OS / Firewall / Cloud Configuration Review & CIS Benchmark Security Assessment Report.

PREPARED FOR

ABC Corporation.

PROJECT NAME: OS / FIREWALL / CLOUD CONFIGURATION REVIEW & CIS BENCHMARK SECURITY ASSESSMENT REPORT.

ASSESSMENT PERIOD	
Start Date	DD/MM/YYYY
End Date	DD/MM/YYYY

1 CONTENTS

1.1 Document Control

VERSION	DATE	AUTHOR	DESCRIPTION
1.0		Pentester / Company Name	Initial Report
1.1		Pentester / Company Name	Re-assessment
1.2		Pentester / Company Name	Finalized

2 EXECUTIVE SUMMARY

The security assessment conducted between the agreed-upon dates was based around the scope of work detailed in the Scope of Engagement section listed below. Multiple tests were conducted against the targeted systems, involving both automated scanning and manual testing, to identify a range of potential vulnerabilities and misconfiguration of the systems.

The security team performed a Configuration Review & CIS Benchmark Security Assessment for **ABC Corporation.** The assessment was performed from both authenticated and unauthenticated perspectives with the provided credentials.

This includes reviewing the **AWS Ec2 Server/ Firewall and Cloud (Azure / AWS) CIS Benchmark** currently version **1.5.0**. Although they vary in impact many of the findings in this section relate to overall account hygiene and hardening. Implementing the remediation advice given would make the account easier to manage, maintain, and audit, reducing the likelihood of security vulnerabilities being introduced in error and making the account much more resilient to attack.

Assessment Finding

This Report is a CIS configuration report, In the Report Summary, the CIS Benchmark Score as per the Used Version, and the Control wise Test case is mapped with the Result

3 PROJECT OVERVIEW

3.1 Scope of Engagement

The following Azure and AWS service account were defined within the scope for this assessment:

CLOUD ID	SERVICE PROVIDER
Tenant ID: 11111111-1111-1111-1111-1111	AZURE
AWS ID: ABCEFGHIJKLMN	AWS

The following systems were defined within scope of the Network infrastructure, Operating system and Build assessment:

OPERATING SYSTEM & BUILD REVIEW	NETWORK / INFRASTRUCTURE IP ADDRESS
Amazon Linux release 2 (Karoo)	1.1.1.1

3.2 Assessment Objectives

Performed security assessment to achieve the following key objectives based upon the agreed upon Scope of Work listed above:

- Perform a security assessment against the targets specified in the Scope of Engagement.
- Prioritise vulnerabilities based upon ease of exploitation, level of effort to remedy, and severity.
- Provide recommendations to improve security practice in line with industry best practice.
- Deliver a manageable and accurate report.

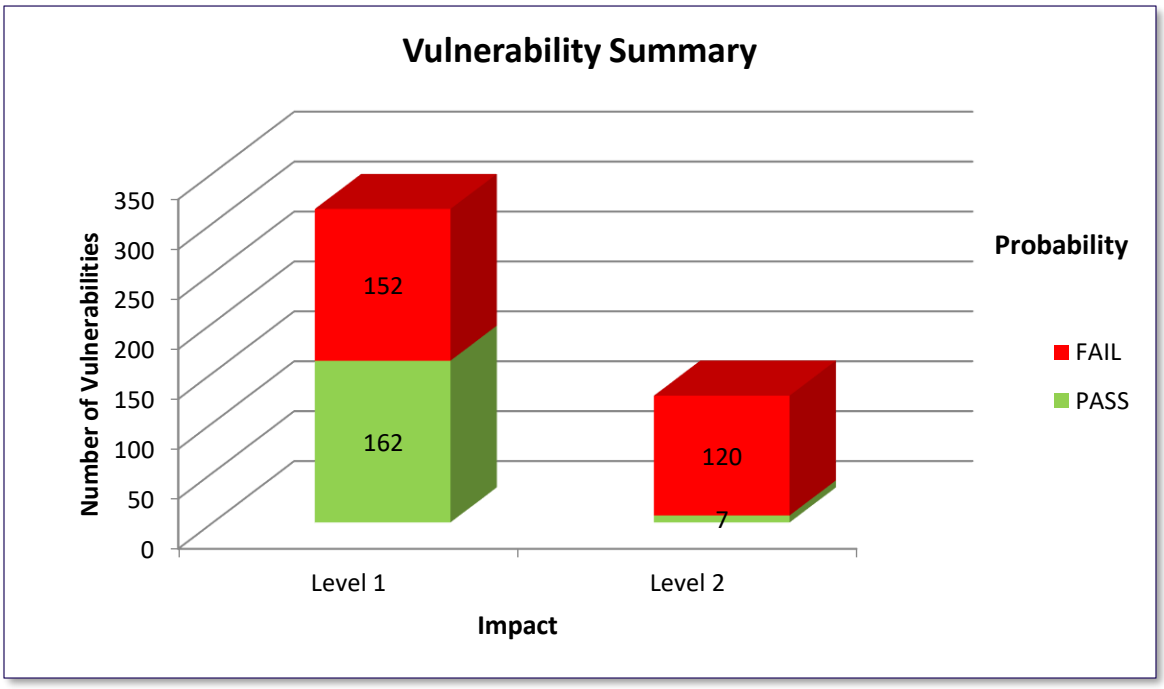
3.3 Contact Information

Contact Details	Customer Contact Details
SecureGuard Inc 123 W Madison, Suite #1700 Chicago,IL 60602 (888) 837 7776 **Tel:** **Email:** Info@SecureGuardAudits.com	**ABC Corporation** 1 Rhode Island Ave NE, Washington, DC 20018 (202) 555 1212 **Tel:** **Email:** Info@ABCCorporation.com

4 SUMMARY OF VULNERABILITIES

4.1 Graphical Summary

Key findings have been ranked and positioned in the following table according to the relative risk or probability of exploit. Vulnerabilities are split into Test Case of Level 1 and Level 2: **PASS**, **FAIL**. Risk is calculated by comparing the impact vs. the probability of exploit which is represented using colour coding. This was during the initial assessment.



After the retest of the application, there were no open vulnerabilities.

5 CONFIGURATION REVIEW & CIS BANCHMARK

5.1 AWS EC2 Server –CIS Security Benchmarks

***CVSS Score:** N/A* ***CVSS Vector:** N/A* ***Impact/Probability:** Info/Info*

***Affected:** 1.1.1.1*

The Linux hosts were assessed against the Center for Internet Security (CIS) Linx benchmarks as described in the Technical Analysis. The Level 1 and 2 benchmarks were used for this assessment which are profiles intended to:

- be practical and prudent; provide a clear security benefit; and not inhibit the utility of the technology beyond acceptable means.

Compliance checks that result in a fail are due to an appropriate registry or group policy settings being set outside of the range of defined values. Compliance checks that result in a warning are generally due to an appropriate registry or group policy setting being missing, for example, Microsoft release a security package called LAPS, if this is not installed then the LAPS checks will result in a warning during the assessment.

5.1.1 Remediation

Consider configuring the expected value in respect to the environment to further harden the build, after thorough testing. Refer to the following resource for further information: https://www.cisecurity.org/cis-benchmarks/

5.1.2 Technical Analysis

The configuration settings can be found in the following appendix:

EXTERNAL DOCUMENT NAME	COMPLIANCE STANDARDS
CIS Security Benchmarks - **3.227.47.131**	CIS Amazon Linux 2 v2.0.0 Server L1 CIS Amazon Linux 2 v2.0.0 Server L2

5.1.3 CIS Benchmark Scores

HOST	LEVEL 1			LEVEL 2		
	PASS	FAIL	TOTAL	PASS	FAIL	TOTAL
CIS Security Benchmarks - **3.227.47.131**	162	152	314	7	120	127

5.1.3.1.1 LEVEL 1

5.1.3.1.1.1 Initial Setup

NO	CHECK NAME	RESULT
1	1.1.1.1 Ensure mounting of cramfs filesystems is disabled - lsmod	PASSED
2	1.1.1.1 Ensure mounting of cramfs filesystems is disabled - modprobe	FAILED
3	1.1.1.2 Ensure mounting of squashfs filesystems is disabled - lsmod	PASSED
4	1.1.1.2 Ensure mounting of squashfs filesystems is disabled - modprobe	FAILED
5	1.1.1.3 Ensure mounting of udf filesystems is disabled - lsmod	PASSED
6	1.1.1.3 Ensure mounting of udf filesystems is disabled - modprobe	FAILED
7	1.1.10 Ensure separate partition exists for /var	FAILED
8	1.1.11 Ensure separate partition exists for /var/tmp	FAILED
9	1.1.12 Ensure /var/tmp partition includes the noexec option	FAILED
10	1.1.13 Ensure /var/tmp partition includes the nodev option	FAILED
11	1.1.14 Ensure /var/tmp partition includes the nosuid option	FAILED
12	1.1.15 Ensure separate partition exists for /var/log	FAILED
13	1.1.16 Ensure separate partition exists for /var/log/audit	FAILED
14	1.1.17 Ensure separate partition exists for /home	FAILED
15	1.1.18 Ensure /home partition includes the nodev option	FAILED
16	1.1.19 Ensure removable media partitions include noexec option	PASSED
17	1.1.2 Ensure /tmp is configured	FAILED
18	1.1.20 Ensure nodev option set on removable media partitions	PASSED
19	1.1.21 Ensure nosuid option set on removable media partitions	PASSED

20	1.1.22 Ensure sticky bit is set on all world-writable directories	FAILED
21	1.1.23 Disable Automounting	PASSED
22	1.1.24 Disable USB Storage - lsmod	PASSED
23	1.1.24 Disable USB Storage - modprobe	FAILED
24	1.1.3 Ensure noexec option set on /tmp partition	FAILED
25	1.1.4 Ensure nodev option set on /tmp partition	FAILED
26	1.1.5 Ensure nosuid option set on /tmp partition	FAILED
27	1.1.6 Ensure /dev/shm is configured - fstab	FAILED
28	1.1.6 Ensure /dev/shm is configured - mount	PASSED
29	1.1.7 Ensure noexec option set on /dev/shm partition	FAILED
30	1.1.8 Ensure nodev option set on /dev/shm partition	PASSED
31	1.1.9 Ensure nosuid option set on /dev/shm partition	PASSED
32	1.2.1 Ensure GPG keys are configured	FAILED
33	1.2.2 Ensure package manager repositories are configured	FAILED
34	1.2.3 Ensure gpgcheck is globally activated	PASSED
35	1.3.1 Ensure AIDE is installed	FAILED
36	1.3.2 Ensure filesystem integrity is regularly checked	FAILED
37	1.4.1 Ensure permissions on bootloader config are configured - grub.cfg	FAILED
38	1.4.1 Ensure permissions on bootloader config are configured - user.cfg	PASSED
39	1.4.2 Ensure authentication required for single user mode - emergency.service	PASSED
40	1.4.2 Ensure authentication required for single user mode - rescue.service	PASSED
41	1.5.1 Ensure core dumps are restricted - /etc/sysctl.conf, /etc/sysctl.d/*	FAILED

