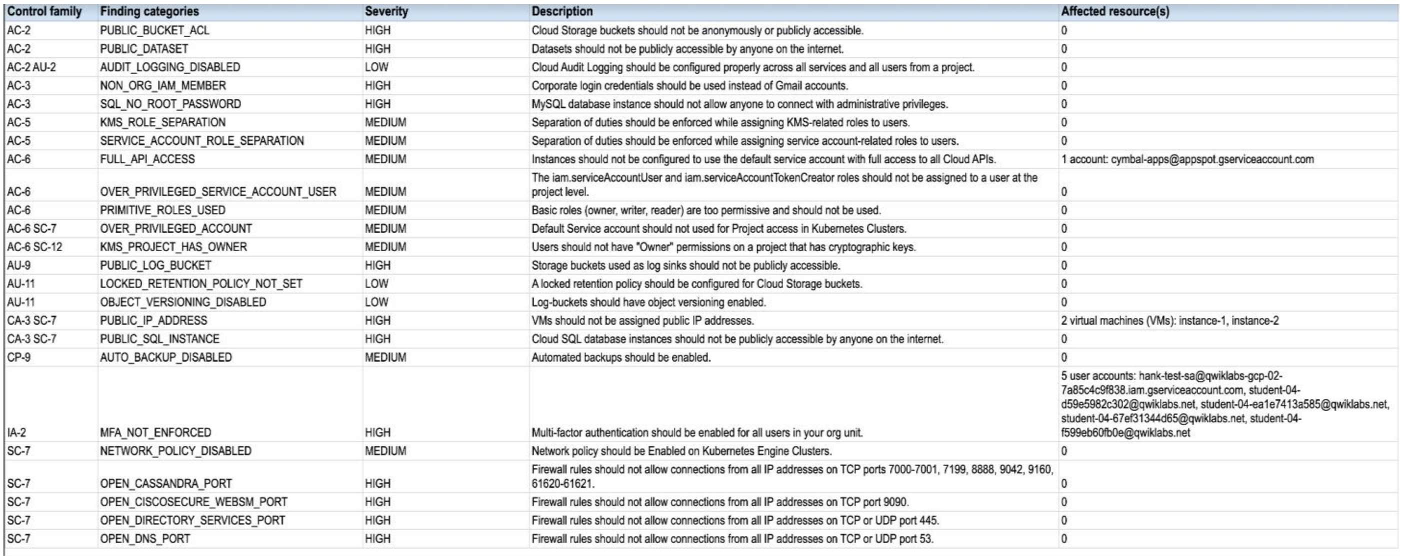
Compliance Report Log (for assessment)



