**ELC – Azure Security Policies Management and Process Documentation**

Text, logo

Description automatically generated, Picture

**By**

A logo with colorful dots

Description automatically generated, Picture

**Wipro Technologies**

**10-June-2025**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Revision** | **Description of Change** | **Reason for Change** | **Reviewed By** |
| 1.0 | 10-June-25 | Initial Draft | NA |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Author/Reviewer/Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Designation** | **Responsibility** | **Date** |
| Felix Jebamani & Sivarami Reddy | Lead Consultant & Consultant | Authors | 10th June 2025 | |
| Kannan Kuppusamy | Technical Lead | Reviewer | 19th June 2025 | |
| Felix Jebamani | Lead Consultant | Reviewer | 19th June 2025 | |
| Salama Omar | Lead, Cloud Cybersecurity Engineer | Reviewer | 26th June 2025 | |
| Jamshid Abedi | ELC ED, Global Head of   Security Engineer | Approver | 26th June 2025 | |

Table of Contents

[1. Overview 3](#_Toc202217358)

[2. Objective and Scope of the Document 3](#_Toc202217359)

[3. Azure Policy 3](#_Toc202217360)

[4. Azure policies compliance standards 4](#_Toc202217361)

[5. ELC Cloud Security standard Controls 4](#_Toc202217362)

[6. Azure policies ID alignment - ELC CSSC (Cloud Security Standard Control) 4](#_Toc202217363)

[7. Azure Policy compliance Monitoring Process 7](#_Toc202217364)

[7.1 Policy Assignment 7](#_Toc202217365)

[7.2 Compliance Evaluation 7](#_Toc202217366)

[7.3 Monitoring Compliance 7](#_Toc202217367)

[8. Azure policy compliance Reports and Automation 8](#_Toc202217368)

[8.1 Azure policy Non-compliance Remediation Tasks 8](#_Toc202217369)

[8.2 Azure Remediation Ticketing Process 8](#_Toc202217370)

[9. Azure policy Exemption Process 9](#_Toc202217371)

[10. Azure policy Enforcement Approach 9](#_Toc202217372)

[10.1 Policy Definition 9](#_Toc202217373)

[12. Reference Documents 11](#_Toc202217374)

# Overview

This document outlines the workflow for identifying, analyzing, and tracking the Azure Policies from Cloud Security Hardening Standard Document deployed across the Azure Policy. It covers the identification of applicable policies from the Cloud Security Hardening Standard; detailed analysis of policy deployed across the Azure global.

# Objective and Scope of the Document

To establish a structured and process for identifying Azure Policies that align with the Cloud Security Hardening Standard, analyzing their impact and applicability, and tracking their implementation to ensure consistent compliance and improved security posture across Azure environments.

# Azure Policy

As part of our cloud governance and compliance initiative, we had successfully deployed a total of 64 Azure Policies within the ELC Azure global. To ensure traceability and alignment with our internal security and compliance framework, we developed a comprehensive tracking sheet. This document maps each Azure Polices to its corresponding cloud security standard policies deployed, associated to its services from the Cloud Security Standard Control Document, and the specific page number where the control is defined. This structured approach enables easier auditing, enhances visibility into policy enforcement, and supports ongoing compliance monitoring efforts.

# Azure policies compliance standards

Azure policies are deployed through the following compliance standards aligned with the Microsoft Cloud Security Benchmarks and are expected to be maintained and upheld by the ELC native cloud environment and please refer to the Session number **3.0 Standards** in ELC Cloud Security Hardening Document.

• 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

• Azure Security Policy standard control document v2.1.0

• CIS Controls v7.1, CIS Controls V8

• PCI-DSS v3.2.1

# ELC Cloud Security standard Controls

The purpose of this cloud security 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.

# Azure policies ID alignment - ELC CSSC (Cloud Security Standard Control)

Azure policies are deployed with defined 64 Azure policies in ELC Azure global in the audit mode across the tenants, these policies are deployed in accordance and aligned with the cloud security standard controls, those corresponding reference policy ids are shown in the attached excel.