42	1.5.1 Ensure core dumps are restricted - coredump.service	PASSED
43	1.5.1 Ensure core dumps are restricted - limits.conf, limits.d/*	FAILED
44	1.5.1 Ensure core dumps are restricted - sysctl	PASSED
45	1.5.2 Ensure XD/NX support is enabled	PASSED
46	1.5.3 Ensure address space layout randomization (ASLR) is enabled	PASSED
47	1.5.4 Ensure prelink is not installed	PASSED
48	1.6.1.1 Ensure SELinux is installed	PASSED
49	1.6.1.2 Ensure SELinux is not disabled in bootloader configuration - enforcing	FAILED
50	1.6.1.2 Ensure SELinux is not disabled in bootloader configuration - selinux	FAILED
51	1.6.1.3 Ensure SELinux policy is configured - config	PASSED
52	1.6.1.3 Ensure SELinux policy is configured - sestatus	FAILED
53	1.6.1.4 Ensure the SELinux mode is enforcing or permissive - config	FAILED
54	1.6.1.4 Ensure the SELinux mode is enforcing or permissive - getenforce	FAILED
55	1.6.1.5 Ensure the SELinux mode is enforcing	FAILED
56	1.6.1.6 Ensure no unconfined services exist	PASSED
57	1.6.1.7 Ensure SETroubleshoot is not installed	PASSED
58	1.6.1.8 Ensure the MCS Translation Service (mcstrans) is not installed	PASSED
59	1.7.1 Ensure message of the day is configured properly - /etc/os-release	PASSED
60	1.7.1 Ensure message of the day is configured properly - banner_check	FAILED
61	1.7.1 Ensure message of the day is configured properly - msrv	PASSED
62	1.7.2 Ensure local login warning banner is configured properly - /etc/os-release	PASSED
63	1.7.2 Ensure local login warning banner is configured properly - banner_check	FAILED

64	1.7.2 Ensure local login warning banner is configured properly - msrv	FAILED
65	1.7.3 Ensure remote login warning banner is configured properly - banner_check	FAILED
66	1.7.3 Ensure remote login warning banner is configured properly - msrv	FAILED
67	1.7.4 Ensure permissions on /etc/motd are configured	PASSED
68	1.7.5 Ensure permissions on /etc/issue are configured	PASSED
69	1.7.6 Ensure permissions on /etc/issue.net are configured	PASSED
70	1.8 Ensure updates, patches, and additional security software are installed	FAILED

5.1.3.1.1.2 Services

NO	CHECK NAME	RESULT
1	2.1.1.1 Ensure time synchronization is in use	PASSED
2	2.1.1.2 Ensure chrony is configured - OPTIONS	FAILED
3	2.1.1.2 Ensure chrony is configured - remote server	FAILED
4	2.1.1.3 Ensure ntp is configured - daemon	PASSED
5	2.1.1.3 Ensure ntp is configured - remote server	PASSED
6	2.1.1.3 Ensure ntp is configured - restrict -4	PASSED
7	2.1.1.3 Ensure ntp is configured - restrict -6	PASSED
8	2.1.10 Ensure IMAP and POP3 server is not installed	PASSED
9	2.1.11 Ensure Samba is not installed	PASSED
10	2.1.12 Ensure HTTP Proxy Server is not installed	PASSED
11	2.1.13 Ensure net-snmp is not installed	PASSED
12	2.1.14 Ensure NIS server is not installed	PASSED
13	2.1.15 Ensure telnet-server is not installed	PASSED
14	2.1.16 Ensure mail transfer agent is configured for local-only mode	PASSED
15	2.1.17 Ensure nfs-utils is not installed or the nfs-server service is masked	FAILED
16	2.1.18 Ensure rpcbind is not installed or the rpcbind services are masked - rpcbind	FAILED
17	2.1.18 Ensure rpcbind is not installed or the rpcbind services are masked - rpcbind.socket	FAILED
18	2.1.19 Ensure rsync is not installed or the rsyncd service is masked	PASSED
19	2.1.2 Ensure X11 Server components are not installed	PASSED
20	2.1.3 Ensure Avahi Server is not installed - avahi	PASSED

21	2.1.3 Ensure Avahi Server is not installed - avahi-autoipd	PASSED
22	2.1.4 Ensure CUPS is not installed	PASSED
23	2.1.5 Ensure DHCP Server is not installed	PASSED
24	2.1.6 Ensure LDAP server is not installed	PASSED
25	2.1.7 Ensure DNS Server is not installed	PASSED
26	2.1.8 Ensure FTP Server is not installed	PASSED
27	2.1.9 Ensure HTTP server is not installed	PASSED
28	2.2.1 Ensure NIS Client is not installed	PASSED
29	2.2.2 Ensure rsh client is not installed	PASSED
30	2.2.3 Ensure talk client is not installed	PASSED
31	2.2.4 Ensure telnet client is not installed	PASSED
32	2.2.5 Ensure LDAP client is not installed	PASSED
33	2.3 Ensure nonessential services are removed or masked	FAILED

5.1.3.1.1.3 Network Configuration

NO	CHECK NAME	RESULT
1	3.1.2 Ensure wireless interfaces are disabled	PASSED
2	3.2.1 Ensure IP forwarding is disabled - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.ip_forward = 0	PASSED
3	3.2.1 Ensure IP forwarding is disabled - /etc/sysctl.conf /etc/sysctl.d/* net.ipv6.conf.all.forwarding = 0	PASSED
4	3.2.1 Ensure IP forwarding is disabled - sysctl net.ipv4.ip_forward = 0	PASSED
5	3.2.1 Ensure IP forwarding is disabled - sysctl net.ipv6.conf.all.forwarding = 0	PASSED
6	3.2.2 Ensure packet redirect sending is disabled - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.all.send_redirects=0	FAILED
7	3.2.2 Ensure packet redirect sending is disabled - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.default.send_redirects=0	FAILED
8	3.2.2 Ensure packet redirect sending is disabled - sysctl net.ipv4.conf.all.send_redirects=0	FAILED
9	3.2.2 Ensure packet redirect sending is disabled - sysctl net.ipv4.conf.default.send_redirects=0	FAILED
10	3.3.1 Ensure source routed packets are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.all.accept_source_route = 0	FAILED
11	3.3.1 Ensure source routed packets are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.default.accept_source_route = 0	FAILED
12	3.3.1 Ensure source routed packets are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv6.conf.all.accept_source_route = 0	FAILED
13	3.3.1 Ensure source routed packets are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv6.conf.default.accept_source_route = 0	FAILED
14	3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv4.conf.all.accept_source_route=0	PASSED
15	3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv4.conf.default.accept_source_route=0	PASSED
16	3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv6.conf.all.accept_source_route=0	PASSED
17	3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv6.conf.default.accept_source_route=0	PASSED
18	3.3.2 Ensure ICMP redirects are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.all.accept_redirects=0	FAILED
19	3.3.2 Ensure ICMP redirects are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.default.accept_redirects=0	FAILED

20	3.3.2 Ensure ICMP redirects are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv6.conf.all.accept_redirects=0	FAILED
21	3.3.2 Ensure ICMP redirects are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv6.conf.default.accept_redirects=0	FAILED
22	3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv4.conf.all.accept_redirects=0	FAILED
23	3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv4.conf.default.accept_redirects=0	FAILED
24	3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv6.conf.all.accept_redirects=0	FAILED
25	3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv6.conf.default.accept_redirects=0	FAILED
26	3.3.3 Ensure secure ICMP redirects are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.all.secure_redirects=0	FAILED
27	3.3.3 Ensure secure ICMP redirects are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.default.secure_redirects=0	FAILED
28	3.3.3 Ensure secure ICMP redirects are not accepted - sysctl net.ipv4.conf.all.secure_redirects=0	FAILED
29	3.3.3 Ensure secure ICMP redirects are not accepted - sysctl net.ipv4.conf.default.secure_redirects=0	FAILED
30	3.3.4 Ensure suspicious packets are logged - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.all.log_martians=1	FAILED
31	3.3.4 Ensure suspicious packets are logged - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.default.log_martians=1	FAILED
32	3.3.4 Ensure suspicious packets are logged - sysctl net.ipv4.conf.all.log_martians=1	FAILED
33	3.3.4 Ensure suspicious packets are logged - sysctl net.ipv4.conf.default.log_martians=1	FAILED
34	3.3.5 Ensure broadcast ICMP requests are ignored - /etc/sysctl.conf /etc/sysctl.d/*	FAILED
35	3.3.5 Ensure broadcast ICMP requests are ignored - sysctl	PASSED
36	3.3.6 Ensure bogus ICMP responses are ignored - /etc/sysctl.conf /etc/sysctl.d/*	FAILED
37	3.3.6 Ensure bogus ICMP responses are ignored - sysctl	PASSED
38	3.3.7 Ensure Reverse Path Filtering is enabled - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.all.rp_filter = 1	FAILED
39	3.3.7 Ensure Reverse Path Filtering is enabled - /etc/sysctl.conf /etc/sysctl.d/* net.ipv4.conf.default.rp_filter = 1	FAILED

40	3.3.7 Ensure Reverse Path Filtering is enabled - sysctl net.ipv4.conf.all.rp_filter = 1	PASSED
41	3.3.7 Ensure Reverse Path Filtering is enabled - sysctl net.ipv4.conf.default.rp_filter = 1	PASSED
42	3.3.8 Ensure TCP SYN Cookies is enabled - /etc/sysctl.conf /etc/sysctl.d/*	FAILED
43	3.3.8 Ensure TCP SYN Cookies is enabled - sysctl	PASSED
44	3.3.9 Ensure IPv6 router advertisements are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv6.conf.all.accept_ra = 0	FAILED
45	3.3.9 Ensure IPv6 router advertisements are not accepted - /etc/sysctl.conf /etc/sysctl.d/* net.ipv6.conf.default.accept_ra = 0	FAILED
46	3.3.9 Ensure IPv6 router advertisements are not accepted - sysctl net.ipv6.conf.all.accept_ra=0	FAILED
47	3.3.9 Ensure IPv6 router advertisements are not accepted - sysctl net.ipv6.conf.default.accept_ra=0	FAILED
48	3.5.1.1 Ensure firewalld is installed - firewalld	PASSED
49	3.5.1.1 Ensure firewalld is installed - iptables	PASSED
50	3.5.1.2 Ensure iptables-services not installed with firewalld	PASSED
51	3.5.1.3 Ensure nftables either not installed or masked with firewalld - masked	PASSED
52	3.5.1.3 Ensure nftables either not installed or masked with firewalld - stopped	PASSED
53	3.5.1.4 Ensure firewalld service enabled and running - enabled	PASSED
54	3.5.1.4 Ensure firewalld service enabled and running - running	PASSED
55	3.5.1.5 Ensure firewalld default zone is set	PASSED
56	3.5.1.6 Ensure network interfaces are assigned to appropriate zone	PASSED
57	3.5.1.7 Ensure firewalld drops unnecessary services and ports	PASSED
58	3.5.2.1 Ensure nftables is installed	PASSED
59	3.5.2.10 Ensure nftables service is enabled	PASSED
60	3.5.2.11 Ensure nftables rules are permanent	PASSED

