Comprehensive Implementation Guide: PRJ-AZURE-SEC-060 - Azure Policy Governance Framework

1. Project Overview

The **PRJ-AZURE-SEC-060: Azure Policy Governance Framework** project is a foundational security initiative designed to establish a robust, automated, and centralized security posture across an entire Azure Management Group (MG). This framework leverages the native capabilities of Azure to enforce security standards by design, ensuring that all current and future subscriptions within the defined scope are automatically onboarded to essential security services.

The primary objective is to eliminate security blind spots and ensure compliance from the moment a new subscription or resource is provisioned. This is achieved through the strategic integration of three core Azure services:

1. **Azure Policy:** Used as the governance backbone to enforce the deployment and configuration of security services at the Management Group level. This ensures a non-bypassable, top-down security mandate.
2. **Microsoft Defender for Cloud (MDC):** Provides Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) capabilities. It continuously assesses the security state of resources and generates security alerts.
3. **Azure Sentinel (SIEM/SOAR):** Acts as the centralized Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platform. It ingests alerts from MDC, correlates them with other data sources, and facilitates automated incident response.

By assigning a policy at the Management Group level, the solution ensures unified security posture management, advanced threat detection, and automated incident response across the entire organizational hierarchy.

2. Business Context

In today's dynamic cloud environment, organizations face a constant barrage of sophisticated threats, including **ransomware**, **phishing**, and **Advanced Persistent Threats (APTs)**. Traditional, siloed security operations are often overwhelmed by the sheer volume and velocity of cloud data, leading to significant security gaps and compliance failures.

The Problem Addressed

The core challenges this framework solves are:

- **Lack of Unified Security Monitoring:** Security tools are often deployed inconsistently across subscriptions, leading to fragmented visibility and a high risk of missing critical security events.
- **Scale and Velocity:** Manual security operations cannot keep pace with the rapid deployment of resources in the cloud, resulting in non-compliant or unprotected resources being exposed for extended periods.
- **Reactive Security:** Security teams spend excessive time reacting to incidents rather than proactively managing risk and improving posture.

Quantified Business Value and ROI

The **Azure Policy Governance Framework** delivers substantial, quantifiable business value by shifting the security paradigm from reactive to proactive and automated.

Value Proposition	Description	Quantified Impact
Unified Security Posture	A single platform (Sentinel) for all Azure security monitoring and management, eliminating silos and providing a holistic view of the security landscape.	**100%** coverage of all in-scope subscriptions for foundational security monitoring.
Automated Incident Response (SOAR)	Integrated SOAR playbooks automatically respond to common threats (e.g., isolating an infected VM), significantly reducing human intervention.	**Up to 80%** reduction in Mean Time To Respond (MTTR), directly mitigating financial and reputational damage from breaches.
Compliance by Design	Azure Policy enforces security service enablement at the Management Group level, ensuring every new subscription is compliant from day one.	**Near-zero** non-compliant subscriptions for foundational security services, reducing audit failure risk.
Risk Mitigation	Continuous, AI-powered threat detection and correlation across all resources.	**Reduced financial loss** from security incidents, with estimated savings of **$3.86 million** (average cost of a data breach in 2023) per avoided major incident.
Operational Efficiency	Centralization of security data and automation of repetitive tasks frees up security analysts to focus on high-value threat hunting and strategic initiatives.	**30-40%** increase in Security Operations Center (SOC) analyst efficiency.

The **80% MTTR reduction** is a critical metric. It is achieved because the framework immediately ingests security alerts from MDC into Sentinel. Sentinel's SOAR capabilities (Logic Apps or Azure Functions) are then triggered by high-fidelity incidents, allowing for actions like automatically disabling a compromised user account, isolating a virtual machine, or blocking a malicious IP address—all within seconds or minutes, a task that would take a human analyst hours.

3. GRC Mapping

This framework is a cornerstone for achieving and maintaining various Governance, Risk, and Compliance (GRC) requirements. By enforcing security controls at the highest level of the Azure hierarchy, it provides robust, auditable evidence of compliance.

