**ELC – Virtual Machine- 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 - Azure Backup should be enabled for linux Virtual Machines. 5](#_Toc159009836)

[1.1 Description 5](#_Toc159009837)

[1.2 Control Domain 5](#_Toc159009838)

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

[1.4 Policy Definition 5](#_Toc159009840)

[1.5 Error Details 6](#_Toc159009841)

[1.6 Exceptions 7](#_Toc159009842)

[2.0 Best Practice 02 - Linux machines that have accounts without passwords. 8](#_Toc159009843)

[2.1 Description 8](#_Toc159009844)

[2.2 Control Domain 8](#_Toc159009845)

[2.3 Non-Compliance 8](#_Toc159009846)

[2.4 Policy Definition 8](#_Toc159009847)

[2.5 Error Details 11](#_Toc159009848)

[2.6 Exceptions 12](#_Toc159009849)

[3.0 Best practice 03 - Authentication to Linux machines should require SSH keys. 13](#_Toc159009850)

[3.1 Description 13](#_Toc159009851)

[3.2 Control Domain 13](#_Toc159009852)

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

[3.4 Policy Definition 13](#_Toc159009854)

[3.5 Error Details 18](#_Toc159009855)

[3.6 Exceptions 18](#_Toc159009856)

[4.0 Best practice 04 - Boot Diagnostics should be enabled on Linux virtual machines. 19](#_Toc159009857)

[4.1 Description 19](#_Toc159009858)

[4.2 Control Domain 19](#_Toc159009859)

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

[4.4 Policy Definition 19](#_Toc159009861)

[4.5 Error Details 20](#_Toc159009862)

[4.6 Exceptions 21](#_Toc159009863)

[5.0 Best practice 05 - A managed identity should be enabled on your machine. 22](#_Toc159009864)

[5.1 Description 22](#_Toc159009865)

[5.2 Control Domain 22](#_Toc159009866)

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

[5.4 Policy Definition 22](#_Toc159009868)

[5.5 Error Details 23](#_Toc159009869)

[5.6 Exceptions 24](#_Toc159009870)

[6.0 Appendix 29](#_Toc159009871)

[6.1 Abbreviations 29](#_Toc159009872)

[7.0 Reference Document links 30](#_Toc159009873)

# **Overview**

Azure Virtual Machines (VMs) 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 Virtual machine 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 Virtual machines in the cloud environment through the Azure security policy to protect and secure the instances, workload running through the VM. Azure Security benchmarks can be referred in the Appendix.

# **Best Practice 01 - Azure Backup should be enabled for linux Virtual Machines.**

## Description

Ensure protection of your Azure Virtual Machines by enabling Azure Backup. Azure Backup is a secure and cost-effective data protection solution for Azure.

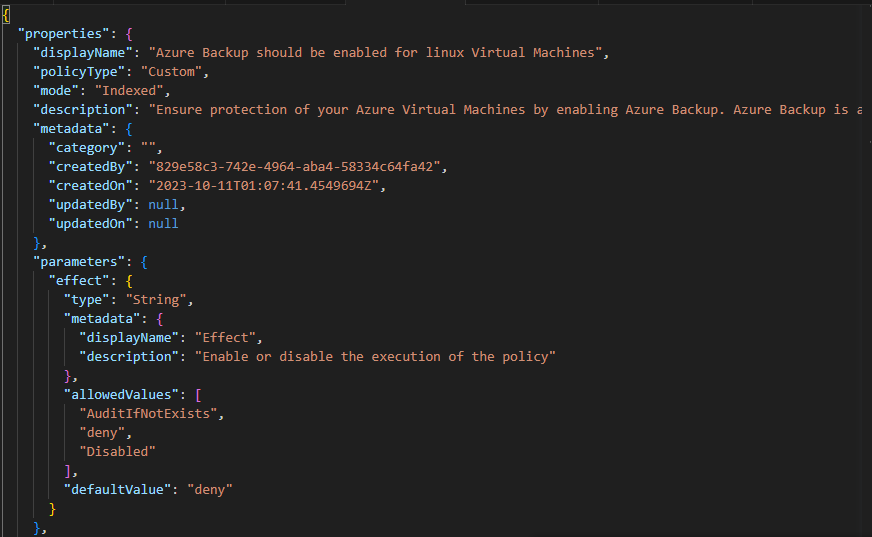
## Control Domain

NIST\_SP\_800-53\_R5, CMMC Level 3

## Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to enable the Azure Backup for Virtual Machines. Please Notify to **'elcitprod@service-now.com'** for any non-compliance or assistance required.