61	3.5.2.2 Ensure firewalld is either not installed or masked with nftables - masked	PASSED
62	3.5.2.2 Ensure firewalld is either not installed or masked with nftables - stopped	PASSED
63	3.5.2.3 Ensure iptables-services not installed with nftables	PASSED
64	3.5.2.4 Ensure iptables are flushed with nftables - ip6tables	PASSED
65	3.5.2.4 Ensure iptables are flushed with nftables - iptables	PASSED
66	3.5.2.5 Ensure an nftables table exists	PASSED
67	3.5.2.6 Ensure nftables base chains exist - hook forward	PASSED
68	3.5.2.6 Ensure nftables base chains exist - hook input	PASSED
69	3.5.2.6 Ensure nftables base chains exist - hook output	PASSED
70	3.5.2.7 Ensure nftables loopback traffic is configured - iif lo	PASSED
71	3.5.2.7 Ensure nftables loopback traffic is configured - ip saddr	PASSED
72	3.5.2.7 Ensure nftables loopback traffic is configured - ip6 saddr	PASSED
73	3.5.2.8 Ensure nftables outbound and established connections are configured - input	PASSED
74	3.5.2.8 Ensure nftables outbound and established connections are configured - output	PASSED
75	3.5.2.9 Ensure nftables default deny firewall policy - forward	PASSED
76	3.5.2.9 Ensure nftables default deny firewall policy - input	PASSED
77	3.5.2.9 Ensure nftables default deny firewall policy - output	PASSED
78	3.5.3.1.1 Ensure iptables packages are installed - iptables	PASSED
79	3.5.3.1.1 Ensure iptables packages are installed - iptables-services	FAILED
80	3.5.3.1.2 Ensure nftables is not installed with iptables	PASSED
81	3.5.3.1.3 Ensure firewalld is either not installed or masked with iptables - masked	PASSED

82	3.5.3.1.3 Ensure firewalld is either not installed or masked with iptables - stopped	PASSED
83	3.5.3.2.1 Ensure iptables loopback traffic is configured - Chain FORWARD	FAILED
84	3.5.3.2.1 Ensure iptables loopback traffic is configured - Chain INPUT	FAILED
85	3.5.3.2.1 Ensure iptables loopback traffic is configured - Chain OUTPUT	FAILED
86	3.5.3.2.2 Ensure iptables outbound and established connections are configured - input	FAILED
87	3.5.3.2.2 Ensure iptables outbound and established connections are configured - output	FAILED
88	3.5.3.2.3 Ensure iptables rules exist for all open ports	FAILED
89	3.5.3.2.4 Ensure iptables default deny firewall policy	FAILED
90	3.5.3.2.5 Ensure iptables rules are saved	FAILED
91	3.5.3.2.6 Ensure iptables is enabled and running - enabled	FAILED
92	3.5.3.2.6 Ensure iptables is enabled and running - running	FAILED
93	3.5.3.3.1 Ensure ip6tables loopback traffic is configured - Chain FORWARD	FAILED
94	3.5.3.3.1 Ensure ip6tables loopback traffic is configured - Chain INPUT	FAILED
95	3.5.3.3.1 Ensure ip6tables loopback traffic is configured - Chain OUTPUT	FAILED
96	3.5.3.3.2 Ensure ip6tables outbound and established connections are configured - INPUT	FAILED
97	3.5.3.3.2 Ensure ip6tables outbound and established connections are configured - OUTPUT	FAILED
98	3.5.3.3.3 Ensure ip6tables firewall rules exist for all open ports	FAILED
99	3.5.3.3.4 Ensure ip6tables default deny firewall policy	FAILED
100	3.5.3.3.5 Ensure ip6tables rules are saved	FAILED
101	3.5.3.3.6 Ensure ip6tables is enabled and running	FAILED
102	3.5.3.3.6 Ensure ip6tables is enabled and running - enabled	FAILED

5.1.3.1.1.4 Logging and Auditing

NO	CHECK NAME	RESULT
1	4.2.1.1 Ensure rsyslog is installed	PASSED
2	4.2.1.2 Ensure rsyslog service is enabled and running	PASSED
3	4.2.1.3 Ensure rsyslog default file permissions are configured	FAILED
4	4.2.1.4 Ensure logging is configured	FAILED
5	4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host	FAILED
6	4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts	FAILED
7	4.2.2.1 Ensure journald is configured to send logs to rsyslog	FAILED
8	4.2.2.2 Ensure journald is configured to compress large log files	FAILED
9	4.2.2.3 Ensure journald is configured to write logfiles to persistent disk	FAILED
10	4.2.3 Ensure logrotate is configured	FAILED
11	4.2.4 Ensure permissions on all logfiles are configured	FAILED

5.1.3.1.1.5 Access, Authentication and Authorization

NO	CHECK NAME	RESULT
1	5.1.1 Ensure cron daemon is enabled and running - enabled	PASSED
2	5.1.1 Ensure cron daemon is enabled and running - running	PASSED
3	5.1.2 Ensure permissions on /etc/crontab are configured	PASSED
4	5.1.3 Ensure permissions on /etc/cron.hourly are configured	PASSED
5	5.1.4 Ensure permissions on /etc/cron.daily are configured	PASSED
6	5.1.5 Ensure permissions on /etc/cron.weekly are configured	PASSED
7	5.1.6 Ensure permissions on /etc/cron.monthly are configured	PASSED
8	5.1.7 Ensure permissions on /etc/cron.d are configured	PASSED
9	5.1.8 Ensure cron is restricted to authorized users - cron.allow	PASSED
10	5.1.8 Ensure cron is restricted to authorized users - cron.deny	PASSED
11	5.1.9 Ensure at is restricted to authorized users - at.allow	PASSED
12	5.1.9 Ensure at is restricted to authorized users - at.deny	PASSED
13	5.2.1 Ensure sudo is installed	PASSED
14	5.2.2 Ensure sudo commands use pty	FAILED
15	5.2.3 Ensure sudo log file exists	FAILED
16	5.3.1 Ensure permissions on /etc/ssh/sshd_config are configured	PASSED
17	5.3.10 Ensure SSH root login is disabled	FAILED
18	5.3.11 Ensure SSH PermitEmptyPasswords is disabled	FAILED
19	5.3.12 Ensure SSH PermitUserEnvironment is disabled	FAILED
20	5.3.13 Ensure only strong Ciphers are used	FAILED

21	5.3.13 Ensure only strong Ciphers are used - approved ciphers	FAILED
22	5.3.14 Ensure only strong MAC algorithms are used - approved MACs	FAILED
23	5.3.14 Ensure only strong MAC algorithms are used - weak MACs	FAILED
24	5.3.15 Ensure only strong Key Exchange algorithms are used - approved algorithms	FAILED
25	5.3.15 Ensure only strong Key Exchange algorithms are used - weak algorithms	FAILED
26	5.3.16 Ensure SSH Idle Timeout Interval is configured - ClientAliveCountMax	FAILED
27	5.3.16 Ensure SSH Idle Timeout Interval is configured - ClientAliveInterval	FAILED
28	5.3.17 Ensure SSH LoginGraceTime is set to one minute or less	FAILED
29	5.3.18 Ensure SSH warning banner is configured	FAILED
30	5.3.19 Ensure SSH PAM is enabled	FAILED
31	5.3.2 Ensure permissions on SSH private host key files are configured	PASSED
32	5.3.21 Ensure SSH MaxStartups is configured	FAILED
33	5.3.22 Ensure SSH MaxSessions is limited	FAILED
34	5.3.3 Ensure permissions on SSH public host key files are configured	PASSED
35	5.3.4 Ensure SSH access is limited - sshd ouput	FAILED
36	5.3.4 Ensure SSH access is limited - sshd_config	FAILED
37	5.3.5 Ensure SSH LogLevel is appropriate	FAILED
38	5.3.7 Ensure SSH MaxAuthTries is set to 4 or less	FAILED
39	5.3.8 Ensure SSH IgnoreRhosts is enabled	FAILED
40	5.3.9 Ensure SSH HostbasedAuthentication is disabled	FAILED
41	5.4.1 Ensure password creation requirements are configured - dcredit	FAILED
42	5.4.1 Ensure password creation requirements are configured - lcredit	FAILED

43	5.4.1 Ensure password creation requirements are configured - minlen	FAILED
44	5.4.1 Ensure password creation requirements are configured - ocredit	FAILED
45	5.4.1 Ensure password creation requirements are configured - password-auth retry=3	PASSED
46	5.4.1 Ensure password creation requirements are configured - password-auth try_first_pass	PASSED
47	5.4.1 Ensure password creation requirements are configured - system-auth retry=3	PASSED
48	5.4.1 Ensure password creation requirements are configured - system-auth try_first_pass	PASSED
49	5.4.1 Ensure password creation requirements are configured - ucredit	FAILED
50	5.4.2 Ensure lockout for failed password attempts is configured - password-auth	FAILED
51	5.4.2 Ensure lockout for failed password attempts is configured - password-auth 'auth sufficient pam_unix.so'	FAILED
52	5.4.2 Ensure lockout for failed password attempts is configured - system-auth	FAILED
53	5.4.2 Ensure lockout for failed password attempts is configured - system-auth 'auth sufficient pam_unix.so'	FAILED
54	5.4.3 Ensure password hashing algorithm is SHA-512 - password-auth	PASSED
55	5.4.3 Ensure password hashing algorithm is SHA-512 - system-auth	PASSED
56	5.4.4 Ensure password reuse is limited - password-auth	FAILED
57	5.4.4 Ensure password reuse is limited - system-auth	FAILED
58	5.5.1.1 Ensure password expiration is 365 days or less - login.defs	FAILED
59	5.5.1.1 Ensure password expiration is 365 days or less - users	PASSED
60	5.5.1.2 Ensure minimum days between password changes is configured - /etc/login.defs	FAILED
61	5.5.1.2 Ensure minimum days between password changes is configured - /etc/shadow	FAILED
62	5.5.1.3 Ensure password expiration warning days is 7 or more - login.defs	PASSED
63	5.5.1.3 Ensure password expiration warning days is 7 or more - users	FAILED

64	5.5.1.4 Ensure inactive password lock is 30 days or less - useradd	FAILED
65	5.5.1.4 Ensure inactive password lock is 30 days or less - users	FAILED
66	5.5.1.5 Ensure all users last password change date is in the past	PASSED
67	5.5.2 Ensure system accounts are secured - non-login shell	PASSED
68	5.5.2 Ensure system accounts are secured - unlocked non-root	PASSED
69	5.5.3 Ensure default group for the root account is GID 0	PASSED
70	5.5.4 Ensure default user shell timeout is configured	FAILED
71	5.5.5 Ensure default user umask is configured - system wide default	FAILED
72	5.5.5 Ensure default user umask is configured - system wide umask	FAILED
73	5.6 Ensure root login is restricted to system console	FAILED
74	5.7 Ensure access to the su command is restricted - /etc/group	FAILED
75	5.7 Ensure access to the su command is restricted - /etc/pam.d/su	FAILED

