Compliance report notes

joining the security team at Cymbal Bank, I'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. I 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.

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	Implement an organization-wide MFA policy.

		@qwiklabs.net • student-04-ea1e7413a585@qwiklabs.net • student-04-67ef31344d65@qwiklabs.net • student-04-f599eb60fb0e@qwiklabs.net	
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.