ESTĒE LAUDER COMPANIES

ELC (Estée Lauder Companies) Cloud Security Policy Standards & Control V2.1

Standard Title	Cloud Security Policy Standard & Control Document	**Date**	09th Oct'23
Standard Owner	Abedi Jamshid Kulbhushan Sharma	**Effective Date**	16th Feb'24
Process	Information Technology Global Information Risk & Security	**Next Revision Date**	16th Feb'25
Approved by	Abedi Jamshid Kulbhushan Sharma	**Role**	Executive Director's, Information Technology Global Information Risk & Security

Version	Date	Name	Reviewed By	Approved By	Comments
ELC-035_2022.1.0	03rd Apr'22	Bhavin Soni	Kulbhushan Sharma	Kulbhushan Sharma	V1.0
ELC-035-2024.2.0	16th Feb'24	Cloud Security Team	Kannan Kuppusamy Felix Jebamani Abedi Jamshid	Abedi Jamshid Kulbhushan Sharma	V2.0
ELC-035-2024.2.0	12th March'24	Cloud Security Team	Giura, Razvan	Abedi Jamshid Kulbhushan Sharma	V2.0
ELC-035-2024.2.0	26th April'24	Cloud Security Team	Abedi Jamshid	Abedi Jamshid Kulbhushan Sharma	V2.0
ELC-035-2024.2.0	Nov 8th 24	Cloud Security Team	Omar Salama	Omar Salama	V 2.1

Table Content

ESTĒE LAUDER COMPANIES

1.0 Policy Statement

In accordance with the ELC Global Information Risk & Security, Cloud Security Standard and Control Document highlights the native cloud security policies and controls that Estee Lauder Companies, Inc. (ELC) should maintain and uphold within its Azure environment.

2.0 Purpose and Scope

The purpose of this standard is to document the native Cloud security Control standards in accordance with the Microsoft cloud security Benchmarks to ensure ELC Azure resources are protected from misconfigurations, data breaches, lack of visibility, and exposure to the public. This standard serves as a general security guideline for expectations and industry best practices.

This standard applies to Estee Lauder Companies Inc. (the "Company") and its subsidiaries throughout the world (collectively, with the Company, "ELC"). The requirements presented herein must be applied to all systems that support financial reporting or financial data.

3.0 Standards

The following standards align with the Microsoft Cloud Security Benchmarks and are expected to be maintained and upheld by the ELC native cloud environment.

- Microsoft Security Benchmark V1.0 2023
- NIST SP 800-53 r4
- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
- ISO/IEC 27001:2022: Information Security Controls
- ISO/IEC 27002:2022 Information Security Standard.
- Azure Security Policy standard control document v2.1.0
- CIS Controls v7.1, CIS Controls V8
- PCI-DSS v3.2.1

4.0 Networking

The Networking section defines the security control and standards for maintaining the security of ELC Information Technology networks to protect them from unauthorized access, restricting the vulnerable ports and internet exposed services, permitting the approved ports. The following industry good-practice frameworks, standards and guidelines were referenced from the standard section documents.

Section 3.2 of Azure Security Policies defines NSG native control under "**ELC Azure Security Policy Standards & Control Document** of Azure Security Benchmark v2.1.0."

4.0.1 Subnets should be associated with a Network Security Group

Control ID	ELC-CS-NS-001
Severity	High
Enforcement	Recommended
Control Definition	All the ELC Subnets Should be associated with an NSG
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Controls v7.1 ID(s) - 14.1, NIST SP800-53 r4 ID(s) - Sec-7, PCI-DSS v3.2.1 ID(s) - 1.1, 1.2, 1.3, ELC-AZS-NS-3.2.2 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf

4.0.2 All network ports should be restricted to network security groups linked with ELC Virtual Machines.

Control ID	ELC-CS-NS-002
Severity	High
Enforcement	Recommended
Control Definition	For Network Ports, NSG's will control which specific ports are accessible to the Virtual Machines, Blocking everything except for necessary services.
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-3, CIS Controls V7.1 (ID'S) - 12.4, CIS Controls V8 (ID'S) - 4.4, NIST SP800-53 r4 ID's - SC-7, PCI-DSS V3.2.1 - 1.1, 1.2, 1.3, ELC-AZS-NS-3.2.3 - Azure Security Policy Standard Document
Recommendation & Procedure	Deploy a security system to perform advanced filtering on network traffic to and from external networks. Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf

4.0.3 All Internet exposed services (IaaS/PaaS) must be restricted and be configured with a default-deny policy.

Control ID	ELC-CS-NS-003
Severity	High
Enforcement	Required
Control Definition	Internet facing services must be restricted via a default deny policy to block all incoming traffic except for explicitly allowed connections. Minimizing potential outside threats.
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Controls v7.1 ID(s) - 12.3, NIST SP800-53 r4 ID(s) - AC-4, PCI-DSS v3.2.1 ID(s) - 1.1, 1.2, 1.3, ELC-AZS-NS-3.2.5 - Azure Security Policy Standard Document

Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf

4.0.4 Web Application Firewall (WAF) should be deployed for all external published web services.

Control ID	ELC-CS-NS-004
Severity	Medium
Enforcement	Recommended
Control Definition	Web Application Firewall should be deployed for all external published web services; Cequence should be used by default for the ELC environment. Additionally Azure WAF/ App Gateway can be used with a security exception
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-6, CIS Controls v7.1 ID(s) - 12.9, NIST SP800-53 r4 ID(s) - Sec-7, PCI-DSS v3.2.1 ID(s) - 1.1, 1.2, 1.3, ELC-AZS-NS-3.2.6 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf

4.0.5 Enable Network Watcher

Control ID	ELC-CS-NS-005
Severity	Low
Enforcement	Recommended
Control Definition	Network Watcher is a regional service that enables you to monitor and diagnose network conditions all throughout Azure. If a compatible resource is enabled and functions like Network Watcher, then this recommendation is met.
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-1, NS-3, CIS Controls V7.1 (ID'S) - 14.2, CIS Controls V8 (ID'S) - 13.12, NIST SP800-53 r4 (ID'S) - SC-2, PCI-DSS V3.2.1 - 1.1,1.2, 1.3,

	ELC-AZS-NS-3.2.7 - Azure Security Policy Standard Document
Recommendation & Procedure	For specific, well-defined applications (such as a 3-tier app), this can be a highly secure "deny by default, permit by exception" approach by restricting the ports, protocols, source, and destination IPs of the network traffic. Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf

4.0.6 Enforce least privilege access policies between network segments.

Control ID	ELC-CS-NS-006
Severity	High
Enforcement	Required
Control Definition	To restrict traffic between network segments in the ELC environment, enforcing least privilege by using NSG, ASG, and NVA policies to allow only necessary communication paths.
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Control v7.1 (ID'S) - 9.4, CIS Control V8 (ID'S) - 13.4, NIST SP800-53 r4 (ID'S) - AC-4 PCI-DSS V3.2.1 - 1.1, 1.2, 1.3
Recommendation & Procedure	To enhance your enterprise segmentation strategy, restrict or monitor traffic between internal resources using network controls. Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf

4.0.7 All Internet Proposed Published Services must undergo an Architecture Assessment

Control ID	ELC-CS-NS-007
Severity	High
Enforcement	Required

Control Definition	Only approved services are allowed. Additionally, each approved service must go through a security focused architecture assessment. (Assessment between cloudsec and engineering)
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Control v7.1 (ID'S) - 9.4, CIS Control V8 (ID'S) - 13.4, NIST SP800-53 r4 (ID'S) - AC-4, PCI-DSS V3.2.1 - 1.1, 1.2, 1.3
Recommendation & Procedure	To enhance your enterprise segmentation strategy, restrict or monitor traffic between internal resources using network controls. Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf
Severity	High

