Policies and Compliance Standards Automation

i.e. Policies management via a Spreadsheet.

The purpose of this document is to assist with **the management of Prisma Cloud policies and compliance standards policy mappings, including the management and creation of custom policies.**

**Methodology Purpose**

This policy automation methodology can be considered as part of the Alerts burndown effort.

Alert burndown - resolution of open alerts, consist of two things:

1. **Resolution of alerts** by remediation of the genuine security risks. This is beyond the scope of control by the security team and provided that the alerts are assigned to the relevant business stakeholders or relevant remediation playbooks are in place, is beyond the security team’s control.
2. **Policy management** - to remove false positives and select policies that are relevant. This is the responsibility of the security team and a process must be established to dismiss alerts or exclude specific resources or policies from generating false positive security risks alerts.   
   Along with the policy selection process and compliance standard reporting, this is the focus of this methodology.  
   This methodology does not cover resources grouping for appropriate policy and alerts coverage. This must be addressed separately by defining the relevant account groups and alert rules.   
   This methodology also does not cover automatic alerts dismissal using resource\_lists\_for\_alert\_rules\_enabled feature flag to automatically dismiss alerts that have specific tags defined on the resource and added to the Resource Lists on Prisma Cloud, but allows for policies customisation to exclude specific policies from generating alerts for the appropriate group of resources within the alert rules.

**Brief description**

This automation allows to:

* Generate a **detailed list of all policies** (and Resolved/Open/Dismissed Alert numbers per policy) in the platform with **focus on a specific customer compliance standard,** includes alert rules (including auto\_dismiss) and notifications channels for the policy
* **Track all policies changes and new policies discovery**
* Track Compliance standard changes and **automatically assign/remove selected supported policies to the given compliance standard** by modifying the relevant policies
* Manage **automatic policies labels** for a given compliance standard, allowing Compliance standard specific alert rules to use policy labels for automatic policies selection
* Creates an **automatically extracted** **Service** column representing a specific cloud product/service **for ALL policies** (build included) which allows you to focus on all policies for that specific service - example: All EC2 policies
* **Create and manage custom policies, assignment of custom policies to compliance standards** and assignment of policy labels for custom policies, validation of custom policies RQL
* Generate Statistics on:
  + policies for cloud type, severity, policy types, custom
  + compliance standard policies status (included, no, maybe, new)
  + compliance standard/requirement/section policies breakdown
  + compliance standard protected (enabled policies) Service - cloud products/services
  + policies statistics by Finding types
  + Resolved/Open/Dismissed alert counts for the above

For Alert burndown specifically, this allows you to filter on policies with a high number of Open or Dismissed alerts that potentially could indicate false positives (or manual/auto-dismiss alerts) and adjust your policies or alert rules accordingly.

From the initial policies discovery run - the default policies that have not been included in the given compliance standard are marked as Included=Maybe if there are alerts present and Review if alerts have been dismissed.

Private Github repo - <https://github.com/okostine-panw/compliance_policies>

Terminologies between cloud providers might be different depending on each cloud provider,  
The policy refers to AWS terminology but applies to all public cloud vendors.  
A reference between cloud providers can be found [here](https://cloud.google.com/docs/get-started/aws-azure-gcp-service-comparison).

[**Proposed Project Scope of Work: 5**](#_heading=h.gg3xyexso5zn)

[**Compliance standard and Policies register spreadsheet 6**](#_heading=h.39romchg7d3x)

[Spreadsheet Format 6](#_heading=h.brcnyi4yd46j)

[**Python Automation Scripts to manage Compliance standard and policies 8**](#_heading=h.c5tjvcweng2l)

[Policies data collection 8](#_heading=h.fghfarwlxwb0)

[Compliance-All-Policies-excel.py 8](#_heading=h.d40vd55cg0r7)

[Policy Updates 8](#_heading=h.9qm5713dza50)

[Compliance-Policies-Update.py 8](#_heading=h.hgb7uvry9mrs)

[Other 9](#_heading=h.fu0hj6acu9og)

[Deletes policies created by specific user - sysadmin for OOTB system policies or user who created policies permissions required 10](#_heading=h.jw79681m69rt)

[Authentication 10](#_heading=h.p87p9mr2ls0e)

[Local credentials API Configuration 10](#_heading=h.sxkkptvpignu)

[(Optional) AWS Secret format to access Prisma Cloud API 10](#_heading=h.pwoftl7fuqm9)

[**Next Actions Plan: 11**](#_heading=h.10c4tmwa5lys)

[**CIS based Example Compliance Standard Requirements and Sections mapping 12**](#_heading=h.21do1it3mqa)

[Threat Detection - PolicyLabel: CU\_THREAT-ANOMALY- 12](#_heading=h.rio7q5hjd181)

[THREAT-ANOMALY-UEBA Anomaly UEBA events 12](#_heading=h.ouziayqwrbjh)

[THREAT-ANOMALY-NET Anomaly network events 12](#_heading=h.zemb7rpxaxf9)

[**Identity and Access Management - PolicyLabel: CU\_IAM- 12**](#_heading=h.yvq329w4r1jb)

[CU\_IAM-ROLE Role-based access control - IAM Policies specific to permissions (OoTB policies for risky permissions available) 13](#_heading=h.c171vyny4nkx)

[CU\_IAM-ROOT Root User Account 13](#_heading=h.41jmsbi6ackn)

[CU\_IAM-PASS Password policy - Password policies for AWS/GCP/Azure 13](#_heading=h.ed4motxoyh8x)

[CU\_IAM-USER IAM configuration changes - resource IAM config policies for AWS/GCP/Azure 13](#_heading=h.2sy50a197dw6)

