the requirements of security standards. Compliance may require auditable least privilege and separation of duties in access control policies. Google Cloud IAM policies, which allow roles to be bound to identities at any level of the hierarchy, with optional IAM conditions to provide fine-grained conditional access, let Cymbal Bank satisfy such requirements.

Diagnostic questions

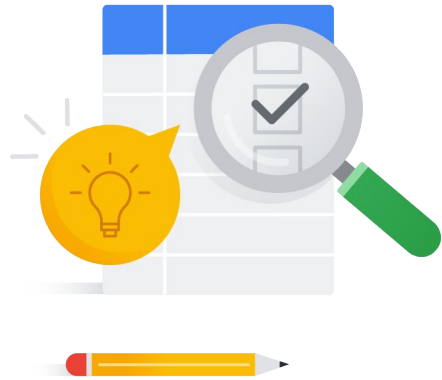


Google Cloud

Now it's your turn to assess your experience and skills related to this section with some diagnostic questions. Remember, the purpose of these questions is to help you better understand what is involved in this section of the exam guide and identify which areas you'll want to focus on in your study plan.

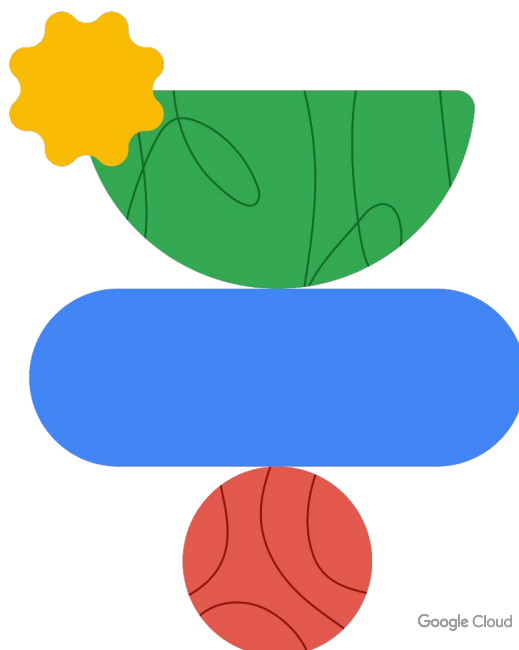
Please complete the diagnostic questions now

- The diagnostic questions are available in the workbook.



Please take 15 minutes to complete the diagnostic questions for this section.

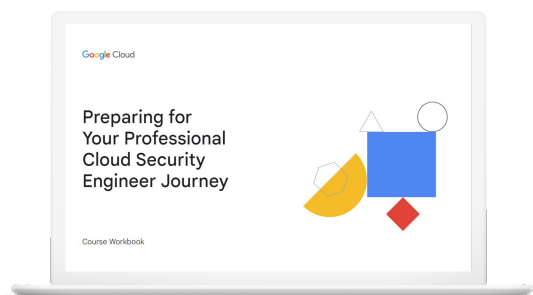
Review and study planning



Now let's review how to use these diagnostic questions to help you identify what to include in your study plan.

Your study plan:

Supporting Compliance Requirements



5.1

Adhering to regulatory and industry standards requirements for the cloud

We'll approach this review by looking at the key areas of this exam section and the questions you just answered about each one. We'll talk about where you can find out more about each area in the learning path for this certification and/or where to find the information in Google Cloud documentation. As we go through each one, take notes on the specific courses (and modules!), skill badges, and documentation pages you'll want to emphasize in your study plan.

5.1 | Adhering to regulatory and industry standards requirements for the cloud

Considerations include:

- Determining technical needs relative to compute, data, network, and storage
- Evaluating the shared responsibility model
- Configuring security controls within cloud environments to support compliance requirements (e.g., Assured Workloads, organizational policies, Access Transparency, Access Approval, regionalization of data and services)
- Determining the Google Cloud environment in scope for regulatory compliance
- Mapping compliance requirements to Google Cloud services and/ security controls (e.g., network and access segmentation, audit log coverage)

Google Cloud

As Professional Cloud Security Engineer, you are expected to help your organization follow regulatory requirements for its cloud environment.

Question 1 tested your knowledge of using encryption key management considerations to satisfy compliance requirements. Question 2 tested your ability to apply Sensitive Data Protection to satisfy privacy requirements. Question 3 explored using VPC service controls to prevent data exfiltration in accordance with requirements for regulatory compliance. Question 4 tested your knowledge of using IAM policies to fulfil requirements for regulatory compliance. Question 5 asked you to design VPC network usage in line regulatory compliance.

