# AWS Requirements

* The client shall **create an IAM User** within their **AWS Account** dedicated to security assessment activities.
* The IAM User must be assigned the **SecurityAudit** policy to provide read-only access for security scanning purposes.
* The client shall **generate an Access Key ID** and **Secret Access Key** for this IAM User. These credentials will be securely recorded and provided to the security testing team for integration into vulnerability assessment tools.
* Upon completion of the setup, the client shall provide the following details to the security testing team:

| **Value** | **Description** |
| --- | --- |
| Access Key ID | Unique identifier for the IAM User |
| Secret Access Key | Secret authentication key for the IAM User |
| AWS Account ID | The client’s AWS Account Identifier |
| Region (optional) | Default region to be used for scanning |

# Azure Requirements

* The client shall **register an application** and create a **Service Principal** within **Microsoft Entra ID**.
* The Service Principal must be assigned the following roles:
  + **Security Reader**
  + **Analytics Reader**
  + **Reader**
* The client shall **generate a Client Secret** for the registered application and securely record both the **Client ID** and **Client Secret**. These credentials will be provided to the security testing team for assessment purposes.
* Under **API Permissions**, the client shall navigate to **Request API Permissions** and add the following delegated permissions:
  + Directory.Read.All
  + Policy.Read.All
* Upon completion of the setup, the client shall provide the following details to the security testing team

| **Value** | **Description** |
| --- | --- |
| Client ID | Application (Client) ID |
| Client Secret | Secret key used for authentication |
| Tenant ID | Microsoft Entra Tenant ID |
| Subscription ID | Azure Subscription Identifier |

# GCP Requirements

* The client shall **create a custom IAM role** named AquaCSPMSecurityAudit within their **GCP Organization or Project**.
  + This role must include the required read-only and audit-related permissions as defined in the aqua-security-audit-role.yaml template.

name: roles/AquaCSPMSecurityAudit  
title: Aqua CSPM Security Audit  
includedPermissions:  
 - cloudasset.assets.listResource  
 - cloudkms.cryptoKeys.list  
 - cloudkms.keyRings.list  
 - cloudsql.instances.list  
 - cloudsql.users.list  
 - compute.autoscalers.list  
 - compute.backendServices.list  
 - compute.disks.list  
 - compute.firewalls.list  
 - compute.healthChecks.list  
 - compute.instanceGroups.list  
 - compute.instances.getIamPolicy  
 - compute.instances.list  
 - compute.networks.list  
 - compute.projects.get  
 - compute.securityPolicies.list  
 - compute.subnetworks.list  
 - compute.targetHttpProxies.list  
 - container.clusters.list  
 - dns.managedZones.list  
 - iam.serviceAccountKeys.list  
 - iam.serviceAccounts.list  
 - logging.logMetrics.list  
 - logging.sinks.list  
 - monitoring.alertPolicies.list  
 - resourcemanager.folders.get  
 - resourcemanager.folders.getIamPolicy  
 - resourcemanager.folders.list  
 - resourcemanager.hierarchyNodes.listTagBindings  
 - resourcemanager.organizations.get  
 - resourcemanager.organizations.getIamPolicy  
 - resourcemanager.projects.get  
 - resourcemanager.projects.getIamPolicy  
 - resourcemanager.projects.list  
 - resourcemanager.resourceTagBindings.list  
 - resourcemanager.tagKeys.get  
 - resourcemanager.tagKeys.getIamPolicy  
 - resourcemanager.tagKeys.list  
 - resourcemanager.tagValues.get  
 - resourcemanager.tagValues.getIamPolicy  
 - resourcemanager.tagValues.list  
 - storage.buckets.getIamPolicy  
 - storage.buckets.list  
 - deploymentmanager.deployments.list  
 - dataproc.clusters.list  
 - artifactregistry.repositories.list  
 - composer.environments.list  
stage: GA

* The client shall **create a Service Account** and assign the following roles:
  + **Viewer**
  + **Security Reviewer**
  + **Stackdriver Accounts Viewer**
  + **Aqua CSPM Security Audit** (the custom role created earlier)
* The client shall **generate a JSON key** for the Service Account and securely download it. This key will be provided to the security testing team for assessment purposes.
* Upon completion of the setup, the client shall provide the following details to the security testing team:

| **Value** | **Description** |
| --- | --- |
| Credential File | Copy of the JSON key file |