GRC Component	Specific Framework Mapping	Control Description
NIST Cybersecurity Framework (CSF)	**Detect (DE.AE-1, DE.CM-1)** and **Respond (RS.RP-1)**	The framework provides continuous monitoring (DE.CM-1) and baseline analysis (DE.AE-1) via MDC and Sentinel. The SOAR playbooks directly support the response planning and execution (RS.RP-1).
ISO/IEC 27001:2022	**A.5.27 (Logging and monitoring)** and **A.5.28 (Secure coding)**	Centralized logging and monitoring via Sentinel (A.5.27) ensures all security events are captured. The enforcement of MDC provides continuous vulnerability management, indirectly supporting secure development practices.
SOC 2 Trust Services Criteria	**CC7.2 (System Monitoring)** and **CC7.3 (Security Events)**	The integration of MDC and Sentinel directly addresses the need for continuous monitoring (CC7.2) and the identification, documentation, and response to security events (CC7.3).
GDPR (General Data Protection Regulation)	**Article 32 (Security of processing)** and **Article 33 (Notification of a personal data breach)**	The automated threat detection and rapid response capabilities ensure appropriate technical and organizational measures (Article 32). The auditable incident records in Sentinel support timely breach notification (Article 33).
PCI DSS (Payment Card Industry Data Security Standard)	**Requirement 10 (Track and monitor all access to network resources and cardholder data)**	Sentinel's centralized logging and correlation capabilities provide the necessary audit trails and monitoring to meet this critical requirement.
MITRE ATT&CK	**Cloud Tactics and Techniques**	MDC and Sentinel's threat intelligence and behavioral analytics are specifically designed to detect techniques mapped to the MITRE ATT&CK framework, such as Initial Access, Execution, and Persistence in cloud environments.

The auditable evidence generated by this framework—including security alerts, incident records, SOAR execution logs, and security posture assessments—is essential

for external and internal audits, proving due diligence in security governance.

4. Prerequisites

Successful deployment requires specific accounts, permissions, and tools to be in place.

Required Tools

1. **Azure CLI:** The Azure Command-Line Interface must be installed and configured on the deployment workstation.
2. **Jq (Optional but Recommended):** A lightweight and flexible command-line JSON processor, useful for parsing complex Azure CLI outputs.

Required Permissions

The user account executing the deployment must have the following role assignments:

- **Owner** or **User Access Administrator** role at the **target Management Group scope**. This is necessary to assign the Azure Policy and to create the required Role Assignment for the Policy's Managed Identity.
- **Contributor** role on the **target subscription** where the Azure Sentinel Log Analytics Workspace will be deployed (Phase 2).

Environment Setup

1. **Login to Azure CLI:**

   ```
   az login
   ```

2. **Set the Target Management Group ID:** Identify and set the ID of the Management Group that will be governed by this policy.

```
# Replace <YOUR_MG_ID> with your target MG ID
MG_ID="mg-corp-security"
```

3. **Register the `Microsoft.Security` Resource Provider:** This step ensures that the Management Group is ready to manage security settings for its child subscriptions.

```
az provider register --namespace Microsoft.Security --management-
group-id $MG_ID
```

5. Architecture Overview

The architecture employs a **top-down governance model** to ensure security controls are uniformly applied across the organization's Azure estate. The design is intentionally simple and relies on native Azure services for maximum integration and minimal overhead.

The central component is the **Azure Policy Assignment** at the Management Group (MG) level. This assignment acts as the enforcement mechanism, ensuring that all child subscriptions inherit the security mandate.

Architectural Flow:

1. **Policy Enforcement:** The Azure Policy is assigned to the **Management Group (`mg-corp-security`)**. This policy is a `DeployIfNotExists` (DINE) policy that checks if Microsoft Defender for Cloud is enabled on a subscription. If it is not, the policy triggers a remediation action.
2. **MDC Onboarding:** The remediation action, executed by a **System-Assigned Managed Identity** with the **Security Admin** role, enables the foundational tier of **Microsoft Defender for Cloud (MDC)** on the target **Subscription**.
3. **Data Generation:** Azure Resources (VMs, Storage Accounts, etc.) are continuously monitored by MDC. MDC generates **Security Alerts** and **Security Recommendations** based on its CSPM and CWPP capabilities.

