



# Azure CIS Controls Assessment

**For:**

**DataMatrix Medical**



**Date:**

December 11, 2024

**Document Version:** 4.0

The following scale was used to measure the audit results:

- **Satisfactory (S)** – The organization meets audit requirements with only a limited number of medium and low risk areas needing to be addressed. Appropriate controls are in place and operating effectively.
- **Satisfactory with Minor Improvements needed (SMI)** – The organization meets most requirements with a limited number of high and a low number of medium priority areas needing to be addressed. Appropriate controls are in place and operating effectively, posing only a low level of risk overall in this area.
- **Needs Improvement (NI)** – The organization does not meet several audit requirements. A significant number of controls are missing or not operating effectively, posing a high or medium level of risk overall in this area.
- **Weak (W)** – The organization does not meet most audit requirements with multiple controls not operating effectively, posing an unacceptable level of risk.

Overall, the rating of the organization around AWS CIS controls is **Satisfactory (S)**. Compass found that the organization meets audit requirements. Appropriate controls are in place and operating effectively.

# DataMatrix Medical

## Summary

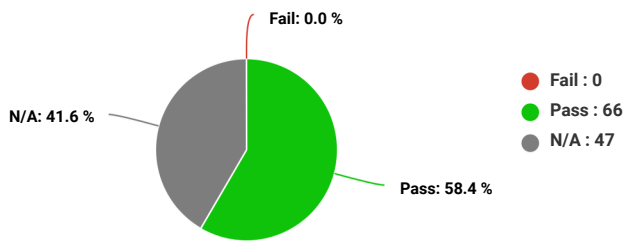
### Total Evaluations



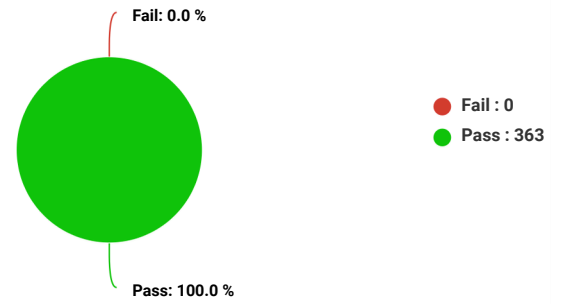
### Failures By Criticality

High	0
Medium	0
Low	0

### Policy Compliance By Controls



### Policy Compliance By Evaluations



# Control Summary

CID	Control	Criticality	Resources			Control Result
			Passed	Failed	With Exception	
50001	Ensure that Data encryption is set to ON for a SQL database '4.1.5'	HIGH	0	0	0	N/A
50002	Ensure no SQL Servers allow ingress from Internet (ANY IP) '4.1.2'	HIGH	0	0	0	N/A
50004	Ensure that Auto provisioning of Log Analytics agent for Azure VMs is set to On '2.1.14'	HIGH	0	0	1	PASS
50005	Ensure that Microsoft Defender Recommendation for Apply system updates status is Completed '2.1.12'	HIGH	1	0	0	PASS
50008	Ensure that Disk encryption should be applied on virtual machines is set to On '7.7'	HIGH	1	0	0	PASS
50011	Ensure that Secure transfer required is set to Enabled '3.1'	HIGH	1	0	0	PASS
50015	Ensure that Microsoft Defender for Servers is set to On '2.1.1'	HIGH	1	0	0	PASS
50016	Ensure that Access through Internet facing endpoint should be restricted is set to On '6.4'	HIGH	1	0	0	PASS
50020	Ensure Additional email addresses is configured with a security contact email '2.1.18'	HIGH	0	0	1	PASS
50022	Ensure that Notify about alerts with the following severity is set to High '2.1.19'	HIGH	1	0	0	PASS
50023	Ensure that All users with the following roles is set to Owner '2.1.17'	HIGH	1	0	0	PASS
50026	Ensure keyvault is recoverable '8.5'	HIGH	1	0	0	PASS
50027	Ensure SQL server Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key '4.1.3'	HIGH	0	0	0	N/A
50029	Disable RDP access on Network Security Groups from Internet (ANY IP) '6.1'	HIGH	11	0	0	PASS
50030	Ensure that the Expiration Date is set for all Secrets in Non RBAC Key Vaults '8.4'	HIGH	0	0	0	N/A
50031	Disable SSH access on Network Security Groups from Internet (ANY IP) '6.2'	HIGH	11	0	0	PASS
50032	Ensure that Unattached disks are encrypted with Customer Managed Key (CMK) '7.4'	HIGH	1	0	0	PASS
50035	Ensure that Microsoft Entra authentication is configured for SQL Servers '4.1.4'	HIGH	0	0	0	N/A
50036	Ensure that Resource Locks are set for Mission-Critical Azure Resources '10.1'	MEDIUM	0	0	8	PASS
50039	Ensure Enforce SSL connection is set to ENABLED for MySQL Database Server '4.4.1'	HIGH	0	0	0	N/A
50040	Ensure Enforce SSL connection is set to ENABLED for PostgreSQL Database Server '4.3.1'	HIGH	0	0	0	N/A
50041	Ensure server parameter log_checkpoints is set to ON for PostgreSQL Database Server '4.3.2'	LOW	0	0	0	N/A
50042	Ensure server parameter log_connections is set to ON for PostgreSQL Database Server '4.3.3'	HIGH	0	0	0	N/A