4.0.8 NVA bypass subnets should apply ASG's to restrict inbound access.

Control ID	ELC-CS-NS-008
Severity	High
Enforcement	Recommended
Control Definition	Application Security Groups to be applied on NVA bypass subnets to restrict any inbound access. Only authorized traffic should be permitted.
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Controls V7.1 (ID'S) - 9.4, CIS Controls V8 (ID'S) - 13.4, NIST SP800-53 r4 (ID'S) - SC-2, PCI-DSS V3.2.1 - 1.1,1.2, 1.3.
Recommendation & Procedure	To enhance your enterprise segmentation strategy, restrict or monitor traffic between internal resources using network controls. Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf

4.0.9 Restrict all NVA Routed communication by using least privilege network access Policies.

Control ID	ELC-CS-NS-009
Severity	High
Enforcement	Required
Control Definition	Restrict all NVA Routed communication via least privilege network access policies. Enforce this by leveraging NVA/ Palo Alto Network Firewalls.
Control Domain	Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Controls V7.1 (ID'S) - 14.2, CIS Controls V8 (ID'S) - 4.4, NIST SP800-53 r4 (ID'S) - SC-7, PCI-DSS V3.2.1 - 1.1,1.2, 1.3
Recommendation & Procedure	To enhance your enterprise segmentation strategy, restrict or monitor traffic between internal resources using network controls. Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure Network_Security_Group_Reference_Document_V1.0.pdf

5.0 Storage

The storage section defines the security control and standards for maintaining the security of ELC Information Technology to protect them from unauthorized access, modification, disclosure, and encrypt sensitive information at rest. The following industry good-practice frameworks, standards and guidelines were referenced from the standard section documents.

Section 3.4 of Azure Security Policies defines **Azure Storage** native control under "**ELC Azure Security Policy Standards & Control Document of Azure Security Benchmark v2.1.0."**

5.0.1 Encrypt Sensitive Information at Rest and in transit

Sensitive data is data that requires protection due to the impact it has if accessed without authorized access. Compromising sensitive data would mean potential security breaches, non-compliance regulations and negative business implications including reputational damage and/or unwanted exposure of intellectual property.

Control ID	ELC-CS-SA-001
Severity	High
Enforcement	Required
Control Definition	Encrypt sensitive data at rest and in transit according to the elc-ecr-013-data-encryption-procedure
Control Domain	MCSB – DP-4 CIS Controls V7.1 (ID'S) – 14.8 CIS Controls V8 (ID'S) – 3.11, NISR SP800-53 r4 (ID'S) – SC-28, PCI-DSS V3.2.1 – 3.4,3.5
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, (6.1 Reference Links attached file 3.1) ELC_Cloud_Security_Azure_Storage_Reference_Document_V1.0.pdf and follow the ELC data encryption procedure document ELC-ECR-013 Data Encryption Procedure (elcompanies.com)

5.0.2 Configure all storage accounts with either service endpoints or private endpoints.

Control ID	ELC-CS-SA-002
Severity	High
Enforcement	Recommended
Control Definition	Private endpoints connect your virtual network to Azure services without a public IP address, limiting the risk of a data leakage. Therefore, it is best practice to configure private endpoints for storage accounts. If a storage account has high data volume, then service endpoints are a viable alternative.
Control Domain	ASB V2 NS-2, NS-3 Microsoft cloud security benchmark NS-2 CIS 3.10
Recommendation & Procedure	Configuring a **private link connection** for an **Azure Storage account** involves creating an **Azure Private Endpoint**. This allows you to securely access your storage account privately within your virtual network. Use Azure Private Link to enable private access to Azure services from your virtual networks, without crossing the internet.

	In situations where Azure Private Link is not yet available, use Azure Virtual Network service endpoints. Azure Virtual Network service endpoints provide secure access to services via an optimized route over the Azure backbone network. Private access is an additional defense in depth measure in addition to authentication and traffic security offered by Azure services. Please refer to the Best Practice Document to proceed further, (for service endpoint 7.1, Private Endpoint 7.2 Reference Links) ELC_Cloud_Security_Azure_Storage_Reference_Document_V1.0.pdf

5.0.3 Encrypt Data at rest by leveraging customer managed Keys.

Control ID	ELC-CS-SA-003
Severity	High
Enforcement	Recommended
Control Definition	Secure your blob and file storage accounts with increased flexibility through customer-managed keys. The key is used to protect and control access to keys for data encryption. Customer-managed keys provide added control over key rotation and cryptographic data erasure.
Control Domain	CIS 1.4.0 – 3.9 Azure Security Benchmark V3 DP-5 CIS Controls v7.1 ID(s) – 14.8 CIS Controls v8 ID(s) – 3.11 NIST SP800-53 r4 ID(s) - SC-12, SC-28 PCI-DSS v3.2.1 ID(s) – 3.4. 3.5 3.6
Recommendation & Procedure	Customer-managed keys offer greater flexibility to manage access controls. Please refer to the Best Practice Document to proceed further, (5.1) ELC_Cloud_Security_Azure_Storage_Reference_Document_V1.0.pdf

5.0.4 Require Custom Sensitivity tags for storage Account resources.

Control ID	ELC-CS-SA-004
Sensitivity	High
Enforcement	Required
Control Definition	Sensitive tags are used to organize Azure storage accounts

	providing more granular data classification and application of required Azure policies. Sensitivity tags can create layered encryption at rest and increase the use of customer managed keys for further stronger data security.
Control Domain	Custom recommendation for a better security.
Recommendation & Procedure	Improving the application owner's experience with the better security for Storage account. Please refer to the Best Practice Document to proceed further, (3.0) ELC_Cloud_Security_Azure_Storage_Reference_Document_V1.0.pdf

5.0.5 Storage accounts that are used to host sensitive data should leverage layered encryption.

Control ID	ELC-CS-SA-005
Severity	High
Enforcement	Recommended
Control Definition	Layered encryption of Azure storage data protects provides independent encryption at multiple points. Therefore, reinforcing data confidentiality and applying stringent security standards.
Control Domain	NIST SP 800-53 Rev. 5 – SC-12 FedRAMP_Moderate_R4 – SC-12
Recommendation & Procedure	Customers who require higher levels of assurance that their data is secure can also enable 256-bit AES encryption at the Azure Storage infrastructure level for double encryption. Please refer to the Best Practice Document to proceed further, (5.0) ELC_Cloud_Security_Azure_Storage_Reference_Document_V1.0.pdf

5.0.6 Enable secure web transfer using TLS 1.2 or higher.

Control ID	ELC-CS-SA-006
Severity	High
Enforcement	Required
Control Definition	Configure a minimum TLS version for secure communication between the client application and the storage account. To minimize security risk, the recommended minimum TLS version is TLS 1.2.
Control Domain	CIS Microsoft Azure Foundations Benchmark 1.4.0 - 3.1 Microsoft Cloud security benchmark - DP-3 NIST SP 800-171 R2 - 3.13.8 NIST SP 800-53 Rev. 4 - SC-8, SC-8(1) NIST SP 800-53 Rev. 5 - SC-8, SC-8(1)
Recommendation & Procedure	Azure Storage currently supports three versions of the TLS protocol: 1.0, 1.1, and 1.2. Azure Storage uses TLS 1.2 on public HTTPS endpoints, but TLS 1.0 and TLS 1.1 are still supported for backward compatibility. Please refer to the Best Practice Document to proceed further, (6.1 Reference Links) ELC_Cloud_Security_Azure_Storage_Reference_Document_V1.0.pdf

5.0.7 All storage accounts should deny internet access by default; access should only be allowed through approved and documented exceptions.