4. **Centralized SIEM:** The **Azure Sentinel** instance, deployed in a dedicated resource group, is connected to MDC via a **Data Connector**. This connector streams all MDC security alerts into the Sentinel Log Analytics Workspace.
5. **Automated Response:** Sentinel's **SOAR Playbooks** (built using Azure Logic Apps or Azure Functions) are triggered by high-severity incidents. These playbooks execute automated remediation actions, such as isolating a resource or enriching the incident data, completing the security loop.

This model ensures that governance is centralized at the MG level, while security data is consolidated in a single, dedicated Sentinel instance for efficient monitoring and response.

6. Step-by-Step Implementation

The deployment is executed in two main, sequential phases: **Policy Enforcement** to enable MDC, and **SIEM/SOAR Deployment** to centralize monitoring with Azure Sentinel.

Phase 1: Policy Enforcement (Enable Microsoft Defender for Cloud)

This phase assigns the built-in policy to the Management Group and initiates a remediation task to onboard existing non-compliant subscriptions.

6.1. Define Configuration Variables

Set the variables for the policy assignment. The `POLICY_DEFINITION_ID` is for the built-in policy "Enable Microsoft Defender for Cloud on your subscription".

```
# --- Configuration Variables ---
MG_ID="mg-corp-security" # Target Management Group ID
POLICY_ASSIGNMENT_NAME="Enable-MDC-MG"
# Built-in: Enable Microsoft Defender for Cloud on your subscription
POLICY_DEFINITION_ID="/providers/Microsoft.Authorization/policyDefinitions/ac0
ddcf-4066-b451-6154267e8ad2"
LOCATION="eastus" # Location for the Managed Identity (must be a region)
# ------------------------------
```

6.2. Create Policy Assignment

Assign the policy to the Management Group. The `--mi-system-assigned` flag is crucial as it creates a Managed Identity required for the remediation task to perform actions on the child subscriptions.

```
echo "Creating Policy Assignment: $POLICY_ASSIGNMENT_NAME on MG: $MG_ID"

az policy assignment create \
    --name $POLICY_ASSIGNMENT_NAME \
    --display-name "Enable Microsoft Defender for Cloud on Management Group"
\
    --scope "/providers/Microsoft.Management/managementGroups/$MG_ID" \
    --policy-definition-id $POLICY_DEFINITION_ID \
    --mi-system-assigned \
    --location $LOCATION \
    --description "Enforces the enablement of Microsoft Defender for Cloud
on all child subscriptions."
```

6.3. Assign Managed Identity Permissions

The Managed Identity created in the previous step needs the necessary permissions to modify the security settings of the child subscriptions. The **Security Admin** role at the Management Group scope grants this capability.

```
echo "Retrieving Managed Identity Principal ID..."
# Retrieve the Principal ID of the newly created Managed Identity
PRINCIPAL_ID=$(az policy assignment show \
    --name $POLICY_ASSIGNMENT_NAME \
    --scope "/providers/Microsoft.Management/managementGroups/$MG_ID" \
    --query identity.principalId \
    --output tsv)

if [ -z "$PRINCIPAL_ID" ]; then
    echo "Error: Could not retrieve Principal ID for the Managed Identity.
Exiting."
    exit 1
fi

echo "Assigning 'Security Admin' role to Principal ID: $PRINCIPAL_ID at MG
scope."
# Assign the "Security Admin" role to the Managed Identity at the MG scope
az role assignment create \
    --assignee $PRINCIPAL_ID \
    --role "Security Admin" \
    --scope "/providers/Microsoft.Management/managementGroups/$MG_ID" \
    --description "Required for Azure Policy DINE effect to enable MDC on
child subscriptions."
```

6.4. Create Remediation Task

The policy assignment only ensures future compliance. The remediation task applies the policy to all existing non-compliant subscriptions under the Management Group.

```
echo "Creating Remediation Task to onboard existing subscriptions..."
az policy remediation create \
    --name "Remediate-MDC-MG" \
    --policy-assignment
"/providers/Microsoft.Management/managementGroups/$MG_ID/providers/Microsoft.A
\
    --resource-discovery-mode ExistingNonCompliant
```

Note: Remediation tasks can take several hours to complete, depending on the number of subscriptions.