CID	Control	Criticality	Resources			Control Result
			Passed	Failed	With Exception	
50043	Ensure server parameter log_disconnections is set to ON for PostgreSQL Database Server '4.3.4'	MEDIUM	0	0	0	N/A
50045	Ensure server parameter log_retention_days is greater than 3 days for PostgreSQL Database Server '4.3.6'	MEDIUM	0	0	0	N/A
50047	Ensure App Service Authentication is set up for apps in Azure App Service '9.1'	HIGH	0	0	0	N/A
50048	Ensure Web app redirects all HTTP traffic to HTTPS '9.2'	HIGH	0	0	0	N/A
50050	Ensure that Register with Entra ID is enabled on App Service '9.4'	MEDIUM	0	0	0	N/A
50051	Ensure Web app is using the latest version of TLS encryption version '9.3'	HIGH	0	0	0	N/A
50052	Ensure default network access rule for Storage Accounts is set to deny '3.8'	HIGH	1	0	0	PASS
50053	Ensure Allow Azure services on the trusted services list to access this storage account is Enabled for Storage Account Access '3.9'	MEDIUM	1	0	0	PASS
50055	Ensure Network Security Group Flow Log retention is greater than 90 days '6.5'	MEDIUM	0	0	0	N/A
50056	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key '5.1.3'	HIGH	0	0	0	N/A
50059	Ensure Activity Log Alert exists for Delete SQL server firewall rule '5.2.8'	LOW	0	0	1	PASS
50061	Ensure that HTTP Version used for web app is latest '9.8'	LOW	0	0	0	N/A
50062	Ensure Network Watcher is Enabled for your Subscription '6.6'	MEDIUM	0	0	1	PASS
50063	Ensure Activity Log Alert exists for Create Policy Assignment '5.2.1'	LOW	0	0	1	PASS
50064	Ensure Activity Log Alert exists for Create or Update Network Security Group '5.2.3'	LOW	1	0	0	PASS
50065	Ensure Activity Log Alert exists for Delete Network Security Group '5.2.4'	LOW	1	0	0	PASS
50068	Ensure Activity Log Alert exists for Create or Update Security Solution '5.2.5'	LOW	0	0	1	PASS
50069	Ensure Activity Log Alert exists for Delete Security Solution '5.2.6'	LOW	0	0	1	PASS
50070	Ensure Activity Log Alert exists for Create or Update SQL Server Firewall Rule '5.2.7'	LOW	0	0	1	PASS
50072	Ensure guest users are reviewed on a monthly basis '1.4'	HIGH	0	0	0	N/A
50073	Ensure that no custom subscription Administrator Roles exist '1.22'	HIGH	0	0	0	N/A
50074	Ensure server parameter connection_throttling is set to ON for PostgreSQL Database Server '4.3.5'	HIGH	0	0	0	N/A
50075	Ensure that diagnostic settings for Azure KeyVault is set to ON '5.1.4'	HIGH	1	0	0	PASS

