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