Phase 2: SIEM/SOAR Deployment (Azure Sentinel)

This phase deploys the centralized Log Analytics Workspace, enables Azure Sentinel, and connects the MDC alerts to the SIEM.

6.5. Define Configuration Variables

Set the variables for the Sentinel deployment. The subscription ID is automatically retrieved.

```
# --- Configuration Variables ---
RG_NAME="rg-sentinel-security" # Resource Group for Sentinel
WORKSPACE_NAME="la-sentinel-sec-060" # Log Analytics Workspace Name
LOCATION="eastus" # Location for the Workspace
SUBSCRIPTION_ID=$(az account show --query id --output tsv)
# ------------------------------
```

6.6. Create Resource Group and Log Analytics Workspace

The Log Analytics Workspace is the data store for Sentinel. The `PerGB2018` SKU is used here, but the SKU should be chosen based on expected data volume.

```
echo "Creating Resource Group: $RG_NAME in $LOCATION"
az group create --name $RG_NAME --location $LOCATION

echo "Creating Log Analytics Workspace: $WORKSPACE_NAME"
az monitor log-analytics workspace create \
    --resource-group $RG_NAME \
    --workspace-name $WORKSPACE_NAME \
    --location $LOCATION \
    --sku PerGB2018
```

6.7. Enable Azure Sentinel

Sentinel is enabled on top of the Log Analytics Workspace using a REST API call, as the Azure CLI command for this is often a wrapper for the REST API.

```
echo "Enabling Azure Sentinel on Workspace: $WORKSPACE_NAME"
az rest --method PUT \
    --uri
"/subscriptions/$SUBSCRIPTION_ID/resourceGroups/$RG_NAME/providers/Microsoft.O
api-version=2020-01-01" \
    --body '{"properties": {}}'
```

6.8. Connect Microsoft Defender for Cloud Data Connector

This final step establishes the critical link, streaming all security alerts generated by MDC (Phase 1) into the new Sentinel workspace for centralized analysis and SOAR execution.

```
echo "Connecting Microsoft Defender for Cloud Data Connector..."
# Get the Workspace Resource ID
WORKSPACE_ID=$(az monitor log-analytics workspace show \
    --resource-group $RG_NAME \
    --workspace-name $WORKSPACE_NAME \
    --query id \
    --output tsv)

if [ -z "$WORKSPACE_ID" ]; then
    echo "Error: Could not retrieve Workspace ID. Exiting."
    exit 1
fi

# Connect the MDC Data Connector to Sentinel
# Note: The data connector is a resource at the subscription level, linking
to the workspace.
az rest --method PUT \
    --uri
"/subscriptions/$SUBSCRIPTION_ID/providers/Microsoft.SecurityInsights/dataConn
api-version=2020-01-01" \
    --body "{\"kind\": \"AzureSecurityCenter\", \"properties\":
{\"dataTypes\": {\"alerts\": {\"state\": \"Enabled\"}}, \"workspaceId\":
\"$WORKSPACE_ID\", \"subscriptionId\": \"$SUBSCRIPTION_ID\"}}"

echo "Deployment Complete. MDC is enforced via Policy, and alerts are
centralized in Sentinel."
```

7. Validation & Testing

After deployment, a rigorous validation process is necessary to confirm the framework is operational and correctly enforcing security standards.

7.1. Policy and Remediation Status Validation

1. **Verify Policy Assignment:** Confirm the policy is correctly assigned to the Management Group.

   ```
   az policy assignment show \
       --name $POLICY_ASSIGNMENT_NAME \
       --scope "/providers/Microsoft.Management/managementGroups/$MG_ID"
   \
   ```

   Expected Output: The `identity.principalId` field should be populated, and `policyDefinitionId` should match the expected ID.

2. **Check Remediation Status:** Monitor the progress of the remediation task.

   ```
   az policy remediation list --scope
   "/providers/Microsoft.Management/managementGroups/$MG_ID"
   ```

   Expected Output: The `status` field should eventually transition to `Succeeded`, and the `successfulDeployments` count should increase, indicating subscriptions are being onboarded.