CID	Control	Criticality	Resources			Control Result
			Passed	Failed	With Exception	
50077	Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected '2.1.20'	LOW	1	0	0	PASS
50078	Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected '2.1.21'	LOW	1	0	0	PASS
50079	Ensure that Microsoft Defender for Azure SQL Databases is set to On '2.1.3'	HIGH	0	0	1	PASS
50080	Ensure that Microsoft Defender for App Services is set to On '2.1.2'	HIGH	0	0	1	PASS
50081	Ensure that Microsoft Defender for Storage is set to On '2.1.7'	HIGH	1	0	0	PASS
50099	Ensure that Azure Cosmos DB accounts Firewalls and Networks is limited to use Selected Networks instead of All Networks '4.5.1'	HIGH	0	0	0	N/A
50117	Ensure Allow access to Azure services for PostgreSQL Database Server is disabled '4.3.7'	HIGH	0	0	0	N/A
50130	Ensure that the endpoint protection for all Virtual Machines is installed '7.6'	MEDIUM	0	0	51	PASS
50133	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage '3.11'	HIGH	0	0	0	N/A
50134	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys '3.12'	HIGH	1	0	0	PASS
50135	Ensure Activity Log Alert exists for Delete Policy Assignment '5.2.2'	LOW	1	0	0	PASS
50136	Ensure FTP deployments are disabled for web apps '9.9'	HIGH	0	0	0	N/A
50137	Ensure that OS and Data disks are encrypted with Customer Managed Key '7.3'	HIGH	52	0	0	PASS
50138	Ensure that UDP Services are restricted from the Internet '6.3'	HIGH	11	0	0	PASS
50140	[LEGACY] Ensure that Microsoft Defender is set to On for Container Registries '2.1.8'	HIGH	0	0	1	PASS
50141	Ensure that Microsoft Defender for Key Vault is set to On '2.1.9'	HIGH	1	0	0	PASS
50142	Ensure Diagnostic Setting captures appropriate categories '5.1.2'	HIGH	1	0	0	PASS
50172	Ensure that Microsoft Defender for Open-Source Relational Databases is set to On '2.1.5'	HIGH	0	0	1	PASS
50175	Ensure that Storage Accounts have infrastructure encryption enabled '3.2'	HIGH	1	0	0	PASS
50176	Ensure that Azure Key Vaults use Private Links '8.7'	MEDIUM	1	0	0	PASS
50181	Ensure Storage Accounts are using the latest version of TLS encryption '3.15'	HIGH	1	0	0	PASS
50197	[LEGACY] Ensure that Microsoft Defender for DNS is set to On '2.1.10'	HIGH	0	0	1	PASS
50215	Ensure Storage logging is enabled for Queue service for read, write and delete requests '3.5'	MEDIUM	0	0	0	N/A
50218	Ensure that the expiry date is set on all keys from RBAC key Vault '8.1'	HIGH	2	0	0	PASS

