**ELC – App Service - Proof of Concept**

**(POC)**

**Initial Draft version v1.1**

**Submitted to**

Text, logo

Description automatically generated

**By**

A logo with colorful dots

Description automatically generated

**Wipro Technologies**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Revision** | **Description of Change** | **Reason for Change** | **Reviewed By** |
| 1.1 | 31-Oct-23 | Initial Draft | NA | Felix & Kannan |
|  |  |  |  |  |
|  |  |  |  |  |

**Author/Reviewer/Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Designation** | **Responsibility** | **Date** |
| Arun Kumar V | Consultant | Author | 31-Oct-23 |
| Kannan Kuppusamy | Technical Lead | Reviewer | 01-Nov-23 |
| Felix Jebamani | Lead Consultant | Reviewer | 01-Nov-23 |
| Jamshid Abedi | ELC ED, Global Head of Security Engineer | Approver | 00-Oct-23 |

**Table of Contents**

[Overview 4](#_Toc159009834)

[Purpose and Scope 4](#_Toc159009835)

[1.0 Best Practice 01 - App Service apps should use the latest TLS version 5](#_Toc159009836)

[1.1 Description 5](#_Toc159009837)

[1.2 Control Domain 5](#_Toc159009838)

[1.3 Non-Compliance Message 5](#_Toc159009839)

[2.0 Best Practice 02 - Function apps should use the latest TLS version. 8](#_Toc159009843)

[2.1 Description 8](#_Toc159009844)

[2.2 Control Domain 8](#_Toc159009845)

[2.3 Non-Compliance 8](#_Toc159009846)

[3.0 Best practice 03 - App Service apps should use managed identity . 13](#_Toc159009850)

[3.1 Description 13](#_Toc159009851)

[3.2 Control Domain 13](#_Toc159009852)

[3.3 Non-Compliance Message 13](#_Toc159009853)

[4.0 Best practice 04 - Function apps should use managed identity.. 19](#_Toc159009857)

[4.1 Description 19](#_Toc159009858)

[4.2 Control Domain 19](#_Toc159009859)

[4.3 Non-Compliance Message 19](#_Toc159009860)

[5.0 Best practice 05 - App Service apps should only be accessible over HTTPS 22](#_Toc159009864)

[5.1 Description 22](#_Toc159009865)

[5.2 Control Domain 22](#_Toc159009866)

[5.3 Non-Compliance Message 22](#_Toc159009867)

[6.0 Best practice 06 - Function apps should only be accessible over HTTPS 22](#_Toc159009864)

[6.1 Description 22](#_Toc159009865)

[6.2 Control Domain 22](#_Toc159009866)

[6.3 Non-Compliance Message 22](#_Toc159009867)

[7.0 Best practice 07 -App Service apps should require FTPS only 22](#_Toc159009864)

[7.1 Description 22](#_Toc159009865)

[7.2 Control Domain 22](#_Toc159009866)

[7.3 Non-Compliance Message 22](#_Toc159009867)

[8.0 Best practice 08 -Function apps should require FTPS only 22](#_Toc159009864)

[8.1 Description 22](#_Toc159009865)

[8.2 Control Domain 22](#_Toc159009866)

[8.3 Non-Compliance Message 22](#_Toc159009867)

[9.0 Best practice 09 -App Service apps should have resource logs enabled 22](#_Toc159009864)

[9.1 Description 22](#_Toc159009865)

[9.2 Control Domain 22](#_Toc159009866)

[9.3 Non-Compliance Message 22](#_Toc159009867)

[10.0 Best practice 10 - App service must be configured with Vnet Integration 22](#_Toc159009864)

[10.1 Description 22](#_Toc159009865)

[10.2 Control Domain 22](#_Toc159009866)

[10.3 Non-Compliance Message 22](#_Toc159009867)

[11.0 Best practice 11 - App Service apps should have remote debugging turned off 22](#_Toc159009864)

[11.1 Description 22](#_Toc159009865)

[11.2 Control Domain 22](#_Toc159009866)

[11.3 Non-Compliance Message 22](#_Toc159009867)

[12.0 Best practice 12 - App Service apps should not have CORS configured to allow every resource to access your apps 22](#_Toc159009864)

[12.1 Description 22](#_Toc159009865)

[12.2 Control Domain 22](#_Toc159009866)

[12.3 Non-Compliance Message 22](#_Toc159009867)

[13.0 Best practice 13 - Function apps should have remote debugging turned off 22](#_Toc159009864)

[13.1 Description 22](#_Toc159009865)

[13.2 Control Domain 22](#_Toc159009866)

[13.3 Non-Compliance Message 22](#_Toc159009867)

[14.0 Best practice 14 - Function apps should not have CORS configured to allow every resource to access your app 22](#_Toc159009864)

[14.1 Description 22](#_Toc159009865)

[14.2 Control Domain 22](#_Toc159009866)

[14.3 Non-Compliance Message 22](#_Toc159009867)

[15.0 Best practice 15 - Azure Defender for App Service should be enabled 22](#_Toc159009864)

[15.1 Description 22](#_Toc159009865)

[15.2 Control Domain 22](#_Toc159009866)

[15.3 Non-Compliance Message 22](#_Toc159009867)

[16.0 Best practice 16 - App Service apps should have resource logs enabled. 22](#_Toc159009864)

[16.1 Description 22](#_Toc159009865)