## Policy Definition



A screen shot of a computer program

Description automatically generated

## Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

A screenshot of a computer

Description automatically generated

Figure 1 - Validation Failed error summary details.

## Exceptions

While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **Best Practice 02 - Linux machines that have accounts without passwords.**

## Description

Machines are non-compliant if Linux machines that have accounts without passwords.

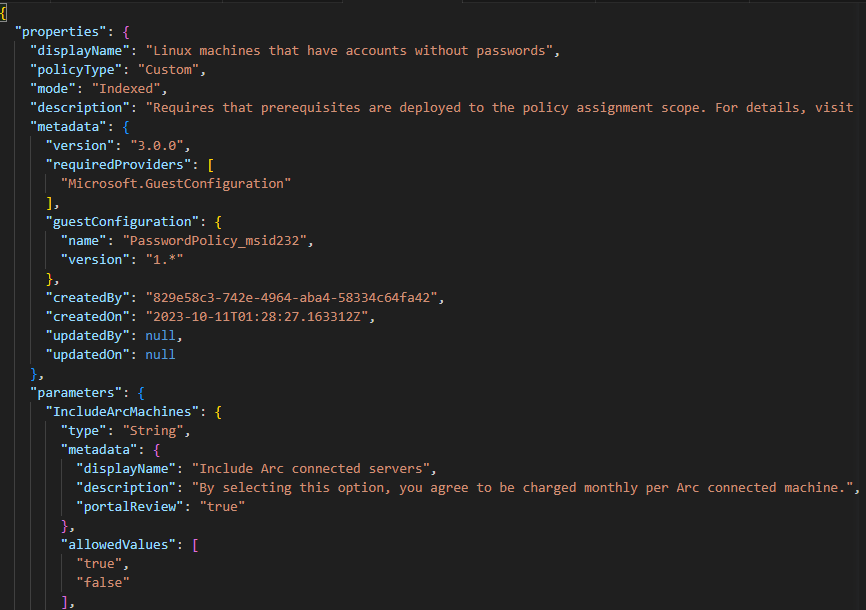
## Control Domain

NIST\_SP\_800-53\_R5, ISO27001 – 2013, CMMC Level 3

## Non-Compliance

MessageIn accordance with ELC IT-Security & Compliance, it is recommended to create a password for the virtual machine. Please Notify to **'elcitprod@service-now.com'** for any non-compliance or assistance required.

## Policy Definition



A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

## Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

A close-up of a computer screen

Description automatically generated

Figure 1 - Validation Failed error summary details.

## Exceptions

While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a login box

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **Best practice 03 - Authentication to Linux machines should require SSH keys.**

## Description

Machines are non-compliant if Linux machines that have accounts without SSH keys.

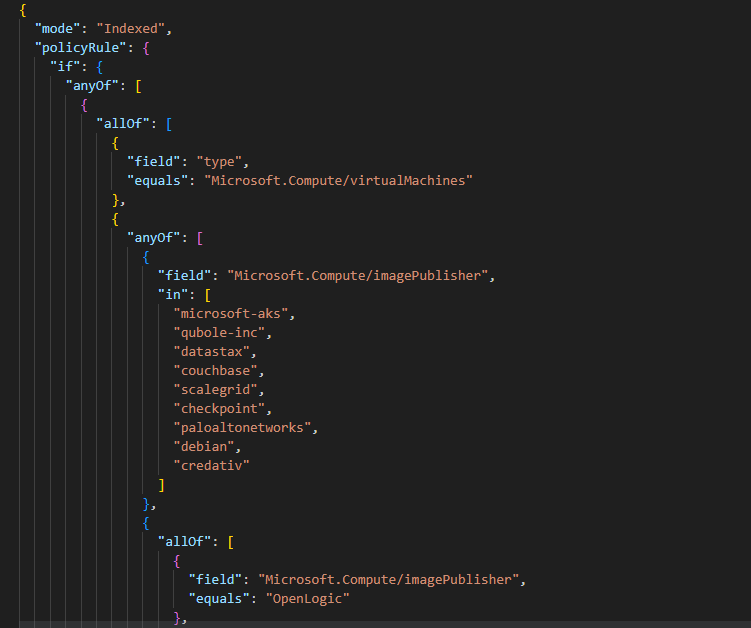
## Control Domain

NIST\_SP\_800-53\_R5, [Azure\_Security\_Benchmark\_v3.0](https://www.azadvertizer.net/complianceControlsAggregated.html#%7B%22col_0%22%3A%7B%22flt%22%3A%22Azure_Security_Benchmark_v3.0%22%7D%7D), CMMC 2.0 Level 2

## Non-Compliance Message

In accordance with ELC IT-Security & Compliance, it is recommended to create a SSH keys for the virtual machine to access. Please Notify to **'elcitprod@service-now.com'** for any non-compliance or assistance required.