3. **Validate MDC Onboarding:**
   - **Azure Portal Check:** Navigate to the Azure Portal -> Microsoft Defender for Cloud -> Environment Settings.
   - **Verification:** Verify that subscriptions under the target Management Group are listed and have the basic plan enabled. For a newly created subscription, check its compliance status in the Azure Policy blade.

7.2. Sentinel Data Flow Validation

1. **Validate Sentinel Connection:**
    - **Azure Portal Check:** Navigate to the Azure Portal -> Azure Sentinel -> Data Connectors.
    - **Verification:** Verify that the **Microsoft Defender for Cloud** connector is listed as **Connected** and shows a healthy data ingestion rate.
2. **Trigger a Test Alert:** The most effective test is to generate a security alert and confirm its end-to-end flow.
    - **Method:** Create a non-compliant resource (e.g., a storage account without secure transfer enabled) in a newly onboarded subscription. MDC should generate a recommendation/alert.
    - **KQL Query in Sentinel:** After a short delay (up to 30 minutes), run the following KQL query in the Sentinel Logs blade:

      ```
      SecurityAlert
      | where ProviderName == "Azure Security Center"
      | where TimeGenerated > ago(1h)
      | project TimeGenerated, AlertName, Description
      ```

    - **Verification:** The test alert should appear in the query results and be visible as an incident in the Azure Sentinel Incidents blade.

8. Troubleshooting

This section outlines common issues encountered during deployment and provides detailed resolution steps.

Issue	Potential Cause	Resolution
Policy Assignment Fails	Incorrect Management Group ID or insufficient permissions for the deploying user.	**Action:** Verify the `MG_ID` variable is correct. Ensure the deploying user has the **Owner** or **User Access Administrator** role at the MG scope.
Managed Identity Role Assignment Fails	The Managed Identity Principal ID was not retrieved correctly, or the deploying user lacks the `Microsoft.Authorization/roleAssignments/write` permission.	**Action:** Re-run the `az policy assignment show` command to confirm the `PRINCIPAL_ID` is retrieved. Ensure the deploying user has the necessary permissions to create role assignments at the MG scope.
Subscriptions Remain Non-Compliant	Remediation task has not run, or the Managed Identity lacks the required **Security Admin** role.	**Action: Patience:** Wait for the remediation task to complete (can take several hours). **Verification:** Verify the Managed Identity has the **Security Admin** role assigned at the MG scope using

Issue	Potential Cause	Resolution
		the Azure Portal or CLI.
MDC Alerts Not in Sentinel	Data connector is not configured correctly, or Sentinel is not enabled on the workspace.	**Action: Check Sentinel Status:** Verify that Sentinel is enabled on the Log Analytics Workspace. **Check Connector Status:** In Sentinel -> Data Connectors, ensure the **Microsoft Defender for Cloud** connector is listed as **Connected**.
`az rest` command fails (Phase 2)	Incorrect API version or malformed JSON body.	**Action:** Verify the `api-version` (e.g., `2020-01-01`) is still valid. Ensure the JSON body for the `az rest` command is correctly formatted and escaped.

9. Cost Optimization

The framework utilizes services that incur costs, primarily Microsoft Defender for Cloud and Azure Sentinel (Log Analytics Workspace). Optimization is key to maintaining a strong security posture without excessive expenditure.

9.1. Microsoft Defender for Cloud (MDC) Tier Selection

The initial policy deploys the **Free** tier, which only provides CSPM features. The **Standard** (or paid) tiers enable CWPP features like Just-in-Time VM access and advanced threat protection.

- **Optimization Strategy:** Only enable the **Standard** tier for subscriptions and resources that host production, high-value, or regulated workloads. Use a separate, more granular Azure Policy to enforce the Standard tier selectively based on resource tags (e.g., `Environment: Production`) or subscription names, rather than applying it broadly.

9.2. Log Analytics Workspace (Azure Sentinel)

Log Analytics is the primary cost driver for Sentinel, based on data ingestion volume and retention period.