5.1.3.1.1.6 System Maintenance

NO	CHECK NAME	RESULT
1	6.1.10 Ensure no world writable files exist	FAILED
2	6.1.11 Ensure no unowned files or directories exist	PASSED
3	6.1.12 Ensure no ungrouped files or directories exist	PASSED
4	6.1.13 Audit SUID executables	FAILED
5	6.1.14 Audit SGID executables	FAILED
6	6.1.2 Ensure permissions on /etc/passwd are configured	PASSED
7	6.1.3 Ensure permissions on /etc/passwd- are configured	PASSED
8	6.1.4 Ensure permissions on /etc/shadow are configured	PASSED
9	6.1.5 Ensure permissions on /etc/shadow- are configured	PASSED
10	6.1.6 Ensure permissions on /etc/gshadow- are configured	PASSED
11	6.1.7 Ensure permissions on /etc/gshadow are configured	PASSED
12	6.1.8 Ensure permissions on /etc/group are configured	PASSED
13	6.1.9 Ensure permissions on /etc/group- are configured	PASSED
14	6.2.1 Ensure accounts in /etc/passwd use shadowed passwords	PASSED
15	6.2.10 Ensure root PATH Integrity	FAILED
16	6.2.11 Ensure all users' home directories exist	PASSED
17	6.2.12 Ensure users own their home directories	PASSED
18	6.2.13 Ensure users' home directories permissions are 750 or more restrictive	PASSED
19	6.2.14 Ensure users' dot files are not group or world writable	PASSED
20	6.2.15 Ensure no users have .forward files	PASSED

21	6.2.16 Ensure no users have .netrc files	PASSED
22	6.2.17 Ensure no users have .rhosts files	PASSED
23	6.2.2 Ensure /etc/shadow password fields are not empty	PASSED
24	6.2.3 Ensure all groups in /etc/passwd exist in /etc/group	PASSED
25	6.2.4 Ensure shadow group is empty - /etc/group	PASSED
26	6.2.4 Ensure shadow group is empty - /etc/passwd	PASSED
27	6.2.5 Ensure no duplicate user names exist	PASSED
28	6.2.6 Ensure no duplicate group names exist	PASSED
29	6.2.7 Ensure no duplicate UIDs exist	PASSED
30	6.2.8 Ensure no duplicate GIDs exist	PASSED
31	6.2.9 Ensure root is the only UID 0 account	PASSED

5.1.3.1.2 LEVEL 2

5.1.3.1.2.1 Initial Setup

NO	CHECK NAME	RESULT
1	1.1.1.2 Ensure mounting of squashfs filesystems is disabled - lsmod	PASSED
2	1.1.1.2 Ensure mounting of squashfs filesystems is disabled - modprobe	FAILED
3	1.1.10 Ensure separate partition exists for /var	FAILED
4	1.1.11 Ensure separate partition exists for /var/tmp	FAILED
5	1.1.15 Ensure separate partition exists for /var/log	FAILED
6	1.1.16 Ensure separate partition exists for /var/log/audit	FAILED
7	1.1.17 Ensure separate partition exists for /home	FAILED
8	1.6.1.5 Ensure the SELinux mode is enforcing	FAILED

5.1.3.1.2.2 Network Configuration

NO	CHECK NAME	RESULT
1	3.1.1 Disable IPv6	FAILED
2	3.4.1 Ensure DCCP is disabled - lsmod	PASSED
3	3.4.1 Ensure DCCP is disabled - modprobe	FAILED
4	3.4.2 Ensure SCTP is disabled - lsmod	PASSED
5	3.4.2 Ensure SCTP is disabled - modprobe	FAILED

5.1.3.1.2.3 Logging and Auditing

NO	CHECK NAME	RESULT
1	4.1.1.1 Ensure auditd is installed - audit	PASSED
2	4.1.1.1 Ensure auditd is installed - audit-libs	PASSED
3	4.1.1.2 Ensure auditd service is enabled and running - enabled	PASSED
4	4.1.1.2 Ensure auditd service is enabled and running - running	PASSED
5	4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled	FAILED
6	4.1.10 Ensure unsuccessful unauthorized file access attempts are collected - auditctl b64 EACCES	FAILED
7	4.1.10 Ensure unsuccessful unauthorized file access attempts are collected - auditctl b64 EPERM	FAILED
8	4.1.10 Ensure unsuccessful unauthorized file access attempts are collected - auditctl EACCES	FAILED
9	4.1.10 Ensure unsuccessful unauthorized file access attempts are collected - auditctl EPERM	FAILED
10	4.1.10 Ensure unsuccessful unauthorized file access attempts are collected - b64 EACCES	FAILED
11	4.1.10 Ensure unsuccessful unauthorized file access attempts are collected - b64 EPERM	FAILED
12	4.1.10 Ensure unsuccessful unauthorized file access attempts are collected - EACCES	FAILED
13	4.1.10 Ensure unsuccessful unauthorized file access attempts are collected - EPERM	FAILED
14	4.1.11 Ensure use of privileged commands is collected	FAILED
15	4.1.12 Ensure successful file system mounts are collected - auditctl b64 mounts	FAILED
16	4.1.12 Ensure successful file system mounts are collected - auditctl mounts	FAILED
17	4.1.12 Ensure successful file system mounts are collected - b64 mounts	FAILED
18	4.1.12 Ensure successful file system mounts are collected - mounts	FAILED
19	4.1.13 Ensure file deletion events by users are collected	FAILED
20	4.1.13 Ensure file deletion events by users are collected - auditctl	FAILED

21	4.1.13 Ensure file deletion events by users are collected - auditctl b64	FAILED
22	4.1.13 Ensure file deletion events by users are collected - b64	FAILED
23	4.1.14 Ensure changes to system administration scope (sudoers) is collected - /etc/sudoers	FAILED
24	4.1.14 Ensure changes to system administration scope (sudoers) is collected - /etc/sudoers.d	FAILED
25	4.1.14 Ensure changes to system administration scope (sudoers) is collected - auditctl /etc/sudoers	FAILED
26	4.1.14 Ensure changes to system administration scope (sudoers) is collected - auditctl /etc/sudoers.d	FAILED
27	4.1.15 Ensure system administrator command executions (sudo) are collected - auditctl 32-bit	FAILED
28	4.1.15 Ensure system administrator command executions (sudo) are collected - auditctl 64-bit	FAILED
29	4.1.15 Ensure system administrator command executions (sudo) are collected - rules.d 32-bit	FAILED
30	4.1.15 Ensure system administrator command executions (sudo) are collected - rules.d 64-bit	FAILED
31	4.1.16 Ensure kernel module loading and unloading is collected - /sbin/insmod	FAILED
32	4.1.16 Ensure kernel module loading and unloading is collected - /sbin/modprobe	FAILED
33	4.1.16 Ensure kernel module loading and unloading is collected - /sbin/rmmod	FAILED
34	4.1.16 Ensure kernel module loading and unloading is collected - auditctl /sbin/insmod	FAILED
35	4.1.16 Ensure kernel module loading and unloading is collected - auditctl /sbin/modprobe	FAILED
36	4.1.16 Ensure kernel module loading and unloading is collected - auditctl /sbin/rmmod	FAILED
37	4.1.16 Ensure kernel module loading and unloading is collected - auditctl b64 init_module	FAILED
38	4.1.16 Ensure kernel module loading and unloading is collected - auditctl init_module	FAILED
39	4.1.16 Ensure kernel module loading and unloading is collected - b64 init_module	FAILED
40	4.1.16 Ensure kernel module loading and unloading is collected - init_module	FAILED
41	4.1.17 Ensure the audit configuration is immutable	FAILED
42	4.1.2.1 Ensure audit log storage size is configured	FAILED

43	4.1.2.2 Ensure audit logs are not automatically deleted	FAILED
44	4.1.2.3 Ensure system is disabled when audit logs are full - action_mail_acct	FAILED
45	4.1.2.3 Ensure system is disabled when audit logs are full - admin_space_left_action	FAILED
46	4.1.2.3 Ensure system is disabled when audit logs are full - space_left_action	FAILED
47	4.1.2.4 Ensure audit_backlog_limit is sufficient	FAILED
48	4.1.3 Ensure events that modify date and time information are collected - adjtimex	FAILED
49	4.1.3 Ensure events that modify date and time information are collected - adjtimex b32	FAILED
50	4.1.3 Ensure events that modify date and time information are collected - adjtimex b64	FAILED
51	4.1.3 Ensure events that modify date and time information are collected - auditctl adjtimex	FAILED
52	4.1.3 Ensure events that modify date and time information are collected - auditctl adjtimex b64	FAILED
53	4.1.3 Ensure events that modify date and time information are collected - auditctl clock_settime	FAILED
54	4.1.3 Ensure events that modify date and time information are collected - auditctl clock_settime b64	FAILED
55	4.1.3 Ensure events that modify date and time information are collected - auditctl localtime	FAILED
56	4.1.3 Ensure events that modify date and time information are collected - clock_settime	FAILED
57	4.1.3 Ensure events that modify date and time information are collected - clock_settime b32	FAILED
58	4.1.3 Ensure events that modify date and time information are collected - clock_settime b64	FAILED
59	4.1.3 Ensure events that modify date and time information are collected - localtime	FAILED
60	4.1.3 Ensure events that modify date and time information are collected - localtime b64	FAILED
61	4.1.4 Ensure events that modify user/group information are collected - /etc/group	FAILED
62	4.1.4 Ensure events that modify user/group information are collected - /etc/gshadow	FAILED
63	4.1.4 Ensure events that modify user/group information are collected - /etc/passwd	FAILED
64	4.1.4 Ensure events that modify user/group information are collected - /etc/security/opasswd	FAILED

65	4.1.4 Ensure events that modify user/group information are collected - /etc/shadow	FAILED
66	4.1.4 Ensure events that modify user/group information are collected - auditctl /etc/group	FAILED
67	4.1.4 Ensure events that modify user/group information are collected - auditctl /etc/gshadow	FAILED
68	4.1.4 Ensure events that modify user/group information are collected - auditctl /etc/passwd	FAILED
69	4.1.4 Ensure events that modify user/group information are collected - auditctl /etc/security/opasswd	FAILED
70	4.1.4 Ensure events that modify user/group information are collected - auditctl /etc/shadow	FAILED
71	4.1.5 Ensure events that modify the system's network environment are collected - /etc/hosts	FAILED
72	4.1.5 Ensure events that modify the system's network environment are collected - /etc/issue	FAILED
73	4.1.5 Ensure events that modify the system's network environment are collected - /etc/issue.net	FAILED
74	4.1.5 Ensure events that modify the system's network environment are collected - /etc/sysconfig/network	FAILED
75	4.1.5 Ensure events that modify the system's network environment are collected - /etc/sysconfig/network-scripts	FAILED
76	4.1.5 Ensure events that modify the system's network environment are collected - auditctl /etc/hosts	FAILED
77	4.1.5 Ensure events that modify the system's network environment are collected - auditctl /etc/issue	FAILED
78	4.1.5 Ensure events that modify the system's network environment are collected - auditctl /etc/issue.net	FAILED
79	4.1.5 Ensure events that modify the system's network environment are collected - auditctl /etc/sysconfig/network	FAILED
80	4.1.5 Ensure events that modify the system's network environment are collected - auditctl /etc/sysconfig/network-scripts	FAILED
81	4.1.5 Ensure events that modify the system's network environment are collected - auditctl b64 sethostname	FAILED
82	4.1.5 Ensure events that modify the system's network environment are collected - auditctl sethostname	FAILED
83	4.1.5 Ensure events that modify the system's network environment are collected - b64 sethostname	FAILED
84	4.1.5 Ensure events that modify the system's network environment are collected - sethostname	FAILED
85	4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected - /etc/selinux	FAILED
86	4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected - /usr/share/selinux	FAILED