Control family	Finding categories	Severity	Description	Affected resource(s)
AC-2	PUBLIC_BUCKET_ACL	HIGH	Cloud Storage buckets should not be anonymously or publicly accessible.	0
AC-2	PUBLIC_DATASET	HIGH	Datasets should not be publicly accessible by anyone on the internet.	0
AC-2 AU-2	AUDIT_LOGGING_DISABLED	LOW	Cloud Audit Logging should be configured properly across all services and all users from a project.	0
AC-3	NON_ORG_IAM_MEMBER	HIGH	Corporate login credentials should be used instead of Gmail accounts.	0
AC-3	SQL_NO_ROOT_PASSWORD	HIGH	MySQL database instance should not allow anyone to connect with administrative privileges.	0
AC-5	KMS_ROLE_SEPARATION	MEDIUM	Separation of duties should be enforced while assigning KMS-related roles to users.	0
AC-5	SERVICE_ACCOUNT_ROLE_SEPARATION	MEDIUM	Separation of duties should be enforced while assigning service account-related roles to users.	0
AC-6	FULL_API_ACCESS	MEDIUM	Instances should not be configured to use the default service account with full access to all Cloud APIs.	1 account: cymbal-apps@appspot.gserviceaccount.com
AC-6	OVER_PRIVILEGED_SERVICE_ACCOUNT_USER	MEDIUM	The iam.serviceAccountUser and iam.serviceAccountTokenCreator roles should not be assigned to a user at the project level.	0
AC-6	PRIMITIVE_ROLES_USED	MEDIUM	Basic roles (owner, writer, reader) are too permissive and should not be used.	0
AC-6 SC-7	OVER_PRIVILEGED_ACCOUNT	MEDIUM	Default Service account should not used for Project access in Kubernetes Clusters.	0
AC-6 SC-12	KMS_PROJECT_HAS_OWNER	MEDIUM	Users should not have "Owner" permissions on a project that has cryptographic keys.	0
AU-9	PUBLIC_LOG_BUCKET	HIGH	Storage buckets used as log sinks should not be publicly accessible.	0
AU-11	LOCKED_RETENTION_POLICY_NOT_SET	LOW	A locked retention policy should be configured for Cloud Storage buckets.	0
AU-11	OBJECT_VERSIONING_DISABLED	LOW	Log-buckets should have object versioning enabled.	0
CA-3 SC-7	PUBLIC_IP_ADDRESS	HIGH	VMs should not be assigned public IP addresses.	2 virtual machines (VMs): instance-1, instance-2
CA-3 SC-7	PUBLIC_SQL_INSTANCE	HIGH	Cloud SQL database instances should not be publicly accessible by anyone on the internet.	0
CP-9	AUTO_BACKUP_DISABLED	MEDIUM	Automated backups should be enabled.	0
IA-2	MFA_NOT_ENFORCED	HIGH	Multi-factor authentication should be enabled for all users in your org unit.	5 user accounts: hank-test-sa@qwiklabs-gcp-02-7a85c4c9f838.iam.gserviceaccount.com, student-04-d59e5982c302@qwiklabs.net, student-04-ea1e7413a585@qwiklabs.net, student-04-67ef31344d65@qwiklabs.net, student-04-f599eb60fb0e@qwiklabs.net
SC-7	NETWORK_POLICY_DISABLED	MEDIUM	Network policy should be Enabled on Kubernetes Engine Clusters.	0
SC-7	OPEN_CASSANDRA_PORT	HIGH	Firewall rules should not allow connections from all IP addresses on TCP ports 7000-7001, 7199, 8888, 9042, 9160, 61620-61621.	0
SC-7	OPEN_CISCOSECURE_WEBSM_PORT	HIGH	Firewall rules should not allow connections from all IP addresses on TCP port 9090.	0
SC-7	OPEN_DIRECTORY_SERVICES_PORT	HIGH	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 445.	0
SC-7	OPEN_DNS_PORT	HIGH	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 53.	0

Compliance Report Notes (Bri’s Answers)

Security control	**Severity**	**Findings**	**Recommendations**
List the missing security control(s).	*List the severity (high, medium, or low).*	*Provide a description of the missing security control.*	*Provide a recommendation for implementing the security control.*
Assessment, Authorization, and Monitoring (Information Exchange) (CA-3) | System & Communication Protection (Boundary Protection) (SC-7)	High	VMs should not be assigned public IP addresses.	VMs should be assigned to private IP addresses in order to prevent public data exchange and sharing with a public network. In addition, for public exchange there should be a managed interface implemented, such as a firewall.
Identification & Authentication (Organizational Users) (IA-2)	High	Multi-factor authentication should be enabled for all users in your org unit.	Configure multi-factor authentication within the Identity and Access Management tool for users to ensure only authorized users have access.
Access Control (Least privilege) (AC-6)	Medium	Instances should not be configured to use the default service account with full access to all Cloud APIs.	People and systems should only be granted access to what they need. Configure access controls to ensure least privilege.

My Self-Assessment:

After reviewing the answers in the Google Exemplar on the following pages. My review and assessment of the security compliance report was correct. However, in the Findings section, I should have listed the exact findings rather than the description of the issue conveyed in the security compliance report. Listing the specific issues such as the instance-1 and instance-2, or the accounts without MFA implemented will provide the security team more in-depth information about what to fix, rather than a general description.