Control ID	ELC-CS-SA-007
Severity	High
Enforcement	Required
Control Definition	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted through approved and documented exceptions
Control Domain	CIS Microsoft Azure Foundations Benchmark 1.3.0 - 3.6 CIS Microsoft Azure Foundations Benchmark 1.4.0 - 3.6

	CIS Microsoft Azure Foundations Benchmark 2.0.0 - 3.8 FedRAMP High - AC-4, SC-7, SC-7(3) FedRAMP Moderate - AC-4, SC-7, SC-7(3) Microsoft Cloud security benchmark - NS-2 NIST SP 800-171 R2 - 3.1.3, 3.13.1, 3.13.2, 3.13.6 NIST SP 800-53 Rev. 4 - AC-4 SC-28, SC-28(1) NIST SP 800-53 Rev. 5 - AC-4 SC-28, SC-28(1)
Recommendation & Procedure	Ensure default network access rule for Storage Accounts is set to deny. Please refer to the Best Practice Document to proceed further, (1.0) ELC_Cloud_Security_Azure_Storage_Reference_Document_V1.0.pdf

6.0 Virtual Machine

The Virtual Machine section defines the security control and standards for maintaining the security of ELC Information Technology to protect them from unauthorized access, secure the VM's with the below mentioned controls from internal and external attack factors. The following industry good-practice frameworks, standards and guidelines were referenced from the standard section documents.

Section 3.6 of Azure Security defines the Azure Virtual Machine native control under "ELC Azure Security Policy Standards & Control Document of Azure Security Benchmark v2.1.0."

6.0.1 Encrypt all data in transit.

Control ID	ELC-CS-VM-001
Severity	High
Enforcement	Required
Control Definition	All data in transit must be encrypted to ensure integrity. Using RDP and SSH are the right management protocol tools that we should use limiting our attack surface.

Control Domain	Microsoft Cloud Security Benchmark V1.0 – DP-3 CIS Controls V7.1 (ID'S) – 14.4 CIS Controls V8 (ID'S) – 3.10, NIST SP800-53 r4 (ID'S) – SC-8, PCI-DSS V3.2.1 – 3.5,3.6,4.1
Recommendation & Procedure	Please refer to the Data Encryption procedure document to proceed further: https://myelc.elcompanies.com/sites/global-it-community/document/250058/ELC-ECR-013-Data-Encryption-Procedure ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.2 Leverage sanctioned managed hosts to perform operational/ privileged functions.

Control ID	ELC-CS-VM-002
Severity	High
Enforcement	Required
Control Definition	Managed hosts, specifically Jump servers are isolated workstations that enhance the security of key roles like admin, developer and more.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PA-6 CIS Controls v7.1 ID(s) – 4.6,11.6,12.12, CIS Controls V8 (ID'S) – 12.8,13.5 NIST SP800-53 r4 ID(s) – AC-2, SC-7, SC-2 PCI-DSS v3.2.1 ID(s) - 1.2, 6.4
Recommendation & Procedure	Use Privileged Access Workstations for Administrative tasks. ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.3 Deny private link connections to external third parties by default.

Control ID	ELC-CS-VM-003
Severity	High
Enforcement	Required
Control Definition	Denying private link connections to external third-party networks prevents unauthorized access and maintains heightened network security. Exceptions need to be approved and documented where applicable.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – NS-2 CIS Controls v7.1 ID(s) – 14.1 CIS Controls V8 (ID'S) – 3.12,4.4, NIST SP800-53 r4 ID(s) – AC-4, SC-7, SC-2 PCI-DSS v3.2.1 ID(s) - 1.1,1.2, 1.3
Recommendation & Procedure	Secure cloud native services with network controls ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.4 Enable backups for Virtual Machines.

Control ID	ELC-CS-VM-004
Severity	High
Enforcement	Recommended
Control Definition	Enabling backups for your Virtual Machines provides a secure and cost-effective data loss prevention solution.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – BR-1 CIS Controls v7.1 ID(s) – 10.1 CIS Controls V8 (ID'S) – 11.2 NIST SP800-53 r4 ID(s) – CP-2, CP-4, CP-9 PCI-DSS v3.2.1 ID(s) – 3.4 ELC-AZS-VM-3.6.4 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.5 All privileged access for local & domain accounts should be routed through the ELC sanctioned privileged access management solution.

Control ID	ELC-CS-VM-005
Severity	High
Enforcement	Recommended
Control Definition	This is to reduce unauthorized access, allows monitoring and controlling over privileged actions to enhance security and does so with proper documented approvals.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – IM-6 CIS Controls v7.1 ID(s) – 4.2,4.5,12.11,16.3 CIS Controls V8 (ID'S) – 6.3,6.4 NIST SP800-53 r4 ID(s) – AC-2, AC-3, IA-2, IA-5, IA-8 PCI-DSS v3.2.1 ID(s) – 7.2,8.2,8.3,8.4 **ELC-AZS-VM-3.6.11 -** Azure Security Policy Standard Document
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, https://myelc.elcompanies.com/sites/global-it-community/document/250052/ELC-ECR-007-Access-Control-Procedure ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.6 Authentication to Linux machines should require SSH keys.

Control ID	ELC-CS-VM-006
Severity	High
Enforcement	Recommended
Control Definition	SSH Keys ensure compliance for Linux machines and that is necessary for our security posture and integrity.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – IM-6 CIS Controls v7.1 ID(s) – 4.2,4.5,12.11,16.3 CIS Controls V8 (ID'S) – 6.3,6.4 NIST SP800-53 r4 ID(s) – AC-2, AC-3, IA-2, IA-5, IA-8 PCI-DSS v3.2.1 ID(s) – 7.2,8.2,8.3,8.4
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.7 Boot Diagnostics should be enabled on virtual machines.

Control ID	ELC-CS-VM-007
Severity	High
Enforcement	Recommended
Control Definition	For adequate troubleshooting and monitoring, boot diagnostics should be enabled on all VM's. These diagnostics provide us logs that should be captured and stored in Splunk.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-4 CIS Controls v7.1 ID(s) – 5.1,5.5,11.3 CIS Controls V8 (ID'S) – 4.1 NIST SP800-53 r4 ID(s) – CM-2, CM-6 PCI-DSS v3.2.1 ID(s) – 2.2
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.8 Enable a managed identity of each Virtual Machine.

Control ID	ELC-CS-VM-008
Severity	High
Enforcement	Recommended
Control Definition	Managed identities allow VM's to connect to Azure Services with simplified identity management, minimizing the need for manual credential storage and rotation.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – IM-1 CIS Controls v7.1 ID(s) – 16.1,16.2 CIS Controls V8 (ID'S) – 6.7,12.5 NIST SP800-53 r4 ID(s) – AC-2, AC-3, IA-2, IA-8 PCI-DSS v3.2.1 ID(s) – 7.2,8.3
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.9 Ensure that 'OS disks' are encrypted.

Control ID	ELC-CS-VM-009
Severity	High
Enforcement	Required
Control Definition	Ensure that OS disks (boot volumes) are encrypted, unless there is a specific documented exception in place.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – DP-4 CIS Controls v7.1 ID(s) – 14.8 CIS Controls V8 (ID'S) – 3.11 NIST SP800-53 r4 ID(s) – SC-28 PCI-DSS v3.2.1 ID(s) – 3.4,3.5
Recommendation & Procedure	Enable data at rest encryption by default. ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.10 Ensure that 'Data disks' are encrypted.

Control ID	ELC-CS-VM-010
Severity	High
Enforcement	Required
Control Definition	Ensure that data disks (non-boot volumes) are encrypted, unless there is a specific documented exception in place.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – DP-4 CIS Controls v7.1 ID(s) – 14.8 CIS Controls V8 (ID'S) – 3.11 NIST SP800-53 r4 ID(s) – SC-28 PCI-DSS v3.2.1 ID(s) – 3.4,3.5
Recommendation & Procedure	Enable data at rest encryption by default. ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.11 Virtual Machines should be deployed with ELC Sanctioned Image.