87	4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected - auditctl /etc/selinux	FAILED
88	4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected - auditctl /usr/share/selinux	FAILED
89	4.1.7 Ensure login and logout events are collected - /var/log/lastlog	FAILED
90	4.1.7 Ensure login and logout events are collected - /var/run/faillock	FAILED
91	4.1.7 Ensure login and logout events are collected - auditctl /var/log/lastlog	FAILED
92	4.1.7 Ensure login and logout events are collected - auditctl /var/run/faillock	FAILED
93	4.1.8 Ensure session initiation information is collected - /var/log/btmp	FAILED
94	4.1.8 Ensure session initiation information is collected - /var/log/wtmp	FAILED
95	4.1.8 Ensure session initiation information is collected - /var/run/utmp	FAILED
96	4.1.8 Ensure session initiation information is collected - auditctl /var/log/wtmp	FAILED
97	4.1.8 Ensure session initiation information is collected - auditctl /var/run/btmp	FAILED
98	4.1.8 Ensure session initiation information is collected - auditctl /var/run/utmp	FAILED
99	4.1.9 Ensure discretionary access control permission modification events are collected - auditctl b64 chmod/fchmod/fchmodat	FAILED
100	4.1.9 Ensure discretionary access control permission modification events are collected - auditctl b64 chown/fchown/lchown/fchownat	FAILED
101	4.1.9 Ensure discretionary access control permission modification events are collected - auditctl b64 setxattr/lsetxattr/fsetxattr	FAILED
102	4.1.9 Ensure discretionary access control permission modification events are collected - auditctl chmod/fchmod/fchmodat	FAILED
103	4.1.9 Ensure discretionary access control permission modification events are collected - auditctl chown/fchown/lchown/fchownat	FAILED
104	4.1.9 Ensure discretionary access control permission modification events are collected - auditctl setxattr/lsetxattr/fsetxattr/removexattr	FAILED
105	4.1.9 Ensure discretionary access control permission modification events are collected - b64 chmod/fchmod/fchmodat	FAILED
106	4.1.9 Ensure discretionary access control permission modification events are collected - b64 chown/fchown/lchown/fchownat	FAILED
107	4.1.9 Ensure discretionary access control permission modification events are collected - b64 setxattr/lsetxattr/fsetxattr/removexattr	FAILED
108	4.1.9 Ensure discretionary access control permission modification events are collected - chmod/fchmod/fchmodat	FAILED

109	4.1.9 Ensure discretionary access control permission modification events are collected - chown/fchown/lchown/fchownat	FAILED
110	4.1.9 Ensure discretionary access control permission modification events are collected - setxattr/lsetxattr/fsetxattr/removexattr	FAILED

5.1.3.1.2.4 Access, Authentication and Authorization

NO	CHECK NAME	RESULT
1	5.3.20 Ensure SSH AllowTcpForwarding is disabled - sshd output	FAILED
2	5.3.20 Ensure SSH AllowTcpForwarding is disabled - sshd_config	FAILED
3	5.3.6 Ensure SSH X11 forwarding is disabled	FAILED

5.1.3.1.2.5 System Maintenance

NO	CHECK NAME	RESULT
1	6.1.1 Audit system file permissions	FAILED

5.1 Cloud Security Configuration & CIS Security Benchmarks

CVSS Score: ***N/A*** ***CVSS Vector:*** *N/A* ***Impact/Probability:*** ***Info/Info***

Affected: *Cloud ID: ABCDEFGHIJKLAMN*

The Azure Tenant and Subscriptions were assessed against the Center for Internet Security (CIS) Azure Cloud security benchmarks as described in the Technical Analysis. The Level 1 and 2 benchmarks were used for this assessment which are profiles intended to:

5.1.1 Remediation

Consider configuring the expected value in respect to the environment to further harden the build, after thorough testing. Refer to the following resource for further information: https://www.cisecurity.org/cis-benchmarks/

5.1.2 Technical Analysis

The configuration settings can be found in the following appendix:

EXTERNAL DOCUMENT NAME	COMPLIANCE STANDARDS
Azure CIS Security Benchmarks	CIS Azure Benchmark v2.0.0 Server L1 CIS Azure Benchmark v2.0.0 Server L2

5.1.3 CIS Benchmark Scores

HOST	LEVEL 1			LEVEL 2		
	PASS	FAIL	TOTAL	PASS	FAIL	TOTAL
Azure CIS Security Benchmarks	38	51	89	22	38	60

5.1.3.1.1 LEVEL 1

5.1.3.1.1.1 Identity and Access Management

NO	CHECK NAME	RESULT
1	1.1.1 Ensure Security Defaults is enabled on Azure Active Directory	FAILED
2	1.1.2 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users	FAILED
3	1.1.4 Ensure that 'Restore multi-factor authentication on all remembered devices' is Enabled	FAILED
4	1.10 Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes'	FAILED
5	1.12 Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No'	FAILED
6	1.13 Ensure that 'Users can add gallery apps to My Apps' is set to 'No'	FAILED
7	1.14 Ensure That 'Users Can Register Applications' Is Set to 'No'	FAILED
8	1.15 Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	FAILED
9	1.17 Ensure That 'Restrict access to Azure AD administration portal' is Set to 'Yes'	FAILED
10	1.2.1 Ensure Trusted Locations Are Defined	FAILED
11	1.2.2 Ensure that an exclusionary Geographic Access Policy is considered	FAILED
12	1.2.3 Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups	FAILED
13	1.2.4 Ensure that A Multi-factor Authentication Policy Exists for All Users	FAILED
14	1.2.5 Ensure Multi-factor Authentication is Required for Risky Sign-ins	FAILED
15	1.2.6 Ensure Multi-factor Authentication is Required for Azure Management	FAILED
16	1.22 Ensure that 'Require Multi-Factor Authentication to register or join devices with Azure AD' is set to 'Yes'	FAILED
17	1.23 Ensure That No Custom Subscription Owner Roles Are Created	FAILED
18	1.4 Ensure Guest Users Are Reviewed on a Regular Basis	FAILED
19	1.5 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled'	FAILED

20	1.6 Ensure That 'Number of methods required to reset' is set to '2'	FAILED
21	1.7 Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization	FAILED
22	1.8 Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	FAILED
23	1.9 Ensure that 'Notify users on password resets?' is set to 'Yes'	FAILED

5.1.3.1.1.2 Microsoft Defender

NO	CHECK NAME	RESULT
1	2.2.1 Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On'	PASSED
2	2.3.1 Ensure That 'All users with the following roles' is set to 'Owner'	FAILED
3	2.3.2 Ensure 'Additional email addresses' is Configured with a Security Contact Email	FAILED
4	2.3.3 Ensure That 'Notify about alerts with the following severity' is Set to 'High'	FAILED
5	2.5 Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed'	FAILED
6	2.6 Ensure Any of the ASC Default Policy Settings are Not Set to 'Disabled'	FAILED

5.1.3.1.1.3 Storage Accounts

No	Check Name	Result
1	3.1 Ensure that 'Secure transfer required' is set to 'Enabled'	PASSED
2	3.10 Ensure Private Endpoints are used to access Storage Accounts	FAILED
3	3.11 Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	FAILED
4	3.15 Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	PASSED
5	3.3 Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	FAILED
6	3.4 Ensure that Storage Account Access Keys are Periodically Regenerated	FAILED
7	3.6 Ensure that Shared Access Signature Tokens Expire Within an Hour	FAILED
8	3.7 Ensure that 'Public access level' is disabled for storage accounts with blob containers	FAILED
9	3.8 Ensure Default Network Access Rule for Storage Accounts is Set to Deny	FAILED

5.1.3.1.1.4 Database Services

No	Check Name	Result
1	4.1.1 Ensure that 'Auditing' is set to 'On'	PASSED
2	4.1.2 Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	PASSED
3	4.1.4 Ensure that Azure Active Directory Admin is Configured for SQL Servers	PASSED
4	4.1.5 Ensure that 'Data encryption' is set to 'On' on a SQL Database	PASSED
5	4.1.6 Ensure that 'Auditing' Retention is 'greater than 90 days'	PASSED
6	4.2.5 Ensure that Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners' is set for each SQL Server	PASSED
7	4.3.1 Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server	PASSED
8	4.3.2 Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	PASSED
9	4.3.3 Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server	PASSED
10	4.3.4 Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	PASSED
11	4.3.5 Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	PASSED
12	4.3.6 Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server	PASSED
13	4.3.7 Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	PASSED
14	4.3.8 Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled'	PASSED
15	4.4.1 Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server	PASSED
16	4.4.2 Ensure 'TLS Version' is set to 'TLSV1.2' for MySQL flexible Database Server	PASSED

5.1.3.1.1.5 Logging and Monitoring

No	Check Name	Result
1	5.1.1 Ensure that a 'Diagnostic Setting' exists	FAILED
2	5.1.2 Ensure Diagnostic Setting captures appropriate categories	FAILED
3	5.1.3 Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible	FAILED
4	5.1.5 Ensure that logging for Azure Key Vault is 'Enabled'	FAILED
5	5.2.1 Ensure that Activity Log Alert exists for Create Policy Assignment	FAILED
6	5.2.10 Ensure that Activity Log Alert exists for Delete Public IP Address rule	FAILED
7	5.2.2 Ensure that Activity Log Alert exists for Delete Policy Assignment	FAILED
8	5.2.3 Ensure that Activity Log Alert exists for Create or Update Network Security Group	FAILED
9	5.2.4 Ensure that Activity Log Alert exists for Delete Network Security Group	FAILED
10	5.2.5 Ensure that Activity Log Alert exists for Create or Update Security Solution	FAILED
11	5.2.6 Ensure that Activity Log Alert exists for Delete Security Solution	FAILED
12	5.2.7 Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	FAILED
13	5.2.8 Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	FAILED
14	5.2.9 Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	FAILED
15	5.3 Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	FAILED

5.1.3.1.1.6 Networking

No	Check Name	Result
1	6.1 Ensure that RDP access from the Internet is evaluated and restricted	PASSED
2	6.2 Ensure that SSH access from the Internet is evaluated and restricted	PASSED
3	6.3 Ensure that UDP access from the Internet is evaluated and restricted	PASSED
4	6.4 Ensure that HTTP(S) access from the Internet is evaluated and restricted	PASSED
5	6.7 Ensure that Public IP addresses are Evaluated on a Periodic Basis	FAILED

5.1.3.1.1.7 Virtual Machines

No	Check Name	Result
1	7.1 Ensure Virtual Machines are utilizing Managed Disks	PASSED
2	7.4 Ensure that Only Approved Extensions Are Installed	PASSED