# Azure Policy compliance Monitoring Process

Azure Policy monitoring ensures that the ELC Azure cloud resources comply with organizational standards by:

**Auditing** existing resources through the ELC 62 custom policies as per the ELC cloud security standard controls

**Enforcing** those 62 policies across the ELC Azure cloud in a phase vice method as per the best practices.

**Tracking & monitoring** the compliance & non-compliance of Azure resources are carried out by the Azure and generate the reports of compliant and non-complaint resources corresponding to the Azure policies deployed over

To monitor Azure Policy compliance, Azure structured process that ensures the cloud resources stay aligned with organizational or regulatory standards. Some of its monitoring methods are shown below

# 7.1 Policy Assignment

Assign policies or initiatives (groups of policies) to scopes like subscriptions, resource groups, or management groups. Policies can Audit, enforce & exempt rules (e.g., deny non-compliant deployments) or audit existing resources.

# 7.2 Compliance Evaluation

Azure automatically evaluates resources against assigned policies to identify the resources with are compliant or non-compliant. Evaluation is triggered by - New policy initiative assignment, Updates to existing policies, Resource creation or modification, Subscription movement within management groups

# 7.3 Monitoring Compliance

Azure policy monitors compliance using several tools: Azure Portal: Through the Azure portal, Reports can be viewed under compliance state under Policy > Compliance.

Azure Monitor Logs: It Send policy data to Log Analytics for custom dashboards and alerts. This is also on the methods to monitor the azure policies.

Azure Resource Graph: One of the other methods using Azure resource graph to Query compliance data at scale also available. Complaints reports will be shown based on the category as Critical, High, Medium due to the severity of the non-compliant reports.

# Azure policy compliance Reports and Automation

Azure compliance status reports can be generated using the alert-driven method using Azure monitor and automation mechanisms through various methods, some evaluations are shown are

Set up “event-driven alerts” using Azure Monitor to notify you when compliance states change.

Automating the reports and automation process through the customized scripts using Python in a Daily, Weekly, Monthly basis as per the requirements. Reports can be generated based on the automated method through the schedule tasks and handled by the respective team for resolution & remediation.

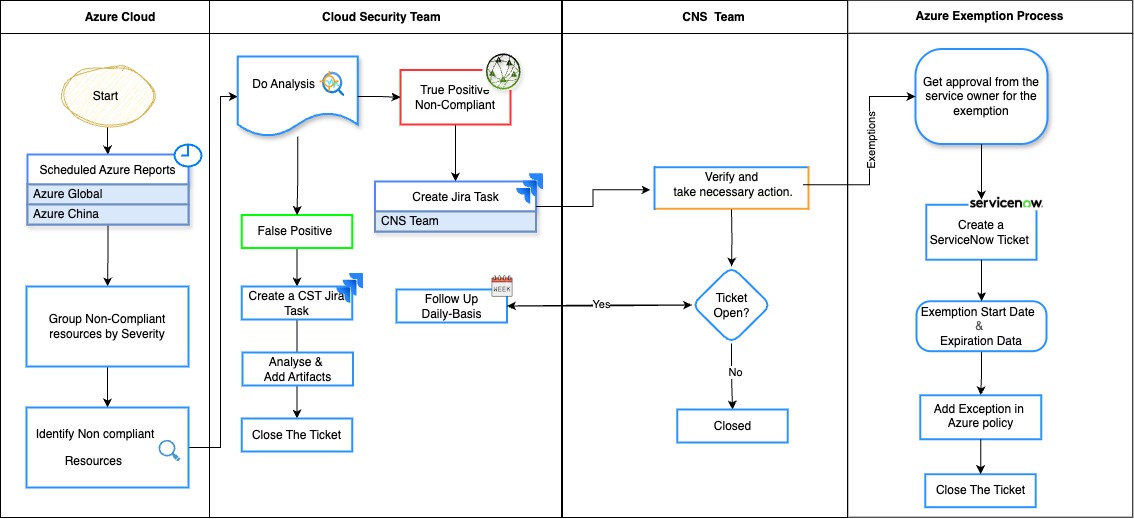
# 8.1 Azure policy Non-compliance Remediation Tasks

Azure policy compliance status may change automatically based on the remediation tasks carried out by the relevant ELC stakeholder and responsible teams where various teams may be involved on the remediation process.