Control ID	ELC-CS-VM-011
Severity	High
Enforcement	Required
Control Definition	All Virtual Machines should contain an ELC Sanctioned image to ensure security, consistency and compliance across our ELC environment.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-5 CIS Controls v7.1 ID(s) – 3.1,3.3,3.6 CIS Controls V8 (ID'S) – 5.5,7.1,7.5,7.6, NIST SP800-53 r4 ID(s) – RA-3, RA-5 PCI-DSS v3.2.1 ID(s) – 6.1,6.2,6.6,11.2 **ELC-AZS-VM-3.6.22 -** Azure Security Policy Standard Document
Recommendation & Procedure	Refer to ELC Standards for Sanctioned Images. ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.12 Virtual machines should be migrated to new Azure Resource Manager resources.

Control ID	ELC-CS-VM-012
Severity	High
Enforcement	Recommended
Control Definition	Use new Azure info Resource Manager for your virtual machines to provide security enhancements like stronger access control (RBAC), improved auditing, governance, access to managed identities, and access to key vault for secrets. ARM also provides Azure Entra ID based authentication and support for tags/resource groups for easier security management.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – AM-2 CIS Controls v7.1 ID(s) – 2.7,2.8,2.9,9.2 CIS Controls V8 (ID'S) – 2.5,2.6,2.7,4.8 NIST SP800-53 r4 ID(s) – CM-8, PM-5 PCI-DSS v3.2.1 ID(s) – 6.3 **ELC-AZS-VM-3.6.20 -** Azure Security Policy Standard Document

Recommendation & Procedure	Use only approved services. ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

6.0.13 All Virtual Machines should be under the Frequently Managed Update Schedule.

Control ID	ELC-CS-VM-013
Severity	High
Enforcement	Required
Control Definition	Apply updated as they become available, monthly if applicable and in some cases sooner if there are critical security updates. This is meant by frequently managing an update schedule for Virtual Machines. This enhances security and limits vulnerabilities.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-6 CIS Controls v7.1 ID(s) – 3.4,3.5,3.7 CIS Controls V8 (ID'S) – 7.2,7.3,7.4,7.7 NIST SP800-53 r4 ID(s) – RA-3, RA-5, SI-2 PCI-DSS v3.2.1 ID(s) – 6.1,6.2,6.5,11.2 **ELC-AZS-VM-3.6.19 -** Azure Security Policy Standard Document
Recommendation & Procedure	Rapidly and automatically remediate vulnerabilities. ELC_Cloud_Security_Azure_Virtual_Machines_Reference_Document_V1.0.pdf

7.0 Logging and Monitoring

The Logging and Monitoring section defines the security control and standards for maintaining the security of ELC Information Technology to protect them from unauthorized access, modification, disclosure of Logs and monitoring the logs as per the standards and encrypt sensitive logging information at rest. The following industry good-practice frameworks, standards and guidelines were referenced from the standard section documents.

Section 3.5of Azure Security Policies defines the **Logging and Monitoring** Native Control under "**ELC Azure Security Policy Standards & Control Document of Azure Security Benchmark v2.1.0**."

7.0.1 Retain resource activity logs for at least one year. Azure activity logs are stored for 90 days in Azure and archived in Splunk for extended retention.

Control ID	ELC-CS-LM-001
Severity	High
Enforcement	Recommended
Control Definition	Utilize Splunk for extended log retention, Azure activity logs are stored for 90 days, and this allows for compliance, auditing and troubleshooting. Where needed archival using Splunk extends our logging period from 90 days to a full year.
Control Domain	MCSB – LT-6 CIS Controls V7.1 (ID'S) – 6.4 CIS Controls V8 (ID'S) – 8.3, 8.10, NIST SP800-53 r4 (ID'S) – AU-11, PCI-DSS V3.2.1 – 10.5,10.7
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Monitoring_Reference_Document_V1.0.pdf https://myelc.elcompanies.com/sites/global-it-community/document/250056/ELC-ECR-011-Logging-and-Monitoring-Procedure

7.0.2 Collect activity logs from all regions using Azure Monitor.

Control ID	ELC-CS-LM-002
Severity	High
Enforcement	Recommended
Control Definition	As per our previous log controls, this control extends to all regions and centralizes logs for more effective and efficient auditing and compliance.
Control Domain	MCSB V1.0 - LT-5, CIS Controls v7.1 ID(s) – 6.5, 6.6, 6.7, 8.6. CIS Controls V8 (ID'S) – 8.9, 8.11, 13.1. NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-11. PCI-DSS v3.2.1 ID(s) – N/A
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Monitoring_Reference_Document_V1.0.pdf

7.0.3 Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action'.

Control ID	ELC-CS-LM-003
Severity	High
Enforcement	Recommended
Control Definition	This policy ensures that a log profile collects logs for categories 'write,' 'delete,' and 'action
Control Domain	MCSB V1.0 - LT-5, CIS Controls v7.1 ID(s) – 6.5, 6.6, 6.7, 8.6. CIS Controls V8 (ID'S) – 8.9, 8.11, 13.1. NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-11. PCI-DSS v3.2.1 ID(s) – N/A
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Monitoring_Reference_Document_V1.0.pdf

7.0.4 Storage account containing the container with activity logs should be encrypted with BYOK.

Control ID	ELC-CS-LM-004
Severity	High
Enforcement	Recommended
Control Definition	This policy audits if the Storage account containing the container with activity logs is encrypted with BYOK. The policy works only if the storage account lies on the same subscription as activity logs by design. More information on Azure Storage encryption at rest can be found here https://aka.ms/azurestoragebyok. Long term should be stored in Splunk or ELC ECR sanctioned logging archival solution. Logging should be stored locally 90 days.
Control Domain	MCSB V1.0 - DP-5, CIS Controls v7.1 ID(s) – 14.8. CIS Controls V8 (ID'S) – 3.11. NIST SP800-53 r4 ID(s) – SC-12, SC-18. PCI-DSS v3.2.1 ID(s) – 3.4, 3.5, 3.6.

Recommendation & Procedure	Please refer to the Best Practice Document to proceed further,ELC_Cloud_Security_Azure_Monitoring_Reference_Document_V1.0.pdf

7.0.5 Azure monitoring agent should be installed on your virtual machine/virtual machine scale sets for Azure Security Center monitoring.

Control ID	ELC-CS-LM-005
Severity	High
Enforcement	Recommended
Control Definition	This policy audits any Windows/Linux virtual machines (VMs) if the Azure monitoring agent is not installed which Security Center uses to monitor for security vulnerabilities and threats. Relevant security logs are captured on ELC sanctioned log monitoring/archival solutions.
Control Domain	MCSB V1.0 - LT-1, CIS Controls v7.1 ID(s) – 6.7. CIS Controls V8 (ID'S) – 8.11. NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-12. PCI-DSS v3.2.1 ID(s) – N/A **ELC-AZS-LM-3.5.1** - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Monitoring_Reference_Document_V1.0.pdf

7.0.6 Resource logs in the IoT Hub should be enabled.

Control ID	ELC-CS-LM-006
Severity	High
Enforcement	Recommended
Control Definition	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigative purposes; when a security incident occurs or when your network is compromised.
Control Domain	MCSB V1.0 - LT-1, CIS Controls v7.1 ID(s) – 6.7.

	CIS Controls V8 (ID'S) – 8.11. NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-12. PCI-DSS v3.2.1 ID(s) – N/A **ELC-AZS-LM-3.5.2** - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Monitoring_Reference_Document_V1.0.pdf

7.0.7 Resource logs in Logic Apps should be enabled.

Control ID	ELC-CS-LM-007
Severity	High
Enforcement	Recommended
Control Definition	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigative purposes; when a security incident occurs or when your network is compromised.
Control Domain	MCSB V1.0 - LT-1, CIS Controls v7.1 ID(s) – 6.7. CIS Controls V8 (ID'S) – 8.11. NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-12. PCI-DSS v3.2.1 ID(s) – N/A
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Monitoring_Reference_Document_V1.0.pdf

7.0.8 Resource logs in Key Vault should be enabled.

Control ID	ELC-CS-LM-008
Severity	High
Enforcement	Recommended
Control Definition	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigative purposes when a security incident occurs or when your network is compromised.