5.1.3.1.1.8 Key Vault

No	Check Name	Result
1	8.1 Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	PASSED
2	8.2 Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	PASSED
3	8.3 Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	PASSED
4	8.4 Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	PASSED
5	8.5 Ensure the Key Vault is Recoverable	PASSED

5.1.3.1.1.9 AppService

No	Check Name	Result
1	9.10 Ensure FTP deployments are Disabled	PASSED
2	9.2 Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service	PASSED
3	9.3 Ensure Web App is using the latest version of TLS encryption	PASSED
4	9.5 Ensure that Register with Azure Active Directory is enabled on App Service	PASSED
5	9.6 Ensure That 'PHP version' is the Latest, If Used to Run the Web App	PASSED
6	9.7 Ensure that 'Python version' is the Latest Stable Version, if Used to Run the Web App	PASSED
7	9.8 Ensure that 'Java version' is the latest, if used to run the Web App	PASSED
8	9.9 Ensure that 'HTTP Version' is the Latest, if Used to Run the Web App	PASSED

5.1.3.1.2 LEVEL 2

5.1.3.1.2.1 Identity and Access Management

No	Check Name	Result
1	1.1.3 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users - List Users	FAILED
2	1.1.3 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users - Role Assignments	FAILED
3	1.1.3 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users - Role Definitions	FAILED
4	1.11 Ensure That 'Users Can Consent to Apps Accessing Company Data on Their Behalf' Is Set To 'Allow for Verified Publishers'	FAILED
5	1.16 Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	FAILED
6	1.18 Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes'	FAILED
7	1.19 Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	FAILED
8	1.20 Ensure that 'Owners can manage group membership requests in the Access Panel' is set to 'No'	FAILED
9	1.21 Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	FAILED
10	1.24 Ensure a Custom Role is Assigned Permissions for Administering Resource Locks	FAILED
11	1.25 Ensure That 'Subscription Entering AAD Directory' and 'Subscription Leaving AAD Directory' Is Set To 'Permit No One'	FAILED
12	1.3 Ensure Access Review is Set Up for External Users in Azure AD Privileged Identity Management	FAILED
13	10.1 Ensure that Resource Locks are set for Mission-Critical Azure Resources	FAILED

5.1.3.1.2.2 Microsoft Defender

No	Check Name	Result
1	2.1.1 Ensure That Microsoft Defender for Servers Is Set to 'On'	FAILED
2	2.1.10 Ensure That Microsoft Defender for Key Vault Is Set To 'On'	FAILED
3	2.1.11 Ensure That Microsoft Defender for DNS Is Set To 'On'	FAILED
4	2.1.12 Ensure That Microsoft Defender for IoT Is Set To 'On'	FAILED
5	2.1.13 Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	FAILED
6	2.1.2 Ensure That Microsoft Defender for App Services Is Set To 'On'	FAILED
7	2.1.3 Ensure That Microsoft Defender for Databases Is Set To 'On'	FAILED
8	2.1.4 Ensure That Microsoft Defender for Azure SQL Databases Is Set To 'On'	FAILED
9	2.1.5 Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	FAILED
10	2.1.6 Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	FAILED
11	2.1.7 Ensure That Microsoft Defender for Storage Is Set To 'On'	FAILED
12	2.1.8 Ensure That Microsoft Defender for Containers Is Set To 'On'	FAILED
13	2.1.9 Ensure That Microsoft Defender for Cosmos DB Is Set To 'On'	FAILED
14	2.2.2 Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On'	PASSED
15	2.2.3 Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On'	PASSED
16	2.4.1 Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected	FAILED
17	2.4.2 Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected	FAILED

5.1.3.1.2.3 Storage Accounts

No	Check Name	Result
1	3.12 Ensure Storage for Critical Data are Encrypted with Customer Managed Keys	FAILED
2	3.13 Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	FAILED
3	3.14 Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	FAILED
4	3.2 Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled'	FAILED
5	3.5 Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	FAILED
6	3.9 Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	PASSED

5.1.3.1.2.4 Database Services

No	Check Name	Result
1	4.1.3 Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	PASSED
2	4.2.1 Ensure that Microsoft Defender for SQL is set to 'On' for critical SQL Servers	PASSED
3	4.2.2 Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account	PASSED
4	4.2.3 Ensure that Vulnerability Assessment (VA) setting 'Periodic recurring scans' is set to 'on' for each SQL server	PASSED
5	4.2.4 Ensure that Vulnerability Assessment (VA) setting 'Send scan reports to' is configured for a SQL server	PASSED
6	4.4.3 Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server	PASSED
7	4.4.4 Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server	PASSED
8	4.5.1 Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	FAILED
9	4.5.2 Ensure That Private Endpoints Are Used Where Possible	FAILED

5.1.3.1.2.5 Logging and Monitoring

No	Check Name	Result
1	5.1.4 Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key	FAILED
2	5.1.6 Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	FAILED
3	5.1.7 Ensure that logging for Azure AppService 'AppServiceHTTPLogs' is enabled.	PASSED

5.1.3.1.2.6 Networking

No	Check Name	Result
1	6.5 Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	PASSED
2	6.6 Ensure that Network Watcher is 'Enabled'	FAILED

5.1.3.1.2.7 Virtual Machines

No	Check Name	Result
1	7.2 Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	PASSED
2	7.3 Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	PASSED
3	7.5 Ensure that Endpoint Protection for all Virtual Machines is installed	PASSED
4	7.6 [Legacy] Ensure that VHDs are Encrypted	PASSED

5.1.3.1.2.8 Key Vault

NO	CHECK NAME	RESULT
1	8.6 Enable Role Based Access Control for Azure Key Vault	PASSED
2	8.7 Ensure that Private Endpoints are Used for Azure Key Vault	PASSED
3	8.8 Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services	PASSED

5.1.3.1.2.9 AppService

No	Check Name	Result
1	9.1 Ensure App Service Authentication is set up for apps in Azure App Service	PASSED
2	9.11 Ensure Azure Key Vaults are Used to Store Secrets	PASSED
3	9.4 Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On'	PASSED

6 APPENDIX A: TESTING METHODOLOGIES

The overall aim is to ensure a thorough security assessment is carried out where critical risks are identified and highlighted. Steps are taken to ensure disruption to the business is minimised and that appropriate communication paths exist to enable quick incident response. The following sections outline the methodology employed to achieve this.

6.1 Internal Infrastructure Testing Methodology

Network Reconnaissance

Network reconnaissance is performed to identify active hosts. The network structure is mapped using DNS lookups/brute-force and zone transfers, route tracing to remote targets, extracting routing information from hosts and network devices, ping sweeps and NetBIOS nameserver enumeration.

Target Identification

At this stage, the gathered information is reviewed to find key devices that could be targeted. Thorough port scanning is conducted to identify active services on each target.

Share Enumeration

Open network shares are enumerated and examined as these may contain passwords for privileged accounts and/or sensitive data. A combination of automated tools and manual file browsing is used to achieve this.

Vulnerability Assessment

Identified services are scanned for security flaws. Typically, an unauthenticated scan is performed first to help identify vulnerabilities that can be used to gain privileged access. Once privileged access is obtained an authenticated scan may be run where additional local checks are performed to ensure more reliable results.

Vulnerability Exploitation

Security flaws discovered previously are exploited to gain access to systems and/or elevate privileges. Compromised hosts are examined for sensitive files and stored credentials that may be used to further compromise the domain. Proof of concept code is written to illustrate potential exploits.

Privilege Escalation

The overall aim is to achieve the highest level of privilege possible, (e.g. “Domain Admin” or “root”) to then gain unrestricted access to hosts connected to the domain. To assist in achieving this brute-forcing weak account passwords, password reuse, impersonation techniques and local privilege escalation exploits are used.

Data Exfiltration

Once access to sensitive data is obtained data exfiltration is verified by attempting to copy non-sensitive data residing within the internal network to an outside system controlled by the tester. This is typically done by establishing direct outbound connections, pivoting via a compromised host or re-configuring a security device.

6.2 Cloud Testing Methodology

6.2.1 Configuration Review

A cloud configuration review consists of a white box assessment of your cloud environments including Microsoft 365, Google Workspace, Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP), to assess compliance with security best practice, and identify weaknesses and common misconfigurations. The configuration review will assess the security posture of the cloud management environment (control plane) as well as the applications and infrastructure hosted within (data plane) and is a useful adjunct to traditional penetration and web application testing.

Your account will be reviewed against industry guidelines and best practices including the CIS Foundations benchmark and Security team own methodology for performing cloud security assessments. The assessment aims to improve the overall security posture of your cloud users, applications and devices by providing defence-in-depth recommendations for further hardening.

Assessment components of a typical Cloud Security Configuration Review include, but are not limited to:

- Industry best practice and benchmarks
- IAM configuration
- Network security controls and segmentation
- Public and exposed services
- Encryption and Key Management
- Secure configurations
- Auditing & Logging
- Account hygiene
- Contextual and client specific findings

In order to assess the configuration of your cloud environments full read access via the web console and APIs is required and because testing is typically white box there is no requirement to inform or obtain authorisation from AWS, Microsoft Azure or GCP in order perform the assessment.

Three service levels are available:

6.2.2 Level 1

A level 1 cloud configuration review aims to improve the overall security posture of your account and deployed resources and provide baseline of security for cloud workloads. CCS will assess accounts against relevant industry guidelines and best practices including:

- CIS Amazon Web Services Foundations Benchmark
- AWS Foundational Security Best Practices Standards
- CIS Microsoft 365 Foundations Benchmark
- Office 365 UK Blueprint - Secure Configuration Alignment
- CIS Microsoft Azure Foundations Benchmark
- CIS Google Cloud Platform Foundations Benchmark

6.2.3 Level 2

A level 2 assessment extends the services provided in level 1 by expanding the number and scope of configuration checks and is often an adjunct to traditional penetration and web application testing.

Performed as a consultant-led white box configuration review, CCS will provide a contextual assessment of the configuration of accounts and deployed services to identify vulnerabilities stemming from misconfigurations, default controls and a lack of security best practice hardening.

This assessment aims to identify security weaknesses affecting both the control plane and data plane configurations which could be leveraged by threat actors to gain and extend unauthorised access to resources; for example, a user manipulating access to the control plane to gain access to secrets within AWS Secrets Manager.

7 APPENDIX B: MICROSOFT AZURE CIS FOUNDATIONS BENCHMARK EVALUATION

Center for Internet Security (CIS) Benchmarks are a standard for prescriptive, industry-accepted best practices for securely configuring traditional IT components. CIS Microsoft Azure Foundations Security Benchmark provides prescriptive guidance for establishing a secure baseline configuration for Microsoft Azure. Version 2 of the guide was created in Feb 2023 and includes the following Services.

1. Identity and Access Management
2. Microsoft Defender for Cloud
3. Storage Accounts
4. Database Services
5. Logging and Monitoring
6. Networking
7. Virtual Machines
8. Key Vault
9. App Service
10. Miscellaneous

The CIS Benchmark defines two security profiles as defined below:

Level 1

Items in this profile intend to:

- Be practical and prudent
- Provide a clear security benefit
- Not inhibit the utility of the technology beyond acceptable means

Level 2

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- Intended for environments or use cases where security is paramount
- Acts as defence in depth measure
- May negatively inhibit the utility or performance of the technology.