CID	Control	Criticality	Resources			Control Result
			Passed	Failed	With Exception	
50226	Ensure that Microsoft Defender for Resource Manager is set to On '2.1.11'	HIGH	1	0	0	PASS
50231	Ensure that Microsoft Defender for SQL Servers on Machines is set to On '2.1.4'	MEDIUM	0	0	1	PASS
50233	Ensure that PHP version is the latest, if used to run the web app '9.5'	LOW	0	0	0	N/A
50234	Ensure that Python version is the latest, if used to run the web app '9.6'	LOW	0	0	0	N/A
50235	Ensure that Java version is the latest, if used to run the web app '9.7'	LOW	0	0	0	N/A
50237	Ensure that Auditing Retention is greater than 90 days for Azure MSSQL Server '4.1.6'	MEDIUM	0	0	0	N/A
50240	Ensure Infrastructure double encryption for PostgreSQL Database Server is Enabled '4.3.8'	HIGH	0	0	0	N/A
50256	Ensure that Network Interfaces dont use public IPs '6.7'	MEDIUM	56	0	0	PASS
50313	Ensure that Azure Storage Accounts are configured with private endpoints '3.10'	HIGH	1	0	0	PASS
50314	Ensure Trusted Launch is enabled on Virtual Machines '7.9'	HIGH	51	0	0	PASS
50327	Ensure that SKU of the load balancer is not Basic '5.5'	HIGH	1	0	0	PASS
50335	Ensure TLS Version is set to TLSV1.2 for MySQL flexible Database Server '4.4.2'	HIGH	0	0	0	N/A
50336	Ensure that Storage Account Access Keys are Periodically Regenerated '3.4'	HIGH	1	0	0	PASS
50343	Ensure that Auditing is Enabled for Azure SQL Server '4.1.1'	MEDIUM	0	0	0	N/A
50360	Ensure that Microsoft Defender for Azure Cosmos DB is set to On '2.1.6'	HIGH	0	0	1	PASS
50363	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics '5.1.5'	MEDIUM	0	0	0	N/A
50436	Ensure that Activity Log Alert exists for Delete Public IP Address Rule '5.2.10'	LOW	1	0	0	PASS
50437	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule '5.2.9'	HIGH	1	0	0	PASS
50438	Ensure Virtual Machines are utilizing Managed Disks '7.2'	HIGH	51	0	0	PASS
50439	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults '8.3'	HIGH	0	0	0	N/A
50440	Ensure that private endpoints are configured for Cosmos DB '4.5.2'	HIGH	0	0	0	N/A
50441	Enable Role Based Access Control for Azure Key Vault '8.6'	HIGH	1	0	0	PASS
50442	Ensure that the expiry date is set on all keys from Non RBAC Key Vault '8.2'	HIGH	0	0	0	N/A

CID	Control	Criticality	Resources			Control Result
			Passed	Failed	With Exception	
50443	Ensure that Enable key rotation reminders is enabled for each Storage Account '3.3'	MEDIUM	1	0	0	PASS
50444	Ensure that logging for Azure Web AppService AppServiceHTTPLogs is enabled '5.1.6'	MEDIUM	0	0	0	N/A
50445	Ensure server parameter audit_log_enabled is set to ON for MySQL Database Server '4.4.3'	MEDIUM	0	0	0	N/A
50446	Ensure server parameter audit_log_events has CONNECTION set for MySQL Database Server '4.4.4'	MEDIUM	0	0	0	N/A
50447	Ensure server parameter audit_log_enabled is set to ON for MySQL Flexible Database Server '4.4.3'	MEDIUM	0	0	0	N/A
50448	Ensure server parameter audit_log_events has CONNECTION set for MySQL flexible Database Server '4.4.4'	MEDIUM	0	0	0	N/A
50449	Ensure that logging for Azure Api AppService AppServiceHTTPLogs is enabled '5.1.6'	MEDIUM	0	0	0	N/A
50450	Ensure Application insights are configured '5.3.1'	MEDIUM	0	0	1	PASS
50451	Ensure an Azure Bastion Host Exists '7.1'	HIGH	0	0	1	PASS
50452	Ensure Public IP Addresses are not using Basic SKU '5.5'	HIGH	4	0	0	PASS
50453	Ensure that SKU Basic/Consumption is not used by SQL PaaS Databases '5.5'	MEDIUM	0	0	0	N/A
50454	Ensure that SKU Basic/Consumption is not used by Redis Cache '5.5'	MEDIUM	0	0	0	N/A
50455	Ensure Storage logging is enabled for Blob service for read, write and delete requests '3.13'	MEDIUM	0	0	0	N/A
50456	Ensure Storage logging is enabled for Table service for read, write and delete requests '3.14'	MEDIUM	0	0	0	N/A
50458	Ensure that cross-tenant replication is set to disabled '3.16'	HIGH	1	0	0	PASS
50460	Ensure that Microsoft Defender is set to On for Containers '2.1.8'	HIGH	0	0	1	PASS
50461	Ensure that Public Network Access is Disabled for storage accounts '3.7'	HIGH	1	0	0	PASS
50462	Ensure that Allow Blob Anonymous Access is set to Disabled '3.17'	HIGH	1	0	0	PASS
50470	Ensure that Private Endpoints are Used for Azure Key Vault '8.7'	HIGH	1	0	0	PASS
50471	Ensure Private Endpoints are used to access Storage Accounts '3.10'	HIGH	1	0	0	PASS