## Policy Definition



A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A computer screen shot of a program code

Description automatically generated

## Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

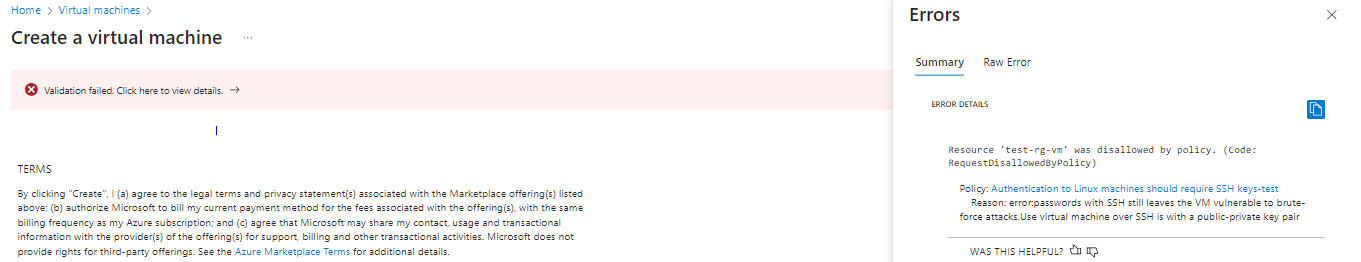


Figure 1 - Validation Failed error summary details.

## Exceptions

While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **Best practice 04 - Boot Diagnostics should be enabled on Linux virtual machines.**

## Description

Machines are non-compliant if Boot Diagnostics on disable in Linux virtual machines.

## Control Domain

[Azure\_Security\_Benchmark\_v3.0](https://www.azadvertizer.net/complianceControlsAggregated.html#%7B%22col_0%22%3A%7B%22flt%22%3A%22Azure_Security_Benchmark_v3.0%22%7D%7D).

## Non-Compliance Message

In accordance with ELC IT-Security & Compliance, it is recommended to enable the Boot Diagnostics on virtual machines. Please Notify to **'elcitprod@service-now.com'** for any non-compliance or assistance required.

## Policy Definition

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

## Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

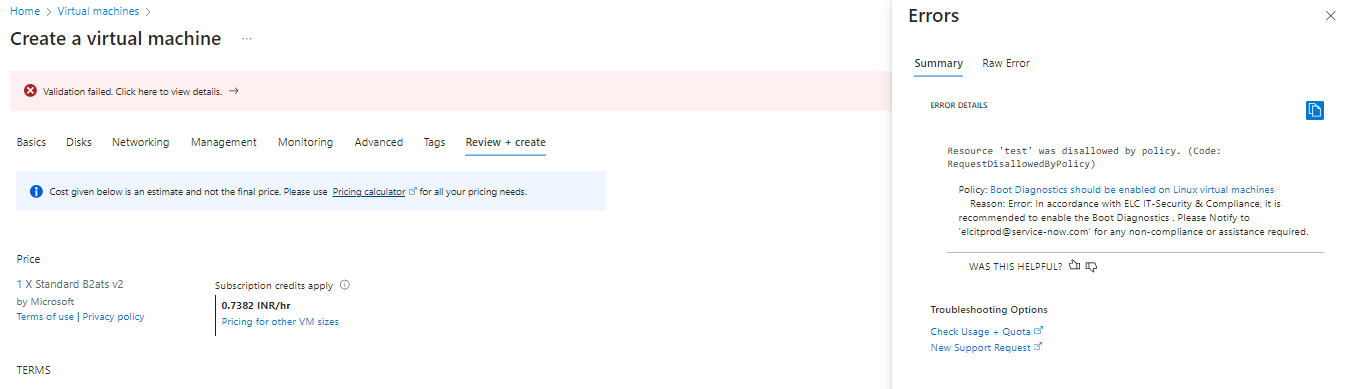


Figure 1 - Validation Failed error summary details.