5.1 Diagnostic Question 01 Discussion



Cymbal Bank's lending department stores sensitive information, such as your customers' credit history, address and phone number, in parquet files. You need to upload this personally identifiable information (PII) to Cloud Storage so that it's secure and compliant with ISO 27018.

How should you protect this sensitive information using Cymbal Bank's encryption keys and using the least amount of computational resources?

- A. Generate an AES-256 key as a 32-byte bytestring. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- B. Generate an RSA key as a 32-byte bytestring. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- C. Generate a customer-managed encryption key (CMEK) using RSA or AES256 encryption. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- D. Generate a customer-managed encryption key (CMEK) using Cloud KMS. Decode it as a base-64 string. Upload the blob to the bucket using this key.

Feedback:

A. Correct! You should use a customer-supplied encryption key (CSEK) to protect sensitive information. AES-256 encryption returns a 32-byte bytestring that needs to be decoded.

B. Incorrect. Although CSEK is the correct choice for encryption, RSA is computationally more resource-intensive. RSA is used to encrypt small amounts of data.

C. Incorrect. CMEK will enable key rotation, but data will still be encrypted using Google-generated keys. RSA is not a useful option to encrypt large chunks of data, such as blobs.

D. Incorrect. CMEK will bring key rotation under the customer's control but will still use Google-generated keys. Our requirement is to use Cymbal bank's encryption keys. Therefore, use CSEK to store sensitive information.

Where to look:

- https://cloud.google.com/storage/docs/samples/storage-upload-encrypted-file#storage_upload_encrypted_file-python
- <https://cloud.google.com/kms/docs/cmek>
- <https://cloud.google.com/storage/docs/encryption/customer-supplied-keys>
- <https://cloud.google.com/storage/docs/encryption>
- <https://cloud.google.com/security/compliance/iso-27018>

Content mapping:

- ILT course: **Security in Google Cloud**
 - M6 Securing Cloud Data: Techniques and Best Practices
- On-demand course: **Security Best Practices in Google Cloud**
 - M6 Securing Cloud Data: Techniques and Best Practices

Summary:

A customer-supplied encryption key (CSEK) adds an additional layer of security on top of Google-managed encryption keys. CSEK lets you provide your own encryption key. Google Cloud uses CSEK to generate and protect Google's encryption keys. The newly generated keys are then used to encrypt the customer's data. A CSEK is different from a customer-managed encryption key (CMEK), which allows only the user to manage key rotation.

5.1 Diagnostic Question 02 Discussion



You are designing a web application for Cymbal Bank so that customers who have credit card issues can contact dedicated support agents. Customers may enter their complete credit card number when chatting with or emailing support agents. You want to ensure compliance with PCI-DSS and prevent support agents from viewing this information in the most cost-effective way.

- A. Use customer-supplied encryption keys (CSEK) and Cloud Key Management Service (KMS) to detect and encrypt sensitive information.
- B. Detect sensitive information with Cloud Natural Language API.
- C. Use customer-managed encryption keys (CMEK) and Cloud Key Management Service (KMS) to detect and encrypt sensitive information.
- D. Implement Sensitive Data Protection using its REST API.

What should you do?

Google Cloud

Feedback:

A. Incorrect. CSEK and Cloud KMS are used for ensuring customer control over Google-generated encryption keys.

B. Incorrect. Cloud Natural Language API can help with text segmentation and named-entity recognition, but not with hiding or masking sensitive information.

C. Incorrect. You will still need some service to detect credit card numbers if BigQuery stores them and does not show them.

D. Correct! Sensitive Data Protection helps with identifying sensitive information along with its INFOTYPE. Sensitive Data Protection can then mask sensitive information programmatically.

Where to look:

- <https://cloud.google.com/dlp/docs/sensitive-data-protection-overview>
- <https://cloud.google.com/architecture/automating-classification-of-data-uploaded-to-cloud-storage>
- <https://cloud.google.com/dlp/docs/libraries>
- <https://cloud.google.com/dlp/demo/#/>

Content mapping:

- ILT course: **Security in Google Cloud**
 - M10 Content-related Vulnerabilities

- On-demand course: **Mitigating Security Vulnerabilities in Google Cloud**
 - M2 Content-related Vulnerabilities

Summary:

DLP API helps you programmatically identify the sensitive blocks in information with 150+ infoTypes. These infoTypes recognize and classify private information blocks such as credit card, date of birth, and PAN. After identification, data can be masked with predefined rules.

5.1 Diagnostic Question 03 Discussion



You are a cloud engineer at Cymbal Bank. You need to share the auditing and compliance standards with your CTO that cover controls over financial reporting and both public and private controls over security, availability, and confidentiality.

