Compliance report notes

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 making sure only private IP exists.

• 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.