The target Microsoft Azure Account was compared against the Azure CIS Foundations Benchmark any discrepancies have been listed below.

7.1.1 Remediation

Consult the Azure CIS Foundations benchmark for step-by-step guidance on how to remediate any highlighted issues.

More information: https://www.cisecurity.org/benchmark/azure/

7.1.2 Technical Analysis

The tables below detail the results of the CIS benchmark v2 audit.

1. Identity and Access Management

1.1 SECURITY DEFAULTS

The Azure "Security Defaults" recommendations represent an entry-level set of recommendations which will be relevant to organizations and tenants that are either just starting to use Azure as an IaaS solution or are only utilizing a bare minimum feature set such as the freely licensed tier of Azure Active Directory. Security Defaults recommendations are intended to ensure that these entry-level use cases are still capable of establishing a strong baseline of secure configuration.

Because CIPFA make use of a Microsoft Entra ID P2 licence these recommendations can be ignored in favour of conditional access.

CHECK	LEVEL	BENCHMARK
1.1.1	1	Ensure Security Defaults is enabled on Azure Active Directory
1.1.2	1	Ensure that 'Multi-Factor' Auth Status is 'Enabled' for all Privileged Users
1.1.3	2	Ensure that 'Multi-Factor' Auth Status is 'Enabled' for all Non-Privileged Users
1.1.4	2	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled

1.2 CONDITIONAL ACCESS

For most Azure tenants, and certainly for organizations with a significant use of Azure Active Directory, Conditional Access policies are recommended and preferred. To use conditional access policies, a licensing plan is required, and Security Defaults must be disabled.

CHECK	LEVEL	BENCHMARK
1.2.1	1	Ensure Trusted Locations Are Defined
1.2.2	1	Ensure that an exclusionary Geographic Access Policy is considered
1.2.3	1	Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups
1.2.4	1	Ensure that A Multi-factor Authentication Policy Exists for All Users
1.2.5	1	Ensure that A Multi-factor Authentication is Required for Risky Sign-ins
1.2.6	1	Ensure that A Multi-factor Authentication is Required for Azure Management
1.3	1	Ensure that 'Users can create Azure AD Tenants' is set to 'No'
1.4	2	Ensure Access Review is Set Up for External Users in AzureAD Privileged Identity Management
1.5	1	Ensure Guest Users Are Reviewed on a Regular Basis
1.6	1	Ensure that 'Number of methods required to reset' is set to '2'
1.7	1	Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization

CHECK	LEVEL	BENCHMARK
1.8	1	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to 0
1.9	1	Ensure that 'Notify users on password resets?' is set to 'Yes'
1.10	1	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes'
1.11	1	Ensure User consent for applications is set to Do not allow user consent
1.12	2	Ensure 'User consent for applications' Is Set To 'Allow for Verified Publishers'
1.13	1	Ensure that 'Users can add gallery apps to My Apps' is set to 'No'
1.14	1	Ensure that 'Users can register applications' is set to 'No'
1.15	1	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'
1.16	2	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'
1.17	1	Ensure That 'Restrict access to Azure AD administration portal' is Set to 'Yes'
1.18	2	Ensure that 'Restrict user ability to access groups features in the Access Pane' is set to 'Yes'
1.19	2	Ensure that 'Users can create security groups in Azure portals API or PowerShell' is set to 'No'
1.20	2	Ensure that 'Owners can manage group membership requests in the Access Panel' is set to 'No'
1.21	2	Ensure that 'Users can create Microsoft 365 groups in Azure portals API or PowerShell' is set to 'No'
1.22	1	Ensure that 'Require Multi-Factor Authentication to register or join devices with Azure AD' is set to 'Yes'
1.23	1	Ensure That No Custom Subscription Administrator Roles Exist
1.24	2	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks
1.25	2	Ensure That 'Subscription Entering AAD Directory' and 'Subscription Leaving AAD Directory' Is Set To 'Permit No One'

2. Microsoft Defender for Cloud

CHECK	LEVEL	BENCHMARK
2.1.1	2	Ensure that Microsoft Defender for servers is set to On
2.1.2	2	Ensure that Microsoft Defender for App Service is set to On
2.1.3	2	Ensure that Microsoft Defender for Databases is set to On
2.1.4	2	Ensure that Microsoft Defender for Azure SQL Databases is set to On
2.1.5	2	Ensure that Microsoft Defender for SQL Servers on Machines is set to On
2.1.6	2	Ensure that Microsoft Defender for Open-Source Relational Databases is set to On
2.1.7	2	Ensure that Microsoft Defender for Storage is set to On
2.1.8	2	Ensure that Microsoft Defender for Containers is set to On
2.1.9	2	Ensure that Microsoft Defender for Cosmos DB is set to On
2.1.10	2	Ensure that Microsoft Defender for Key Vault is set to On
2.1.11	2	Ensure that Microsoft Defender for DNS is set to On
2.1.12	2	Ensure that Microsoft Defender for Resource Manager is set to On
2.1.13	1	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed'
2.1.14	1	Ensure Any of the ASC Default Policy Settings are Not Set to 'Disabled'
2.1.15	1	Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On'
2.1.16	2	Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On'
2.1.17	2	Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On'
2.1.18	1	Ensure That 'All users with the following roles' is set to 'Owner'
2.1.19	1	Ensure 'Additional email addresses' is Configured with a Security Contact Email
2.1.20	1	Ensure That 'Notify about alerts with the following severity' is Set to 'High'
2.1.21	2	Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected

CHECK	LEVEL	BENCHMARK
2.1.22	2	Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected
2.2.1	2	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'

3. Storage Accounts

CHECK	LEVEL	BENCHMARK
3.1	1	Ensure that 'Secure transfer required' is set to 'Enabled'
3.2	2	Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled'
3.3	1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account
3.4	1	Ensure that storage account access keys are periodically regenerated
3.5	2	Ensure Storage logging is enabled for Queue service for read write and delete requests
3.6	1	Ensure that Shared Access Signature Tokens Expire Within an Hour
3.7	1	Ensure that 'Public access level' is disabled for storage accounts with blob containers
3.8	2	Ensure default network access rule for Storage Accounts is set to deny
3.9	2	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access
3.10	1	Ensure Private Endpoints are used to access Storage Accounts
3.11	1	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage
3.12	2	Ensure storage for critical data are encrypted with Customer Managed Keys
3.13	2	Ensure Storage logging is enabled for Blob service for read write and delete requests
3.14	2	Ensure Storage logging is enabled for Table service for read write and delete requests
3.15	1	Ensure the 'Minimum TLS version' is set to 'Version 1.2'

4. Database Services

SQL SERVER – AUDITING

CHECK	LEVEL	BENCHMARK
4.1.1	1	Ensure that 'Auditing' is set to 'On'
4.1.2	1	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)
4.1.3	2	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key
4.1.4	1	Ensure that Azure Active Directory Admin is configured for SQL Servers
4.1.5	1	Ensure that 'Data encryption' is set to 'On' on a SQL Database
4.1.6	1	Ensure that 'Auditing' Retention is 'greater than 90 days'

SQL SERVER – MICROSOFT DEFENDER FOR SQL

CHECK	LEVEL	BENCHMARK
4.2.1	2	Ensure that Microsoft Defender for SQL is set to 'On' for critical SQL Servers
4.2.2	2	Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account
4.2.3	2	Ensure that VA setting Periodic Recurring Scans is enabled on a SQL server
4.2.4	2	Ensure that VA setting Send scan reports to is configured for a SQL server
4.2.5	2	Ensure that VA Setting 'Also send email notifications to admins and subscription owners' is set for a SQL server

POSTGRESQL DATABASE SERVER

CHECK	LEVEL	BENCHMARK
4.3.1	1	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server
4.3.2	1	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server
4.3.3	1	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server
4.3.4	1	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server

CHECK	LEVEL	BENCHMARK
4.3.5	1	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server
4.3.6	1	Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server
4.3.7	1	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled
4.3.8	1	Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled'

MYSQL DATABASE

CHECK	LEVEL	BENCHMARK
4.4.1	1	Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server
4.4.2	1	Ensure 'TLS Version' is set to 'TLSV1.2' for MySQL flexible Database Server
4.4.3	2	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server
4.4.4	2	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server

COSMOS DB

CHECK	LEVEL	BENCHMARK
4.5.1	2	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks
4.5.2	2	Ensure That Private Endpoints Are Used Where Possible
4.5.3	1	Use Azure Active Directory (AAD) Client Authentication and Azure RBAC where possible.

5. Logging and Monitoring

CONFIGURING DIAGNOSTIC SETTINGS

CHECK	LEVEL	BENCHMARK
5.1.1	1	Ensure that a 'Diagnostics Setting' exists

CHECK	LEVEL	BENCHMARK
5.1.2	1	Ensure Diagnostic Setting captures appropriate categories
5.1.3	1	Ensure the storage container storing the activity logs is not publicly accessible
5.1.4	2	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key
5.1.5	1	Ensure that logging for Azure KeyVault is 'Enabled'
5.1.6	2	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics
5.1.7	2	Ensure that logging for Azure AppService 'HTTP Logs' is enabled.

MONITORING USING ACTIVITY LOG ALERTS

CHECK	LEVEL	BENCHMARK
5.2.1	1	Ensure that Activity Log Alert exists for Create Policy Assignment
5.2.2	1	Ensure that Activity Log Alert exists for Delete Policy Assignment
5.2.3	1	Ensure that Activity Log Alert exists for Create or Update Network Security Group
5.2.4	1	Ensure that Activity Log Alert exists for Delete Network Security Group
5.2.5	1	Ensure that Activity Log Alert exists for Create or Update Security Solution
5.2.6	1	Ensure that Activity Log Alert exists for Delete Security Solution
5.2.7	1	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule
5.2.8	1	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule
5.2.9	1	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule
5.2.10	1	Ensure that Activity Log Alert exists for Delete Public IP Address rule
5.3	2	Ensure Application Insights are Configured
5.4	1	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it
5.5	2	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)

6. Networking

CHECK	LEVEL	BENCHMARK
6.1	1	Ensure that RDP access from the Internet is evaluated and restricted
6.2	1	Ensure that SSH access from the Internet is evaluated and restricted
6.3	1	Ensure that UDP access from the Internet is evaluated and restricted
6.4	1	Ensure that HTTP(S) access from the Internet is evaluated and restricted
6.5	2	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'
6.6	2	Ensure that Network Watcher is 'Enabled'
6.7	1	Ensure that Public IP addresses are Evaluated on a Periodic Basis

7. Virtual Machines

CHECK	LEVEL	BENCHMARK
7.1	2	Ensure an Azure Bastion Host Exists
7.2	1	Ensure Virtual Machines are utilizing Managed Disks
7.3	2	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)
7.4	1	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)
7.5	1	Ensure that only approved extensions are installed
7.6	2	Ensure that the endpoint protection for all Virtual Machines is installed
7.7	2	[Legacy]Ensure that VHDs are encrypted