- A. FIPs 140-2
- B. GDPR
- C. PCI-DSS
- D. SOX

Which compliance standard covers this?

Google Cloud

Feedback:

A. Incorrect. FIPs 140-2 is a security standard that sets requirements for cryptographic modules, including hardware, software, and/or firmware, for U.S. federal agencies.

B. Incorrect. GDPR lays out specific requirements for businesses and organizations who are established in Europe or who serve users in Europe.

C. Incorrect. PCI DSS is a set of network security and business best practices guidelines adopted by the PCI Security Standards Council to establish a “minimum security standard” to protect customers’ payment card information.

D. Correct! SOX covers controls over financial reporting and both public and private controls over security, availability, and confidentiality.

Where to look:

<https://cloud.google.com/security/compliance/>

Content mapping:

No coverage in training materials

Summary:

SOX obligations include establishing and monitoring internal controls, including those maintained by a third party, such as a cloud service provider. Any organization that

processes accounting or financial information on Google Cloud must make its own judgment regarding whether specific Google Cloud services are in scope for meeting its SOX obligations.

5.1 Diagnostic Question 04 Discussion



Cymbal Bank's Insurance Analyst needs to collect and store anonymous protected health information of patients from various hospitals. The information is currently stored in Cloud Storage, where each hospital has a folder that contains its own bucket. You have been tasked with collecting and storing the healthcare data from these buckets into Cymbal Bank's Cloud Storage bucket while maintaining HIPAA compliance.

What should you do?

- A. Create a new folder. Create a new Cloud Storage bucket in this folder. Give the Insurance Analyst the 'Editor' role on the new folder. Collect all hospital data in this bucket. Use the Google Cloud Healthcare Data Protection Toolkit to monitor this bucket.
- B. Create a new Project. Create a new Cloud Storage bucket in this Project with customer-supplied encryption keys (CSEK). Give the Insurance Analyst the 'Reader' role on the Project that contains the Cloud Storage bucket. Use the DLP API to find and mask personally identifiable information (PII) data to comply with HIPAA.
- C. Create a new Project. Use the Google Cloud Healthcare Data Protection Toolkit to set up a collection bucket, monitoring alerts, audit log sinks, and Forseti monitoring resources. Use Dataflow to read the data from source buckets and write to the new collection buckets. Give the Insurance Analyst the 'Editor' role on the collection bucket.
- D. Use the Cloud Healthcare API to read the data from the hospital buckets and use de-identification to redact the sensitive information. Use Dataflow to ingest the Cloud Healthcare API feed and write data in a new Project that contains the Cloud Storage bucket. Give the Insurance Analyst the 'Editor' role on this Project.

Google Cloud

Feedback:

A. Incorrect. If you collect hospital data in a new bucket directly, you will store the sensitive information, which you need to avoid. The Google Cloud Healthcare Data Protection Toolkit needs to run before the data collection begins to set up the HIPAA-compliant infrastructure and monitoring.

B. Incorrect. Customer-supplied encryption keys will use your encryption keys instead of Google's to encrypt the data. Users will still be able to view sensitive information. Using the DLP API after the data is stored defeats the purpose.

C. Incorrect. Although this solution is suitable for HIPAA-compliant architecture and the storage requirements, it does not anonymize hospital data.

D. Correct! The Cloud Healthcare API has a de-identification module to redact patient information and is already HIPAA-compliant. You can then use Dataflow to read the information from source and write into a target bucket with anonymization for further analysis.

Where to look:

- <https://cloud.google.com/blog/topics/healthcare-life-sciences/getting-to-know-the-google-cloud-healthcare-api-part-1>
- https://cloud.google.com/storage/docs/collaboration#top_of_page
- <https://cloud.google.com/files/gcp-hipaa-overview-guide.pdf>
- <https://cloud.google.com/architecture/setting-up-a-hipaa-aligned-project#storage>

- [ge_browser](#)

Content mapping:

No coverage in training materials


Summary:

The Cloud Healthcare API and the Google Cloud Healthcare Data Protection Toolkit can be used to maintain HIPAA compliance for data storage, application development, data analysis, and machine learning. The Google Cloud Healthcare Data Protection Toolkit helps you set up HIPAA-compliant architecture using an infrastructure-as-a-code script (IaaS). The Cloud Healthcare API is a fully managed HIPAA-compliant service that contains a de-identification module, along with security built around location and privacy.

5.1 Diagnostic Question 05 Discussion

Cymbal Bank plans to launch a new public website where customers can pay their equated monthly installments (EMI) using credit cards. You need to build a secure payment processing solution using Google Cloud which should follow the PCI-DSS isolation requirements. How would you architect a secure payment processing environment with Google Cloud services to follow PCI-DSS?