Control Domain	MCSB V1.0 - LT-3, CIS Controls v7.1 ID(s) – 6.2, 6.3, 8.8. CIS Controls V8 (ID'S) – 8.2, 8.5, 8.12. NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-12, SI-4. PCI-DSS v3.2.1 ID(s) – 10.1, 10.2, 10.3.
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_Monitoring_Reference_Document_V1.0.pdf

8.0 App Service

The App Service section defines the security control and standards for maintaining the security of ELC Information Technology Storage to protect them from unauthorized access, modification, disclosure, and encrypt sensitive data with the strong encryption standards. The following industry good-practice frameworks, standards and guidelines were referenced from the standard section documents.

Section 3.7 of Azure Security Policies defines the Azure App Services and Function Apps native control **under "ELC Azure Security Policy Standards & Control Document of Azure Security Benchmark v2.1.0."**

8.0.1 App Service apps must use the TLS 1.2 version or higher.

Control ID	ELC-CS-AS-001
Severity	High
Enforcement	Required
Control Definition	Must use the TLS 1.2 version or higher for App Service apps to take advantage of security fixes, and/or new functionalities that come with the latest version.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – NS-8, DP-3 CIS Controls V7.1 (ID'S) – 9.2, 14.4 CIS Controls V8 (ID'S) – 4.4,4.8, 3.10 NIST SP800-53 r4 (ID'S) – CM-2, CM-6, CM-7, SC-8 PCI-DSS V3.2.1 – 4.1, A2.1, A2.2, A2.3, 3.5,3.6,4.1
Recommendation & Procedure	Detect and disable insecure services and protocols. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.2 Function apps should use the latest TLS version (minimum TLS 1.2)

Control ID	ELC-CS-AS-002
Severity	High
Enforcement	Required
Control Definition	Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, and/or new functionalities that come with the latest version.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – NS-8, DP-3 CIS Controls V7.1 (ID'S) – 9.2, 14.4 CIS Controls V8 (ID'S) – 4.4,4.8, 3.10 NIST SP800-53 r4 (ID'S) – CM-2, CM-6, CM-7, SC-8 PCI-DSS V3.2.1 – 4.1, A2.1, A2.2, A2.3, 3.5,3.6,4.1
Recommendation & Procedure	Detect and disable insecure services and protocols. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.3 App Services apps should use managed identity

Control ID	ELC-CS-AS-003
Severity	High
Enforcement	Recommended
Control Definition	Managed identities enhance security by automating identity management and removing the need for manual credential handling
Control Domain	Microsoft Cloud Security Benchmark V1.0 – IM-3 CIS Controls v7.1 ID(s) – N/A CIS Controls V8 (ID'S) – N/A NIST SP800-53 r4 ID(s) – AC-2, AC-3, IA-4, IA-5, IA-9 PCI-DSS v3.2.1 ID(s) – N/A **ELC-AZS-AS-3.7.2 -** Azure Security Policy Standard Document
Recommendation & Procedure	Manage application identities securely and automatically. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.4 Function apps should use managed identity.

Control ID	ELC-CS-AS-004
Severity	High
Enforcement	Recommended
Control	Managed identities enhance security by automating identity

Definition	management and removing the need for manual credential handling.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – IM-3 CIS Controls v7.1 ID(s) – N/A CIS Controls V8 (ID'S) – N/A NIST SP800-53 r4 ID(s) – AC-2, AC-3, IA-4, IA-5, IA-9 PCI-DSS v3.2.1 ID(s) – N/A
Recommendation & Procedure	Manage application identities securely and automatically. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf
Severity	High

8.0.5 App Service apps should be published only via HTTPS

Control ID	ELC-CS-AS-005
Severity	High
Enforcement	Required
Control Definition	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks
Control Domain	Microsoft Cloud Security Benchmark V1.0 – DP-3 CIS Controls v7.1 ID(s) – 14.4 CIS Controls V8 (ID'S) – 3.10 NIST SP800-53 r4 ID(s) – SC-8 PCI-DSS v3.2.1 ID(s) – 3.5,3.6,4.1 **ELC-AZS-AS-3.7.1 -** Azure Security Policy Standard Document
Recommendation & Procedure	Encrypt sensitive data in transit. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.6 Function apps should be published only via HTTPS

Control ID	ELC-CS-AS-006
Severity	High
Enforcement	Required
Control Definition	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks
Control Domain	Microsoft Cloud Security Benchmark V1.0 – DP-3 CIS Controls v7.1 ID(s) – 14.4 CIS Controls V8 (ID'S) – 3.10 NIST SP800-53 r4 ID(s) – SC-8

	PCI-DSS v3.2.1 ID(s) – 3.5,3.6,4.1
Recommendation & Procedure	Encrypt sensitive data in transit. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.7 App Service applications should enforce FTPS only

Control ID	ELC-CS-AS-007
Severity	High
Enforcement	Required
Control Definition	FTPS-only access ensures secure file transfers, helps protect data in transit through encryption and reduces the risk of a breach or possible unauthorized access.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – DP-3 CIS Controls v7.1 ID(s) – 14.4 CIS Controls V8 (ID'S) – 3.10 NIST SP800-53 r4 ID(s) – SC-8 PCI-DSS v3.2.1 ID(s) – 3.5,3.6,4.1
Recommendation & Procedure	Encrypt sensitive data in transit. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.8 Function apps should require FTPS only

Control ID	ELC-CS-AS-008
Severity	High
Enforcement	Required
Control Definition	Enable FTPS enforcement for enhanced security. If FTPS required should only restricted to ELC internal networks
Control Domain	Microsoft Cloud Security Benchmark V1.0 – DP-3 CIS Controls v7.1 ID(s) – 14.4 CIS Controls V8 (ID'S) – 3.10 NIST SP800-53 r4 ID(s) – SC-8 PCI-DSS v3.2.1 ID(s) – 3.5,3.6,4.1
Recommendation & Procedure	Encrypt sensitive data in transit. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.9 App Service apps should have resource logs enabled

Control ID	ELC-CS-AM-009
Severity	High
Enforcement	Recommended
Control Definition	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigative purposes if a security incident occurs or your network is compromised.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – LT-3 CIS Controls v7.1 ID(s) – 6.2,6.3,8.8 CIS Controls V8 (ID'S) – 8.2,8.5,8.12 NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-12, SI-4 PCI-DSS v3.2.1 ID(s) – 10.1,10.2,10.3
Recommendation & Procedure	Enable logging for security investigation. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.10 App service must be configured with Vnet Integration

Control ID	ELC-CS-AS-010
Severity	High
Enforcement	Recommended
Control Definition	The App Service virtual network integration feature enables your apps to access resources in or through a virtual network.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-2 CIS Controls v7.1 ID(s) – 5.4,5.5,11.3 CIS Controls V8 (ID'S) – 4.1,4.2 NIST SP800-53 r4 ID(s) – CM-2, CM-6 PCI-DSS v3.2.1 ID(s) –2.2
Recommendation & Procedure	Audit and enforce secure configurations. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.11 App Service apps should have remote debugging turned off

Control ID	ELC-CS-AS-011
Severity	High
Enforcement	Required
Control Definition	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-2 CIS Controls v7.1 ID(s) – 5.4,5.5,11.3 CIS Controls V8 (ID'S) – 4.1,4.2 NIST SP800-53 r4 ID(s) – CM-2, CM-6 PCI-DSS v3.2.1 ID(s) –2.2 **ELC-AZS-AS-3.7.4-** Azure Security Policy Standard Document
Recommendation & Procedure	Audit and enforce secure configurations. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.12 App Service apps should not have CORS configured to allow every resource to access your apps

