2.3 Compliance Report Review Notes

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Control (NIST SP 800-53)** | **Severity** | **Findings** | **Recommendations** |
| Assessment, Authorization and Monitoring (CA-3),  System and Communications Protection (SC-7) | High | 2 virtual machines have public IP addresses:   1. instance-1 2. instance-2 | Secure the virtual machines by changing the public IP addresses to private IP addresses |
| Identification and Authentication (IA-2) | High | 5 user accounts do not have MFA enabled:   1. hank-test-sa @qwiklabs-gc p-02-7a85c4 c9f838.iam.gs erviceaccount .com 2. student-04-d 59e5982c302 @qwiklabs.ne t 3. student-04-e a1e7413a585 @qwiklabs.ne t 4. student-04-6 7ef31344d65 @qwiklabs.ne t 5. student-04-f 599eb60fb0e @qwiklabs.ne t | Implement MFA policy across entire organisation |
| Access Control (AC-6) | Medium | 1 account is configured as the default service account and has full access to all Cloud APIs:   1. cymbal-apps@appspot.gserviceaccount.com | Implement principle of least privilege to ensure account only has access to services it needs |