Select the two correct choices

- 
- A. Create a new Google Cloud project with restricted access (separate from production environment) for the payment processing solution. Create a new Compute Engine instance and configure firewall rules, a VPN tunnel, and an internal load balancer.
 - B. Create a new Google Cloud project with restricted access (separate from production environment) for the payment processing solution. Configure firewall rules, a VPN tunnel, and a proxy Network Load Balancer for a new App Engine flexible environment.
 - C. Create a new Google Cloud project with restricted access (separate from production environment) for the payment processing solution. Configure firewall rules, a VPN tunnel, and an Application Load Balancer for a new Compute Engine instance.
 - D. Deploy an Ubuntu Compute Engine instance. Install the libraries needed for payment solutions and encryption/decryption. Deploy using Terraform.
 - E. Deploy a Linux base image from preconfigured operating system images. Install only the libraries you need. Deploy using Terraform.

Google Cloud

Feedback:

A. Incorrect. An internal load balancer will not communicate with the public internet, which will render this system unusable.

B. Incorrect. Firewall rules and load balancer settings do not apply to the App Engine flexible environment.

C. Correct! You need an isolated Linux base (Compute Engine) environment that is separate from your production environment as per PCI-DSS isolation requirements for payment solutions.

D. Incorrect. If you choose an Ubuntu base image, it will contain many libraries your payment interface does not need. That violates PCI-DSS and exposes Compute Engine to vulnerability.

E. Correct! Having a minimalist operating system with only the libraries required for your application limits the attack surface. Use Terraform to ensure that only the current deployment happens, without interruption.

Where to look:

https://cloud.google.com/architecture/pci-dss-compliance-in-gcp#cloud_storage

Content mapping:

- ILT course: **Security in Google Cloud**

- M1 Foundations of Google Cloud Security
- On-demand course: **Managing Security in Google Cloud**
 - M1 Foundations of Google Cloud Security

Summary:

Payment processing requires your system to be compliant with PCI-DSS. As a part of this compliance, you need to ensure that the payment collection environment is separate from your production environment. You need to follow the PCI-DSS guidelines and best practices. Security is a shared responsibility: Google Cloud provides tools and configuration options to implement compliance procedures, and you need to apply the configurations and procedures.

5.1 Determining regulatory requirements for the cloud

Documentation

[Upload an object by using CSEK | Cloud Storage](#)
[Customer-managed encryption keys \(CMEK\) | Cloud KMS Documentation](#)

[Customer-supplied encryption keys | Cloud Storage](#)

[Data encryption options | Cloud Storage](#)

[ISO/IEC 27018 Certified Compliant | Google Cloud](#)

[Automating the Classification of Data Uploaded to Cloud Storage | Cloud Architecture Center | Google Cloud](#)

[Sensitive Data Protection overview](#)

[Sensitive Data Protection client libraries | Data Loss Prevention Documentation](#)

[Data Loss Prevention Demo](#)

[Overview of VPC Service Controls | Google Cloud](#)

[Getting to know the Google Cloud Healthcare API: Part 1](#)

[Sharing and collaboration | Cloud Storage](#)

[Google Cloud Platform HIPAA overview guide](#)

[Setting up a HIPAA-aligned project | Cloud Architecture Center](#)

[PCI Data Security Standard compliance | Cloud Architecture Center](#)

Let's consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these links.

- https://cloud.google.com/storage/docs/samples/storage-upload-encrypted-file#storage_upload_encrypted_file-python
- <https://cloud.google.com/kms/docs/cmek>
- <https://cloud.google.com/storage/docs/encryption/customer-supplied-keys>
- <https://cloud.google.com/storage/docs/encryption>
- <https://cloud.google.com/security/compliance/iso-27018>
- <https://cloud.google.com/architecture/automating-classification-of-data-uploaded-to-cloud-storage>
- <https://cloud.google.com/dlp/docs/sensitive-data-protection-overview>
- <https://cloud.google.com/dlp/docs/libraries>
- <https://cloud.google.com/dlp/demo/#/>
- <https://cloud.google.com/vpc-service-controls/docs/overview>
- <https://cloud.google.com/blog/topics/healthcare-life-sciences/getting-to-know-the-google-cloud-healthcare-api-part-1>
- https://cloud.google.com/storage/docs/collaboration#top_of_page
- <https://cloud.google.com/files/gcp-hipaa-overview-guide.pdf>

- https://cloud.google.com/architecture/setting-up-a-hipaa-aligned-project#storage_browser
- https://cloud.google.com/architecture/pci-dss-compliance-in-gcp#cloud_storage