Control ID	ELC-CS-AS-012
Severity	High
Enforcement	Required
Control Definition	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your app. Allow only required domains to interact with your app.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-2 CIS Controls v7.1 ID(s) – 5.4,5.5,11.3 CIS Controls V8 (ID'S) – 4.1,4.2 NIST SP800-53 r4 ID(s) – CM-2, CM-6 PCI-DSS v3.2.1 ID(s) –2.2
Recommendation & Procedure	Audit and enforce secure configurations. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.13 Function apps should have remote debugging turned off

Control ID	ELC-CS-AS-013
Severity	High
Enforcement	Required
Control Definition	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-2 CIS Controls v7.1 ID(s) – 5.4,5.5,11.3 CIS Controls V8 (ID'S) – 4.1,4.2 NIST SP800-53 r4 ID(s) – CM-2, CM-6 PCI-DSS v3.2.1 ID(s) –2.2 **ELC-AZS-AS-3.7.5 -** Azure Security Policy Standard Document
Recommendation & Procedure	Audit and enforce secure configurations. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.14 Function apps should not have CORS configured to allow every resource to access your apps

Control ID	ELC-CS-AS-014
Severity	High
Enforcement	Required
Control Definition	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your Function app. Allow only required domains to interact with your Function app.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-2 CIS Controls v7.1 ID(s) – 5.4,5.5,11.3 CIS Controls V8 (ID'S) – 4.1,4.2 NIST SP800-53 r4 ID(s) – CM-2, CM-6 PCI-DSS v3.2.1 ID(s) –2.2
Recommendation & Procedure	Audit and enforce secure configurations. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.15 Azure Defender for App Service should be enabled

Control ID	ELC-CS-AS-015
Severity	High
Enforcement	Recommended
Control Definition	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – LT-1 CIS Controls v7.1 ID(s) – 6.7 CIS Controls V8 (ID'S) – 8.11 NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-12, SI-4 PCI-DSS v3.2.1 ID(s) –10.6,10.8, A3.5,
Recommendation & Procedure	Enable threat detection capabilities. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.16 App Service apps should have resource logs enabled.

Control ID	ELC-CS-AS-016
Severity	High
Enforcement	Recommended
Control Definition	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – LT-3 CIS Controls v7.1 ID(s) – 6.2,6.3,8.8 CIS Controls V8 (ID'S) – 8.2,8.5,8.12 NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-12, SI-4 PCI-DSS v3.2.1 ID(s) –10.1,10.2,10.3
Recommendation & Procedure	Enable logging for security investigation. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

8.0.17 Ensure that App service ingress/egress route paths to from the internet are internally routed.

Control ID	ELC-CS-AS-017
Severity	High
Enforcement	Required
Control Definition	They should route via the east/west traffic via the east/west firewalls and ingress/egress traffic via the north/south Firewalls.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – LT-3 CIS Controls v7.1 ID(s) – 6.2,6.3,8.8 CIS Controls V8 (ID'S) – 8.2,8.5,8.12 NIST SP800-53 r4 ID(s) – AU-3, AU-6, AU-12, SI-4 PCI-DSS v3.2.1 ID(s) –10.1,10.2,10.3
Recommendation & Procedure	Enable logging for security investigation. ELC_Cloud_Security_Azure_AppService_Reference_Document_V1.0.pdf

9.0 Azure Kubernetes Service

The Azure Kubernetes Services section defines the security control and standards for maintaining the security of ELC Information Technology to protect them from unauthorized access, modification, disclosure, and encrypt sensitive data inside the AKS services. The following industry good-practice frameworks, standards and guidelines were referenced from the standard section documents.

Section 3.8 of Azure Security Policies defines the Azure Kubernetes Services native control under "**ELC Azure Security Policy Standards & Control Document of Azure Security Benchmark v2.1.0**".

9.0.1 Use Azure Role-Based Access Control (RBAC) on Kubernetes services.

Control ID	ELC-CS-AKS-001
Severity	High
Enforcement	Required
Control Definition	Ensures only authorized users have the appropriate level of access and provides least access privilege within the Kubernetes environment.

Control Domain	CIS Microsoft Azure Foundations Benchmark V1.0, V1.3.0, V1.4.0 – Control ID – 8.5, CMMC Level 3 - AC.1.001, AC.1.002, AC.2.007, AC.2.016, AC.1.062, Microsoft Cloud Security Benchmark V1.0 – PA-7, NIST SP800-53 r4 ID(s) – AC (3)-7, NIST SP800-53 r5 ID(s) – AC (3)-7 ELC-AZS-AKS-3.3.12 - Azure Security Policy Standard Document
Recommendation & Procedure	To provide granular filtering on the actions that users can perform, use Azure Role-Based Access Control (RBAC) to manage permissions in Kubernetes Service Clusters and configure relevant authorization policies. ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf

9.0.2 Kubernetes clusters should be accessible only over HTTPS.

Control ID	ELC-CS-AKS-002
Severity	High
Enforcement	Required
Control Definition	HTTPS access protects data in transit, prevents it from being intercepted; and reduces the risk of unauthorized access to the cluster.
Control Domain	FedRAMP High – SC-8 Microsoft Cloud Security Benchmark V1.0 – IM-3 CIS Controls v7.1 ID(s) – N/A CIS Controls V8 (ID'S) – N/A NIST SP800-53 r4 ID(s) – AC-2, AC-3, IA-4, IA-5, IA-9 PCI-DSS v3.2.1 ID(s) – N/A
Recommendation & Procedure	Manage application identities securely and automatically. ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf

9.0.3 CPU and memory resource limits for Kubernetes cluster containers should not exceed specified thresholds.

Control ID	ELC-CS-AKS-003
Severity	High
Enforcement	Recommended
Control Definition	This prevents Kubernetes Cluster containers from consuming excessive resources which will prevent service disruptions and stabilize performance.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV2 Fed Ramp Moderate – CM6 Fed Ramp High – CM6 NIST SP 800-171 R2 – 3.4.1, 3.4.2 NIST SP800-53 r4 ID(s) – CM-6 NIST SP800-53 r5 ID(s) – SC-8 NL BIO Cloud Theme – C.04.7
Recommendation & Procedure	Enforce container CPU and memory resource limits to prevent resource exhaustion attacks in a Kubernetes cluster ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf

9.0.4 Authorized IP ranges should be defined on Kubernetes Services.

Control ID	ELC-CS-AKS-004
Severity	High
Enforcement	Required
Control Definition	Established Authorized IP ranges for Kubernetes services restrict access to specified sources. This works to protect our Kubernetes environment from potential outside threats.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – NS2 Fed Ramp Moderate – AC4, SC-7, SC-7(3) Fed Ramp High – AC4, SC-7, SC-7(3) NIST SP 800-171 R2 – 3.1.3, 3.13.1, 3.13.2, 3.13.5, 3.13.6 NIST SP800-53 r4 ID(s) – AC-4, SC-7, SC-7(3) NIST SP800-53 r5 ID(s) – AC-4, SC-7, SC-7(3) NL BIO Cloud Theme – U.07.1
Recommendation & Procedure	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized IP

	ranges to ensure that only applications from allowed networks can access the cluster. ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf

9.0.5 Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your cluster.