Compliance report notes (Google's Exemplar)

Security control	**Severity**	**Findings**	**Recommendations**
● Assessment, Authorization, and Monitoring (CA-3) ● System and Communications Protection (SC-7)	High	2 VMs are assigned public IP addresses: ● instance-1 ● instance-2	Review the VM configuration. Secure the VM by changing the IP addresses to private IPs.
Identification and Authentication (IA-2)	High	5 user accounts do not have multi-factor authentication (MFA) enabled: ● hank-test-sa@qwiklabs-gcp-02-7a85c4c9f838.iam.gserviceaccount.com ● student-04-d59e5982c302@qwiklabs.net ● student-04-ea1e7413a585@qwiklabs.net ● student-04-67ef31344d65@qwiklabs.net ● student-04-f599eb60fb0e@qwiklabs.net	Implement an organization-wide MFA policy.
Access Control (AC-6)	Medium	1 account is configured to use the default service account with full access to all Cloud APIs: ● cymbal-apps@appspot.gserviceaccount.com	Review the account and implement the principle of least privilege to ensure that the account only has access to the APIs it needs to perform its duties.

GOOGLE COMPLIANCE REPORT ACTIVITY INSTRUCTIONS

Scenario:

Review the following scenario. Then, access the supporting materials before moving on to the next course item.

After joining the security team at Cymbal Bank, you've witnessed the rapid digital transformation that the company is currently undergoing. They have combined their on-premises infrastructure with cloud services to move to a hybrid cloud model. Despite the added benefits that the move to the cloud has provided, it has also introduced complexity, especially concerning the configuration of assets. In addition, Cymbal Bank must also ensure compliance for several compliance and regulatory frameworks. As part of the move to hybrid cloud, the security team is working on a plan for Cymbal Bank to meet compliance requirements and protect Cymbal Bank's critical assets.

Due to the massive scope of this project, the security team has split up into several groups. Each group is tasked with addressing a compliance framework and its respective requirements. You have joined the team that is working on implementing security recommendations using a National Institute of Standards and Technology (NIST) framework. This unified framework, NIST SP 800-53, provides a catalog of security controls for protecting 1 information system. The U.S. federal government is required to use this framework; however, any organization can use it to strengthen the security of their information systems.

Your group's goal is to identify any ineffective cloud security controls that are contributing to compliance gaps. Your supervisor has requested your help with this specific task. To deliver on this request, you must review the details of a compliance report for the cloud resources in a cloud project. Begin by identifying any compliance gaps and then provide recommendations for remediating them. Step-By-Step Instructions

Consult the supporting materials to answer the quiz questions in the asset that follows. After you complete the quiz, you can compare your answers to the feedback provided.

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the questions.

Step 2: Review the security controls

Review the Security controls table. NIST SP 800-53 has over a thousand security and privacy controls. Reviewing all of these controls is beyond the scope of this activity, but you should know that these security controls are categorized into 20 control families. Each control family contains security controls that are related to the specific topic of the family. For example, the control family Identification and Authentication (IA) deals with security controls involving identity and access management. Each security control within the family is identified with a control number (for example, IA-1). Pro tip: If you'd like to learn more about the NIST SP 800-

53, including the complete catalog of security and privacy controls, review the official publication linked in the supporting materials.

Step 3: Analyze the compliance report

Analyze the details of the NIST SP 800-53 compliance report. Examine each of the columns, which contain the following information:

- Control family: This column contains the NIST SP 800-53 control family related to the finding. Notice that not all 20 of the control families are listed
- Finding categories: An abbreviation of the description of the security control.
- Severity: The risk level of the finding category: low, medium, or high
- Description: A description of the compliance issue
- Affected resource(s): The name and number of resources that are affected with each compliance standard. A count of 0 indicates that no ineffective security controls were found

Step 4: Identify the ineffective security controls

After you've reviewed the Compliance report, identify the four ineffective security controls.

- Begin by referring to the Affected resource(s) column. Determine which security controls are ineffective by identifying security controls with a findings count of 1 or more. The number indicates how many times the security control was detected as ineffective. Findings with a count of 0 indicate that no ineffective security controls were found.
- Refer to the Description column to identify what the compliance issue is.
- In the Compliance report notes template, fill out the Security control, Severity, and Findings columns. Your goal is to identify the details of each compliance issue and its associated security control.

Step 5: Provide recommendations to implement the security controls

Next record your recommendations for implementing the security controls. Ensure that you order the recommendations according to their severity.

In the Compliance report notes template, write 2–3 sentences in the Recommendations section describing your recommendations for fixing each security control and why.