[16.2 Control Domain 22](#_Toc159009866)

[16.3 Non-Compliance Message 22](#_Toc159009867)

[17.0 Best practice 17 - Ensure that App service ingress/egress route paths to from the internet are internally routed. 22](#_Toc159009864)

[17.1 Description 22](#_Toc159009865)

[17.2 Control Domain 22](#_Toc159009866)

[17.3 Non-Compliance Message 22](#_Toc159009867)

[18.0 Appendix 29](#_Toc159009871)

[18.1 Abbreviations 29](#_Toc159009872)

[19.0 Reference Document links 30](#_Toc159009873)

# **Overview**

Azure App Service are a key component of Microsoft Azure's Infrastructure as a Service (IaaS) offering. They provide on-demand computing resources in the form of virtualized hardware, allowing you to run Windows or Linux-based applications and workloads in the cloud. Here's an overview of Azure Virtual Machines. The best practice of Azure Policy will ensure the ELC Cloud operations team to adhere to the ELC Global information security policy guidelines respect to the Cloud Security and follow the Azure App Service Security policy. This procedure enables the technology controls and processes needed to ensure transparency and auditability across the technology environment, which will empower ELC’s ability to perform investigations, regulatory audits, and incident and problem management to make sure the best practices are followed adhered as per the regulatory standards.

# **Purpose and Scope**

As per the ELC’s Global Information Security, Adopting the Azure Security benchmarks and the Azure Security Policy framework to Secure ELC Cloud services by creating and implementing strong Azure security policies in the Azure services for App Service in the cloud environment through the Azure security policy to protect and secure the instances, workload running through the App service. Azure Security benchmarks can be referred in the Appendix.

# **Best Practice 01 - App Service apps should use the latest TLS version**

## Description

Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, or enhance speed. Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, if any, and/or new functionalities of 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

## Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to App Service apps should use the latest TLS version. Please Notify to **'elcitprod@service-now.com'** for any non-compliance or assistance required.

# **Best Practice 02 - [Function apps should use the latest TLS version](https://portal.azure.com/" \l "blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Ff9d614c5-c173-4d56-95a7-b4437057d193" \t "_blank)**

## Description

Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for Function apps to take advantage of security fixes, if any, and/or new functionalities of 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

## Non-Compliance

MessageIn accordance with ELC IT-Security & Compliance, it is recommended to [Function apps should use the latest TLS version](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Ff9d614c5-c173-4d56-95a7-b4437057d193). Please Notify to **'elcitprod@service-now.com'** for any non-compliance or assistance required.

# **Best Practice 03 - App Service apps should use managed identity**

## Description

## Use a managed identity for enhanced authentication security

## 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-VM-3.7.2 -** Azure Security Policy Standard Document

## Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to App Service apps should use managed identity . Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 04 - Function apps should use managed identity.**

## Description

## Use a managed identity for enhanced authentication security

## 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

## Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to Function apps should use managed identity . Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 05 - App Service apps should only be accessible over HTTPS.**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to App Service apps should only be accessible over HTTPS. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - Function apps should only be accessible over HTTPS.**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **Function apps should only be accessible over HTTPS**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - App Service apps should require FTPS only.**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **App Service apps should require FTPS only**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - Function apps should require FTPS.**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **Function apps should require FTPS**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - App Service apps should have resource logs enabled only .**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **App Service apps should have resource logs enabled only** . Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - App service must be configured with Vnet Integration.**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **App service must be configured with Vnet Integration**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **0 Best Practice** 06 **- App Service apps should have remote debugging turned off**

# Description

## 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-VM-3.7.4-** Azure Security Policy Standard Document

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **App Service apps should have remote debugging turned off**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - App Service apps should not have CORS configured to allow every resource to access your apps**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **App Service apps should not have CORS configured to allow every resource to access your apps**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - Function apps should have remote debugging turned off**

## Description

## 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-VM-3.7.5 -** Azure Security Policy Standard Document

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **Function apps should have remote debugging turned off.** Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - Function apps should not have CORS configured to allow every resource to access your apps**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **Function apps should not have CORS configured to allow every resource to access your apps**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - Azure Defender for App Service should be enabled**

## Description

## 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,

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **Azure Defender for App Service should be enabled**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - App Service apps should have resource logs enabled.**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to **App Service apps should have resource logs enabled.**Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Best Practice 06 - Ensure that App service ingress/egress route paths to from the internet are internally routed.**

## Description

## 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

Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to  **Ensure that App service ingress/egress route paths to from the internet are internally routed.**. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **Appendix**

## Abbreviations

|  |  |
| --- | --- |
| **Abbreviations** | **Descriptions** |
| **CIS** | Center for Internet Security |
| **CMMC** | Cybersecurity Maturity Model Certification |
| **VM** | Virtual Machine |
| **IoT** | Internet of Things |
| **NIST** | National Institute of Standards and Technology |
| **NA** | Not Applicable |

# **Reference Document links**

* Azure Security Benchmark 3.0

[Overview of the Azure Security Benchmark v3 | Microsoft Learn](https://learn.microsoft.com/en-us/security/benchmark/azure/overview-v3)

* Regulatory Compliance

[Regulatory Compliance details for ISO 27001:2013 - Azure Policy | Microsoft Learn](https://learn.microsoft.com/en-us/azure/governance/policy/samples/iso-27001#compliance)