Control ID	ELC-CS-AKS-005
Severity	High
Enforcement	Required
Control Definition	Install and enable Azure Policy Add on for AKS to enforce up to date compliance and governance within the cluster. This will remediate any non-compliant resources in the cluster.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV2 Fed Ramp Moderate – CM6 Fed Ramp High – CM6 NIST SP 800-171 R2 – 3.4.1, 3.4.2 NIST SP800-53 r4 ID(s) – CM-6 NIST SP800-53 r5 ID(s) – CM-6
Recommendation & Procedure	Kubernetes service (AKS) extends Gatekeeper v3, an admission controller webhook for Open Policy Agent (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner. ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf

9.0.6 Kubernetes cluster containers should only use allowed images.

Control ID	ELC-CS-AKS-006
Severity	High
Enforcement	Required
Control Definition	Kubernetes cluster containers should only use trusted images, this ensures consistency and reliability in deployments.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV2 Fed Ramp Moderate – CM6 Fed Ramp High – CM6

	NIST SP 800-171 R2 – 3.4.1,3.4.2 NIST SP800-53 r4 ID(s) – CM-6 NIST SP800-53 r5 ID(s) – CM-6
Recommendation & Procedure	ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0

9.0.7 Kubernetes cluster pods and containers should only run with approved user and group ID.

Control ID	ELC-CS-AKS-007
Severity	High
Enforcement	Required
Control Definition	Approved user and group IDs for Kubernetes cluster pods and containers enforces least privilege principles and furthers our security posture.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-2 Fed Ramp Moderate – CM6 Fed Ramp High – CM6 NIST SP 800-171 R2 – 3.4.1,3.4.2 NIST SP800-53 r4 ID(s) – CM-6 NIST SP800-53 r5 ID(s) – CM-6 NL BIO Cloud Theme – C.04.7 RMIT – 10.55
Recommendation & Procedure	Control the user, primary group, supplemental group, and file system group IDs that pods and containers can use to run in a Kubernetes Cluster ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf

9.0.8 Define IP Ranges on Kubernetes Services.

Control ID	ELC-CS-AKS-008
Severity	High
Enforcement	Required
Control Definition	Access needs to be restricted to trusted IP addresses; this supports network segmentation and increases compliance with access related policies.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – NS-2 FedRamp High – AC-4, SC-7, SC-7(3)

	FedRamp Moderate – AC-4, SC-7, SC-7(3) NIST SP 800-171 R2 – 3.1.3, 3.13.1, 3.13.2, 3.13.5, 3.13.6, NIST SP800-53 r4 ID(s) – AC-4, SC-7, SC-7(3) NIST SP800-53 r5 ID(s) – AC-4, SC-7, SC-7(3) NL BIO Cloud Theme – U.07.1
Recommendation & Procedure	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf

9.0.9 Resource logs in Azure Kubernetes Service should be enabled.

Control ID	ELC-CS-AKS-009
Severity	High
Enforcement	Recommended
Control Definition	Capture detailed information through logs and position us to monitor and troubleshoot potential issues within the AKS environment efficiently.
Control Domain	Microsoft Cloud Security Benchmark V1.0 – LT-3 NL BIO Cloud Theme – U.15.1
Recommendation & Procedure	Azure Kubernetes Service's resource logs can help recreate activity trails when investigating security incidents. Enable it to make sure the logs will exist when needed. ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf

9.0.10 Azure running container images should have vulnerabilities resolved.

Control ID	ELC-CS-AKS-010
Severity	High
Enforcement	Required
Control Definition	This is for various third-party applications, we will enable FTPS enforcement for enhanced security
Control Domain	Microsoft Cloud Security Benchmark V1.0 – PV-6, DS-6 NL BIO Cloud Theme – U.09.3
Recommendation & Procedure	Container image vulnerability assessment scans container images running on your Kubernetes clusters for security

	vulnerabilities and exposes detailed findings for each image. Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks. ELC_Cloud_Security_Azure Kubernetes_Services_Reference_Document_V1.0.pdf
Severity	High

10.0 Data Protection

The Data Protection section defines the security control and standards for maintaining the security of ELC Information Technology to protect them from unauthorized access, modification, disclosure, and encrypt sensitive information at rest and transit. The following industry good-practice frameworks, standards and guidelines were referenced from the standard section documents.

Section 3.3 of Azure Security Policies defines the Data Protection native control under "**ELC Azure Security Policy Standards & Control Document of Azure Security Benchmark v2.1.0**".

10.0.1 All cloud hosted DBs must be encrypted at rest.

Control ID	ELC-CS-DP-001
Severity	High
Enforcement	Required
Control Definition	All IaaS/PaaS DBs must be encrypted at rest with the minimum system managed keys. When hosting sensitive/critical data customer managed keys are recommended. Azure Key vault can be used for key storage.
Control Domain	MCSB – DP-5 ASB v3-DP-5 CIS Controls V7.1 ID(s) – 14.8 CIS Controls V8 ID(s) – 3.11 NIST SP800-53 r4 ID(s) – SC-12, SC-28. PCI-DSS V3.2.1 ID(s) – 3.4, 3.5, 3.6 ELC-AZS-DP-3.3.1 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_DataProtection_Reference_Document_V1.0.pdf

10.0.2 All the data at transit must be encrypted between DB server and Client.

Control ID	ELC-CS-DP-002
Severity	High
Enforcement	Required
Control Definition	Enforcing encryption such as SSL/TLS between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application.
Control Domain	MCSB V1.0 - DP-3. ASB v3-DP-3. CIS Controls v7.1 ID(s) – 14.4. CIS Controls V8 ID(s) – 3.10 NIST SP800-53 r4 ID(s) – SC-8 PCI-DSS v3.2.1 ID(s) – 3.5, 3.6, 4.1 ELC-AZS-DP-3.3.2 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_DataProtection_Reference_Document_V1.0.pdf

10.0.3 Key vault items must be rotated /renewed periodically.

Control ID	ELC-CS-DP-003
Severity	High
Enforcement	Recommended
Control Definition	Key vault items should have defined expiry date and rotated/renewed periodically. key vault items that are valid forever provide a potential attacker with more time to compromise them. It is a recommended security practice to set expiration dates on secrets/keys.
Control Domain	MCSB V1.0 – DP-6. ASB v3-DP-6 CIS Controls v7.1 ID(s) – N/A CIS Controls V8 ID(s) – N/A NIST SP800-53 r4 ID(s) – IA-5, SC-12, SC-28. PCI-DSS v3.2.1 ID(s) – 3.6 ELC-AZS-DP-3.3.3 - Azure Security Policy Standard Document

Recommendation & Procedure	Please refer the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_DataProtection_Reference_Document_V1.0.pdf

10.0.4 Database servers should use customer-managed keys to encrypt data at rest.

Control ID	ELC-CS-DP-004
Severity	High
Enforcement	Recommended
Control Definition	Implementing Transparent Data Encryption (TDE) with your own key provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to data classified with related compliance requirements.
Control Domain	MCSB – DP-5 ASB v3-DP-5 CIS Controls V7.1 ID(s) – 14.8 CIS Controls V8 ID(s) – 3.11 NIST SP800-53 r4 ID(s) – SC-12, SC-28. PCI-DSS V3.2.1 ID(s) – 3.4, 3.5, 3.6 ELC-AZS-DP-3.3.4 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_DataProtection_Reference_Document_V1.0.pdf

10.0.5 Transparent Data Encryption on SQL databases should be enabled.

Control ID	ELC-CS-DP-005
Severity	High
Enforcement	Recommended
Control Definition	Transparent data encryption should be enabled to protect data-at-rest, as per ELC data classifications and protection requirements.
Control Domain	MCSB V1.0 - DP-4.