# 8.2 Azure Remediation Ticketing Process

Remediation and mitigation of azure non-compliance resources are carried out by the below following methods. Once the report was generated from the portal. ELC cloud security team will validate the True and False positive on the resources shown as non-compliant and share the true positives to Cloud Ops team or the respective owners for remediating the non-compliant resources. Tickets will be created and assigned to the Cloud Ops team through the SNOW / JIRA along with the identified non-compliant resources.

The non-complaints resources reports are categorized as Critical, High, medium and shown based on the severity. The remediation process from the initial to the remediation will be followed using the below flowchart as shown below



Azure security policy process flow chart

# Azure policy Exemption Process

Azure policy exemptions allow you to temporarily or permanently exclude specific resources or scopes from policy enforcement—without removing the policy itself. This is especially useful when certain resources need to exempt from enforcement policy due to business needs. Exemption of azure resources go through process as shown in the flow chart. Once we receive the request to exempt the resource, Cloud security team will raise the Azure exemption request through the SNOW, Once the SNOW was approved by the stakeholders, Cloud security team will exempt the resources in the Azure policy exemption.

# Azure policy Enforcement Approach

Azure Policy’s enforcement approach is all about ensuring your Azure resources stay compliant with organizational or regulatory standards — automatically and at scale by applying the enforcement of ELC 62 Azure policies in the enforcement mode. Here's how it works

# Policy Definition

A policy definition describes the condition under which a resource is evaluated and the effect that should be enforced.

Common effects include:

Deny: Blocks non-compliant resource creation or updates.

Audit: Flags non-compliant resources without blocking.

DeployIfNotExists : Automatically deploys a required resource if missing.

Modify: Alters resource properties during deployment.

10.2 Policy Assignment

Policies are assigned to a scope as per the business requirements through the management group, subscription, resource group, or individual resource.

Enforcement policy assignment defines exclusions within the scope to skip certain resources.

10.3 Evaluation and Enforcement

Azure continuously evaluates resources against assigned policies:

On resource creation or update, when policies are assigned or updated periodically in the background to ensure that the azure resources are enforced with the policies corresponding with their service and allows if the resources are compliant and blocks if it is non-compliant.

If a resource violates a policy with a `Deny` effect, the deployment is blocked.

If `DeployIfNotExists` or `Modify` is used, Azure can remediate the resource automatically.

10.4 Remediation Tasks

For existing non-compliant resources, remediation tasks will take effect immediately in an automated method to bring them into compliance.

Such tasks use the same logic as `DeployIfNotExists` or `Modify` effects.

1. Azure Policy enforcement phase wise approach

Azure policy enforcement approach will take place in a phase wise method based on the criticality of the business continuity of applications, services or resources that are running in the azure environments. As part of the best practice, ELC Cloud security team will focus on the services that are exposed to public internet as the first phase of approach.

The enforcement approach is to bring down the non-compliant resources from highest percent of non-compliance to the minimum non-compliant percentage and providing exemption on critical applications that are considered as non-compliant due to the business requirements.

Below is the example of deployed azure policy that defines the Azure services that are exposed to public Internet.



Thus, the azure enforcement approach would be planned in a phase wise method to minimum the business impact and make sure the ELC compliance and security IT guidelines are followed and adhered as per the ELC cloud security standard controls.

# Reference Documents

* [Azure\_Policies\_with\_Control\_ID](https://elcompanies.sharepoint.com/:f:/r/sites/CloudSecurity/Shared%20Documents/General/Azure_Policies_with_Control_ID?csf=1&web=1&e=ZeNtwr)
* [ELC-ECR-035 Cloud Security Hardening Standard](https://elcompanies.sharepoint.com/:b:/r/sites/CV-IT-ECR/Shared%20Documents/ELC-ECR-035%20Cloud%20Security%20Hardening%20Standard.pdf?csf=1&web=1&e=PoUmnL)