- **Data Retention:** Configure the Log Analytics Workspace data retention to balance compliance needs with cost. While security logs often require 90 days or more for compliance, setting a shorter interactive retention (e.g., 30 days) and using **Azure Storage** for long-term, low-cost archival (via Export Rules) can save significant costs.
- **Data Filtering:** Use **Data Collection Rules (DCRs)** to filter out high-volume, low-value logs *before* they are ingested into the workspace. For example, if certain verbose application logs are not required for security monitoring, exclude them from the workspace.
- **Commitment Tiers:** If the data ingestion volume is consistently high (e.g., >100 GB/day), consider moving from the **Pay-As-You-Go** model to a **Commitment Tier** to receive a discount on the ingested data.

9.3. SOAR Efficiency

SOAR playbooks, often implemented with Azure Logic Apps or Azure Functions, incur execution costs.

- **Optimization Strategy:** Optimize KQL queries within Sentinel to minimize the number of false positives that trigger a playbook. Design playbooks to be efficient, minimizing the number of steps and external API calls, which can

quickly drive up costs. For high-volume, simple automation, prefer Azure Functions (Consumption Plan) over Logic Apps for better cost control.

10. Security Best Practices

Beyond the core deployment, several best practices must be followed to ensure the long-term security and integrity of the governance framework itself.

10.1. Principle of Least Privilege for Managed Identity

The Managed Identity for the Policy Assignment was granted the **Security Admin** role, which is a highly privileged role necessary for the initial onboarding of subscriptions.

- **Hardening Step:** Once all existing subscriptions are onboarded and the remediation task is complete, the **Security Admin** role assignment on the Managed Identity should be reviewed. If the policy is only intended to onboard *new* subscriptions, the role can be removed and only re-assigned temporarily when a new remediation is required. Alternatively, if the policy is only enforcing the **Free** tier, the required role might be less privileged, such as **Security Reader** or a custom role.

10.2. Enable Enhanced Defender Plans

The framework's true value is unlocked by enabling the **Standard** (paid) Defender plans for critical workloads.

- **Hardening Step:** Modify the Azure Policy definition to enforce the **Standard** tier for specific Defender plans (e.g., Defender for Servers, Defender for Storage) on production subscriptions. This enables critical CWPP features like **Just-in-Time VM access**, **Adaptive Network Hardening**, and **File Integrity Monitoring**, which are essential for a mature security posture.

10.3. Secure the Sentinel Workspace

The Log Analytics Workspace contains all security data and is a high-value target for attackers.

- **Hardening Step:**

- **RBAC:** Implement strict Role-Based Access Control (RBAC) on the Log Analytics Workspace and the Sentinel instance, restricting access to only the Security Operations Center (SOC) team. Use built-in roles like **Sentinel Reader** and **Sentinel Contributor**.
- **Private Link:** Configure **Azure Private Link** for the Log Analytics Workspace to ensure that all data ingestion and query traffic occurs over the Azure backbone network, preventing exposure to the public internet.

10.4. SOAR Playbook Hardening

Automated response is powerful but carries the risk of unintended consequences (e.g., isolating a critical production server).

- **Hardening Step:** All SOAR playbooks must be thoroughly tested in a non-production environment. For high-impact actions (e.g., isolating a VM, disabling a user), implement a **"human-in-the-loop"** approval process where the playbook pauses and requires explicit approval from a security analyst before executing the final, destructive action.

11. Cleanup (Optional)

If the framework needs to be decommissioned, the following steps should be executed in reverse order of deployment.

```
# 1. Remove Policy Assignment
az policy assignment delete \
    --name $POLICY_ASSIGNMENT_NAME \
    --scope "/providers/Microsoft.Management/managementGroups/$MG_ID"

# 2. Remove Role Assignment for Managed Identity
# Note: You need the PRINCIPAL_ID from the deployment phase
# PRINCIPAL_ID="..."
az role assignment delete \
    --assignee $PRINCIPAL_ID \
    --role "Security Admin" \
    --scope "/providers/Microsoft.Management/managementGroups/$MG_ID"

# 3. Delete Log Analytics Workspace and Resource Group
# Note: This will also delete the Sentinel instance and data connector
configuration
az group delete --name $RG_NAME --yes --no-wait
```

This implementation guide is a product of Manus AI and is based on the project documentation for PRJ-AZURE-SEC-060.