	ASB v3-DP-4. CIS Controls v7.1 ID(s) – 14.8. CIS Controls V8 ID(s) – 3.11. NIST SP800-53 r4 ID(s) – SC-28. PCI-DSS v3.2.1 ID(s) – 3.4, 3.5. ELC-AZS-DP-3.3.8 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_DataProtection_Reference_Document_V1.0.pdf

10.0.6 Key vaults should have soft delete enabled.

Control ID	ELC-CS-DP-06
Severity	High
Enforcement	Recommended
Control Definition	Deleting a key vault without soft delete enabled permanently deletes all secrets, keys, and certificates stored in the key vault. Accidental deletion of a key vault can lead to permanent data loss. Soft delete allows you to recover an accidentally deleted key vault for a configurable retention period.
Control Domain	MCSB V1.0 - DP-8. ASB v3-DP-8. CIS Controls v7.1 ID(s) – N/A. CIS Controls V8 ID(s) – N/A. NIST SP800-53 r4 ID(s) – IA-5, SC-12, SC-17. PCI-DSS v3.2.1 ID(s) – 3.6. ELC-AZS-DP-3.3.11 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_DataProtection_Reference_Document_V1.0.pdf

10.0.7 Managed disks should have Layered encryption with both platform-managed and customer-managed keys.

Control ID	ELC-CS-DP-07
Severity	High
Enforcement	Recommended
Control Definition	High security sensitive customers who are concerned of the risk associated with any encryption algorithm, implementation, or key being compromised can opt for additional layer of encryption using a different encryption algorithm/mode at the infrastructure layer using platform managed encryption keys. The disk encryption sets are required to use double encryption. Learn more at https://aka.ms/disks-doubleEncryption.
Control Domain	MCSB V1.0 - DP-3. ASB v3-DP-3. CIS Controls v7.1 ID(s) – 14.4. CIS Controls V8 ID(s) – 3.10 NIST SP800-53 r4 ID(s) – SC-8 PCI-DSS v3.2.1 ID(s) – 3.5, 3.6, 4.1 ELC-AZS-DP-3.3.13 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_DataProtection_Reference_Document_V1.0.pdf

10.0.8 Vulnerability assessment should be enabled on SQL Managed Instance.

Control ID	ELC-CS-DP-08
Severity	High
Enforcement	Recommended
Control Definition	Audit each SQL Managed Instance and ensure vulnerability assessment scans are enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.
Control Domain	MCSB V1.0 - PV-5. ASB v3-DP-5. CIS Controls v7.1 ID(s) – 3.1, 3.3, 3.6. CIS Controls V8 ID(s) – 5.5, 7.1, 7.5, 7.6. NIST SP800-53 r4 ID(s) – RA-3, RA-5. PCI-DSS v3.2.1 ID(s) – 6.1, 6.2, 6.6, 11.2. ELC-AZS-DP-3.3.15 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer the Best Practice Document to proceed further, ELC_Cloud_Security_Azure_DataProtection_Reference_Document_V1.0.pdf

11.0 Identity Management

The Identity Management section defines the security control and standards for maintaining the security of ELC Information Technology to protect them from unauthorized access, modification, disclosure of identity management. The following industry good-practice frameworks, standards and guidelines were referenced from the standard section documents.

Section 3.1 of Azure Security Policies defines the IAM native control under **"ELC Azure Security Policy Standards & Control Document of Azure Security Benchmark v2.1.0."**

11.0.1 Azure API Management Services should have local authentication disabled.

Control ID	ELC-CS-IAM-01
Severity	High
Enforcement	Required
Control Definition	Portal local user authentication should be disabled. Local user authentication should be enabled with ELC managed Identity platform (currently ForgeRock)
Control Domain	Microsoft Cloud Security Benchmark V1.0 - IA-9, CIS Controls V7.1 (ID'S) - NA CIS Controls V8 (ID'S) - NA, NIST SP800-53 r4 (ID'S) - IA-9 PCI-DSS V3.2.1 - NA
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further. ELC_Cloud_Security_Azure_Identity_Management_Reference_Document_V1.0.pdf

11.0.2 Management of Azure PaaS Databases should be authenticated through ELC Sanctioned IAM Platform.

Control ID	ELC-CS-IAM-02
Severity	High
Enforcement	Required
Control Definition	Audit provisioning of an Azure Entra ID administrator for your SQL server to enable Azure Entra authentication. Azure Entra authentication enables simplified permission management and centralized identity management of database users and other Microsoft services.
Control Domain	ABS V3 – IM-1 CIS Controls V7.1 (ID'S) – 16.1,16.2 CIS Controls V8 (ID'S) – 6.7,12.5, NIST SP800-53 r4 (ID'S) – AC-2, AC-3, IA-2, IA-8 PCI-DSS V3.2.1 – 7.2,8.3
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further.ELC_Cloud_Security_Azure_Identity_Management_Reference_Document_V1.0.pdf

11.0.3 Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity.

Control ID	ELC-CS-IAM-03
Severity	High
Enforcement	Required
Control Definition	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity.
Control Domain	ABS V3 – IM-3 CIS Controls V7.1 (ID'S) -NA CIS Controls V8 (ID'S) - NA NIST SP800-53 r4 (ID'S) – AC-2, AC-3, IA-4, IA-5, IA-9. PCI-DSS V3.2.1 - NA
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further. ELC_Cloud_Security_Azure_Identity_Management_Reference_Document_V1.0.pdf

11.0.4 Access to owner privileges should be restricted and limited.

Control ID	ELC-CS-IAM-04
Severity	High
Enforcement	Required
Control Definition	It is recommended to designate maximum up to 3 subscription owners. Owner privileges should be accessed through the Break Glass procedure sanctioned by ELC Security and Cloud Ops. All Azure access should be restricted to Least Privileged Role Based Access Control Policies (RBAC)
Control Domain	ABS V3 – PA-1 CIS Controls V7.1 (ID'S) -4.3, 14.6 CIS Controls V8 (ID'S) – 5.4, 6.8 NIST SP800-53 r4 (ID'S) – AC-2, AC-6 PCI-DSS V3.2.1 – 7.1, 7.2, 8.1 ELC-AZS-IAM-3.1.3, 3.1.6 - Azure Security Policy Standard Document
Recommendation & Procedure	Please refer to the Best Practice document to proceed further. ELC_Cloud_Security_Azure_Identity_Management_Reference_Document_V1.0.pdf

11.0.5 Audit all the Privileged Roles

Control ID	ELC-CS-IAM-05
Severity	High
Enforcement	Recommended
Control Definition	Audit all privileged roles and keep logs for 12 months
Control Domain	ABS V3 – PA-7 CIS Controls V7.1 (ID'S) – 14.6 CIS Controls V8 (ID'S) – 3.3, 6.8 NIST SP800-53 r4 (ID'S) - AC-2, AC-3, AC-6 PCI-DSS V3.2.1 – 7.1, 7.2
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further.ELC_Cloud_Security_Azure_Identity_Management_Reference_Document_V1.0.pdf

11.0.6 All accounts should have MFA enabled.

Control ID	ELC-CS-IAM-06
Severity	High
Enforcement	Required
Control Definition	All accounts should have MFA enabled. Their can be exemptions which will be documented in a Policy document and will be treated case by case.
Control Domain	Microsoft cloud security benchmark V1 - IM-6 ABS V3 – IM-6 CIS Controls V7.1 (ID'S) -NA CIS Controls V8 (ID'S) - NA NIST SP800-53 r4 (ID'S) - NA PCI-DSS V3.2.1 - NA
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further. ELC_Cloud_Security_Azure_Identity_Management_Reference_Document_V1.0.pdf

11.0.7 Azure Data Factory linked services should use system-assigned managed identity authentication when it is supported.

Control ID	ELC-CS-IAM-07
Severity	High
Enforcement	Recommended
Control Definition	Using system-assigned managed identity when communicating with data stores via linked services avoids the use of less secured credentials such as passwords or connection strings.
Control Domain	ABS V3 – NA CIS Controls V7.1 (ID'S) - NA CIS Controls V8 (ID'S) - NA NIST SP800-53 r4 (ID'S) - NA PCI-DSS V3.2.1 - NA
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further.ELC_Cloud_Security_Azure_Identity_Management_Reference_Document_V1.0.pdf

11.0.8 Configure Azure Event Grid partner namespaces to disable local authentication.

Control ID	ELC-CS-IAM-08
Severity	High
Enforcement	Required
Control Definition	Disable local authentication methods so that your Azure Event Grid partner namespaces exclusively require Azure Active Directory identities for authentication.
Control Domain	ABS V3 – NA CIS Controls V7.1 (ID'S) - NA CIS Controls V8 (ID'S) - NA NIST SP800-53 r4 (ID'S) - NA PCI-DSS V3.2.1 - NA
Recommendation & Procedure	Please refer to the Best Practice Document to proceed further. ELC_Cloud_Security_Azure_Identity_Management_Reference_Document_V1.0.pdf

12.0 Reference Document links

Reference Document