## Exceptions

While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

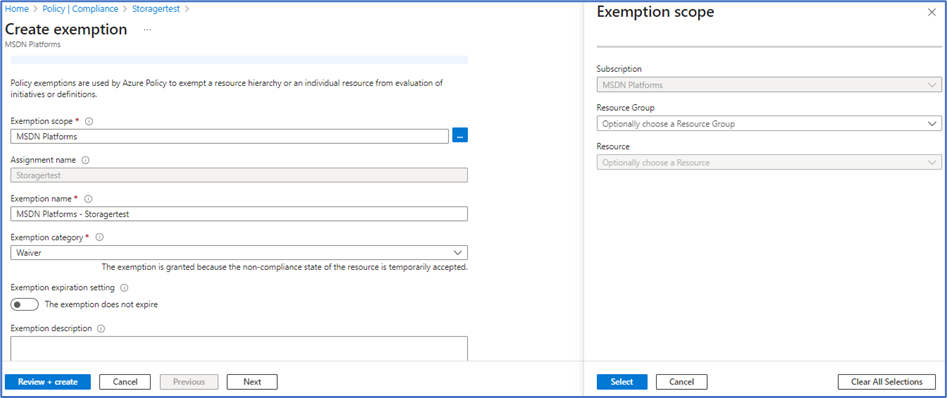


Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **Best practice 05 - A managed identity should be enabled on your machine.**

## Description

Machines are non-compliant Resources managed by Auto manage should have a managed identity.

## Control Domain

NIST\_SP\_800-53\_R5, [Azure\_Security\_Benchmark\_v3.0](https://www.azadvertizer.net/complianceControlsAggregated.html#%7B%22col_0%22%3A%7B%22flt%22%3A%22Azure_Security_Benchmark_v3.0%22%7D%7D).

## Non-Compliance Message

In accordance with ELC IT-Security & Compliance, it is recommended to managed identity should be enabled on your machine. Please Notify to **'elcitprod@service-now.com'** for any non-compliance or assistance required.

## Policy Definition

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

## Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.



Figure 1 - Validation Failed error summary details.

## Exceptions

While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **7.0 Best practice 07 - All Data in transit should be encrypted.**

**Description:**

Protect the data in transit against 'out of band' attacks (such as traffic capture) using encryption to ensure that attackers cannot easily read or modify the data. For remote management of VMs, use SSH (for Linux) or RDP/TLS (for Windows) instead of an unencrypted protocol.

**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

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " All Data in transit should be encrypted.". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

## 7.0 Best practice 07 - Leverage sanctioned managed hosts to perform operational/ privileged functions.

**Description:**

Jump servers is Secured, isolated workstations are critically important for the security of sensitive roles like administrator, developer, and critical service operator.

**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

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " Leverage sanctioned managed hosts to perform operational/ privileged functions ". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

## 8.0 Best practice 08 - Private link to external 3rd party is DENIED by default.

**Description:**

Secure cloud services by establishing a private access point for the resources. You should also disable or restrict access to the public network when possible. Any exception to this control should be reviewed and go through approval process.

**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

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " Private link to external 3rd party is DENIED by default ". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

## 9.0 Best practice 09 - All privileged access for local & domain accounts should go through the ELC sanctioned privileged access management solution

**Description:**

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

**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   

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " All privileged access for local & domain accounts should go through the ELC sanctioned privileged access management solution ". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

## 10.0 Best practice 10 - Ensure that 'OS disks' are encrypted

**Description:**

Ensure that OS disks (boot volumes) are encrypted, where possible.

**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

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " Ensure that 'OS disks' are encrypted ". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

## 11.0 Best practice 11 - Ensure that 'Data disks' are encrypted

**Description:**

Ensure that data disks (non-boot volumes) are encrypted, where possible.

**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

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " Ensure that 'Data disks' are encrypted ". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

## 12.0 Best practice 12 - Virtual Machines should be deployed with ELC Sanctioned Image

**Description:**

Virtual Machines should be deployed with all the security agents and latest security updates and with all the security hardening guidelines.

**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   

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " Virtual Machines should be deployed with ELC Sanctioned Image ". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

## 14.0 Best practice 14 - Virtual machines should be migrated to new Azure Resource Manager resources.

**Description:**

Use new Azure info Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and 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   

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " Virtual machines should be migrated to new Azure Resource Manager resources. ". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

## 15.0 Best practice 15 - All Virtual Machines should be under Frequently Managed Update Schedule

**Description:**

Audit whether there are any missing system security updates and critical updates that should be installed to ensure that your Windows and Linux virtual machine are secure.

**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   

**Non-Compliance Error Message:**

In accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to " All Virtual Machines should be under Frequently Managed Update Schedule ". 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)

* <https://elcompanies.sharepoint.com/:f:/s/CloudSecurity/EijeYgvn7QJMroSKfXcXaSUBX8h5fditQG2ZMtJHPpNSzQ?e=wwhdsH>
* 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)