8. Key Vault

CHECK	LEVEL	BENCHMARK
8.1	1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults

CHECK	LEVEL	BENCHMARK
8.2	1	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults
8.3	1	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults
8.4	1	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults
8.5	1	Ensure the Key Vault is Recoverable
8.6	2	Enable Role Based Access Control for Azure Key Vault
8.7	2	Ensure that Private Endpoints are Used for Azure Key Vault
8.8	2	Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services

9. App Service

CHECK	LEVEL	BENCHMARK
9.1	2	Ensure App Service Authentication is set up for apps in Azure App Service
9.2	1	Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service
9.3	1	Ensure Web App is using the latest version of TLS encryption
9.4	2	Ensure the web app has Client Certificates (Incoming client certificates) set to On
9.5	1	Ensure that Register with Azure Active Directory is enabled on App Service
9.6	1	Ensure That 'PHP version' is the Latest, If Used to Run the Web App
9.7	1	Ensure that 'Python version' is the Latest Stable Version, if Used to Run the Web App
9.8	1	Ensure that Java version is the latest, if used to Run the Web App
9.9	1	Ensure that HTTP Version is the latest, if used to Run the Web App
9.10	1	Ensure FTP deployments are disabled
9.11	2	Ensure Azure Keyvaults are used to store secrets

10. Miscellaneous

CHECK	LEVEL	BENCHMARK
10.1	2	Ensure that Resource Locks are set for Mission-Critical Azure Resources

8 APPENDIX C: CLOUD SECURITY DEFENSIVE STRATEGIES

8.1 Overview

Though many of the security controls and principals used in traditional on-premises networks are similar to those employed within cloud environments, there are numerous practical differences that organisations need to be familiar with to successfully secure cloud deployments.

A practical application of cloud technology allows administrators to create, configure and deploy assets from anywhere in the world, however these changes also generate additional risk. Attackers with privileged access to the cloud control plane, can modify data plane objects to read, modify or destroy data from any part of the cloud environment, regardless of network security controls. As such, when designing security within a cloud environment, a risk-based, defence-in-depth approach should be taken to identify security requirements and develop overlapping security controls to prevent and reduce the threats faced by an organisation.

8.2 Organisational Controls

CONTROL	DESCRIPTION	RECOMMENDATIONS
User and Credential Management	When traditional network boundaries are no longer in play the user identities and credentials become the security boundary and should be subject to controls and management in order to reduce the likelihood and impact of compromised accounts being used to access the cloud environment. MFA and a strong Password Policy should be configured to enforce length and complexity requirement and protect the account from credential stuff and brute force attacks. Rotating credentials including password, access keys, API keys and certificates limits the lifespan of credentials and reduces the risk and effectiveness of credential-based attacks by reducing the window of opportunity for attackers to operate. Cloud environments provide powerful collaboration features which allow guest and 3rd parties to access and work on resources within your tenancy. These accounts may not be subject to the same strict security controls as native users and should be controlled and monitored appropriately to maintain data confidentiality and integrity. Conditional or context aware access enables security teams to implement policies and fine-grained access controls over who and how users can access cloud resources.	MFA should be enabled as a default control for all users, especially those who hold privileged access. Hardware MFA tokens and Apps should be used in preference to SMS based MFA. It is recommended that the Password Policy enforce a minimum password length of 14 characters. The use of complex passwords and prevent password reuse, where possible a blacklist of known weak passwords should also be maintained. There are no dedicated recommendations for the frequency of rotation, but a sensible approach is to consider the usage and security requirements of the users, platform and data stored or processed within. As an example, highly privileged administrator accounts should rotate credentials more often than standard users. Additional API access through the use of access keys should only be granted to users that require programmatic access to cloud resources and not as a matter of course. The number of keys each user has should also be kept to a minimum, ideally one unless in the process of being rotated. Guest and 3rd party access should be minimized and subject to the principle of least privilege. Accounts should be regularly reviewed and removed when there is no longer a business case for access being maintained. Apply context and risk-based profiling to user activity and authentication requests. Restrict access based on IP and Device, blocking the use of legacy protocols and services, and denying access based on geographical location.

CONTROL	DESCRIPTION	RECOMMENDATIONS
Privileged Identity Management	Privileged accounts represent the most powerful users within a cloud environment. Controlling, monitoring, and auditing privileged identities should be a top priority for any organization to reduce the likelihood of a malicious actor gaining compromised access to privileged accounts and preventing unauthorized access to sensitive resources. Most cloud providers offer a native PIM service, however where PIM is not directly available, several third-party offerings are available which can be integrated with a given cloud provider. Alternatively, custom policies and technical controls could be implemented to reduce standing access to privileged accounts and achieve similar results.	Successfully implementing secure PIM practices involves a multi-tiered approach. Alongside common IAM controls such as MFA and the principle of least privilege, several other controls should also be considered, including: Cloud-only administrative accounts - Where organisations sync cloud accounts with an on-premises domain controller, the privileged administrative accounts should be implemented as cloud-only. Dedicated administrative accounts – to reduce their attack surface, admin accounts should not be used for day-to-day activities such as accessing emails and applications. Separate daily user accounts with minimal privileges should be used for daily functions whilst ensuring admin accounts are signed out when not in use. Break-Glass Access – A break glass process should provide stakeholders with emergency access accounts for disaster recovery scenarios. Strong credentials should be configured for break-glass accounts and credentials should be securely stored. Enhanced logging and monitoring for emergency account usage should also be enabled. users with Just-in-Time (JIT) Access –JIT reduces standing access to privileged accounts, ensuring users only have the privileges to access sensitive accounts when they need it. Membership of privileged roles should be regularly reviewed and removed when no longer required.
Least Privilege	By restricting the privileges applied to entities, organisations can reduce unintentional capabilities which could lead to privilege escalation and exposure of data and resources	A sensible approach to creating access policies is to start with a deny by default statement, adding additionally individual privileges through a dedicated request and approval process. A simple naming convention for groups and roles which clearly indicate the level of access granted is recommended to ensure good account hygiene and enhanced maintainability. Additionally, permissions should applied at the group and role level and not directly to user principals
Network Security Controls and Firewalls	Virtual Private Clouds (VPC) can provide network isolation and segregation through multiple controls including network access control lists, security groups and Firewalls. These controls should be configured to logically segment subnets and define security boundaries using a zero-trust approach.	To reduce attack surface network security controls should use a whitelist approach to restrict access to service from a list of approved IP addresses. Internal traffic should also be restricted to reduce lateral movement opportunities within the internal networks. Internet access should be restricted and where possible, the use of cloud private ‘backbone’ endpoints should be used to connect services to cloud APIs without the need for public internet access. Managed services should also be reviewed to ensure endpoints are not publicly exposed

CONTROL	DESCRIPTION	RECOMMENDATIONS
Encryption	Cloud platforms provide native encryption services to secure data in-transit and at-rest. Commonly this is achieved via a Key Management Solution (KMS) which can be used to implement Platform Managed Keys (PMK) and Customer Managed Keys (CMK) wherein the cloud provider will automatically handle the encryption and decryption of data as required.	Efforts should be made to ensure all data is secured in transit and at rest with TLS, block and or file level encryption and trusted certificates. Although PMKS reduces the operational overhead of maintaining key policies, CMK allows administrators to decouple access to encryption keys from the data they protect. This can add an additional layer of protection for sensitive resources and should be used wherever practical. Where organisations must meet strict regulatory compliance standards, cloud Hardware Security Modules (HSM) options are available to provide dedicated devices for managing encryption keys
Monitor Suspicious Activities	Cloud providers offer several services that can be used to provide threat detection to monitor and analyze events within the platform to identify suspicious activity.	Native or third-party security solutions should be implemented to monitor for high-risk security events and suspicious activities that may indicate an account compromise
Source Code and Configuration Management	Use of the cloud enables resources to be managed and deployed programmatically and at scale, deployment and build artifacts like secrets, passwords and API keys that are stored in source code and configuration files can often get exposed inadvertently resulting in sensitive data exposure and or complete account compromise.	Source code should be subject to access control and only provided to developers and administrators that require it to perform their day-to-day tasks. Secrets should not be stored in configuration files but securely injected into the deployment process by using a native secrets management solution that will encrypt and protect secret data from unauthorized access. Do not hard code access keys, role-based access control should be used instead, roles, including cross account roles, can then be assumed when access is required and provide an additional boundary of protection against unauthorized account access.

9 APPENDIX D: VULNERABILITY RATINGS

9.1 Vulnerability Impact

Each listed vulnerability is assigned an "Impact" rating of "**High**", "**Medium**" or "**Low**". Impact is calculated by considering the potential Business Impact if the vulnerability was exploited by a malicious attacker.

EVALUATION	QUALIFYING FACTORS
High	Successful exploitation could lead to highly privileged access to the target host or data. Exploitation could lead to a Denial-of-Service condition of a critical host or service.
Medium	Exploitation of the vulnerability will not directly lead to privileged access to the host, service or data. However, vulnerabilities with a medium impact can often be combined with other flaws to elevate their impact.
Low	This impact rating is assigned to vulnerabilities that, when exploited in isolation, have a negligible impact on security. Typically, vulnerabilities that disclose information that may be useful to the attacker are considered to have a low impact.

9.2 Exploitation Probability

Each listed vulnerability is assigned a "Probability" rating based on how likely the vulnerability is to be exploited. Probability is determined by considering several factors including:

- How difficult vulnerability is to exploit.
- If the vulnerability can be exploited automatically.
- If the vulnerability is or is likely to be exploited by an internet worm or botnet.
- What the attacker would achieve by exploiting the flaw.
- Probability ratings are applied subjectively whilst considering the profile of the organization and who is likely to target the assessed resource.

The following table lists each probability evaluation rating along with a list of qualifying factors. One or more of the listed qualifying factors may be considered in each case.

Each vulnerability is evaluated on a case-by-case basis and therefore other factors that are not listed below may also be considered.

EVALUATION	QUALIFYING FACTORS
High	The vulnerability can be exploited using exploit code freely available on the internet. The vulnerability could be targeted automatically by an Internet worm or Botnet. The vulnerability could be exploited by an unskilled intruder.
Medium	To exploit the vulnerability the attacker would need to have a working knowledge of how the vulnerability operates. Some customizations to the exploit or exploit procedure are required. The attacker is required to perform a degree of social engineering to exploit the flaw and/or user interaction is required.
Low	To exploit the vulnerability the attacker would need to write custom exploit code. The vulnerability cannot be exploited reliably and/or requires in-depth knowledge of the target systems configuration. Other prerequisites must exist before the exploitation is possible and during the period of the assessment, those prerequisites were not met.

9.3 Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment.

The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

The company assigns a CVSS Base score, and where necessary a CVSS Temporal score, to each vulnerability where appropriate or required by various compliance standards. Vulnerabilities are often considered to have the following severity based on this scoring system:

- "High" severity if they have a CVSS base score of 7.0 -10.0.
- "Medium" severity if they have a base CVSS score of 4.0-6.9.
- "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that unless explicitly required to do so, the Company's impact metric does not necessarily align with the severity implied by the CVSS score.