[CU\_IAM-BREAKGLASS Breakglass IAM users - Custom IAM Config policies 14](#_heading=h.jvbdr5wobn3o)

[CU\_IAM-SAML Cross-Account Roles - Between <customer\_name> accounts - IAM Config policies 15](#_heading=h.vzz8l9s6v621)

[**Logging - PolicyLabel: CU\_LOG- 16**](#_heading=h.s94ohnag8y6n)

[CU\_LOG-TRAIL Audit Logs - CloudTrail 16](#_heading=h.9a3czta4nafp)

[CU\_LOG-FLOW Flow Logs - AWS Level 2 Logging 3.9 16](#_heading=h.69bm982ge9rv)

[**Monitoring - PolicyLabel: CU\_LOG- 16**](#_heading=h.k8vylighdnpr)

[**Compute workloads, OS & Application Security PolicyLabel: CU\_COMPUTE-WORKLOADS- 16**](#_heading=h.bxxqehkfdx2g)

[CU\_COMPUTE-WORKLOADS Compute workloads 17](#_heading=h.xfhtc7l9p09m)

[CU\_COMPUTE-WORKLOADS Vulnerability & Asset Management - Workload Vulnerability Management Process 17](#_heading=h.9wp5xh4rw0as)

[**Networking - PolicyLabel: CU\_NET- 17**](#_heading=h.uv2u32ua4eq9)

[CU\_NET-TOPOLOGY Network Topology - Networking config and exposure policies 18](#_heading=h.pf7q5425ytky)

[CU\_NET-SG Security Groups - Inbound Rules - Networking config and exposure policies 18](#_heading=h.o28u59l3u0h6)

[**Data Protection (Storage) - PolicyLabel: CU\_DATA 19**](#_heading=h.stc9m0bolbqj)

[CU\_DATA-REST Data At Rest 19](#_heading=h.4g4wouuswcwp)

[CU\_DATA-TRANSIT Data in Transit 20](#_heading=h.ssj3evq8gpnc)

[**Existing CIS Standards requirements definitions 21**](#_heading=h.dy8iboxbl4aj)

[GCP 21](#_heading=h.16t8rvu0brhl)

[Azure 22](#_heading=h.2w69tfocvye4)

[**Mapping of other Standards requirements definitions to <customer\_name> v2 Compliance standard requirements 23**](#_heading=h.6qalkz56ssi6)

[**Resources 23**](#_heading=)

## 

## Proposed Project Scope of Work:

1) Define new <customer> Custom Compliance standards based on CIS (or other) format for:

1. AWS
2. GCP
3. Azure
4. OCI
5. Alibaba Cloud
6. IBM

2) <customer> input into definitions of each Compliance Requirements sections

3) Review existing policies that are part of other standards and map them to the relevant <customer> requirement section

4) Review other platform policies and add them to the relevant <customer> requirement section,

5) Review specific <customer> requirement sections and select/create policies/controls for each, map policies to the relevant <customer> standard/requirement section

6) Create API automation for new custom policies creation and assignment of default or custom policies to the <customer> compliance standard

7) Providing examples of custom policies developed by PS already. Creation and validation of 50 new <customer> custom policies for GCP/Azure/OCI (optional)

# Compliance standard and Policies register spreadsheet

**compliance\_policies\_<customer\_name>*<standard*name>\_latest.xslx**

## Spreadsheet Format

**Columns:**

Annotations:

**\* - Retrieved by the script** (Except Custom policies that are not part of the compliance standard - i.e. have not been processed and don’t have a Policy ID)

**\*\* - Updated by Script**

**\*\*\* - Manual value** used from the spreadsheet, **update this as required before running policies update register or policies update script**

**Standard\*** - Compliance Standard name

**Included\*\*\*** - Policy Status:

* **<customer\_name>** - included in the new standard, **updated automatically to this value after YES policies update is performed**
* **YES** - policies to be added to the compliance standard and new labels update
* **REMOVE** - policies to be removed from the compliance standard
* **MAYBE** - possible inclusion in the standard
* **REVIEW** - for review to be included
* **NO - Not included**
* RUN-NEW - new Config policies (including Attack Path) added to the platform - needs review
* BUILD - build policies - not currently mapped to compliance standards
* BUILD-NEW - new build policies added to the platform
* NO\_SUPPORT - Attack Path policies, currently can’t be added to a compliance standard
* DUPLICATE - duplicate of existing policy
* IGNORE - to ignore

**SectionOption\*\*\*** - Custom value for Standard Section (retrieved as selection options for policies included in the Standard, can be changed if required, custom labels will be updated from this value)

**Resolved\*** - Resolved Alerts

**Open\*** - Open Alerts

**Dismissed\*** - Dismissed Alerts

**Enabled\*** - Policy Status

**Rules\***  - Alert rules that include this policy

**CloudType\*\*** - AWS, Azure, GCP, OCI  
**Service\*\*** - Cloud Service/App related to the policy

**PolicyName\*** - Policy Name

**FindingTypes\*** - MISCONFIGURATION, INTERNET\_EXPOSURE, HIGH\_PRIVILEGED\_ROLE, USER\_ANOMALY, etc.

**Severity\*** - Policy Severity

**Owner\*** - policy owner user

**PolicyType\*** - Policy Type

**PolicySubTypes\*** - Policy Subtype

**Requirement\*\*** - Default Standard Requirement from the policy compliance

**Section ID\*\*** - Default Standard Requirement

**Labels\*\*** - Policy Labels, includes automatically retrieved current policy labels + labels created by this script for <customer\_name> standard name and the Section\_ID value <Cloud\_Type>\_CU\_<P\_Section> for each policy, does not recreate already existing automated script policy labels but will be updated if P\_Section is changed in the spreadsheet and the script is run again. CU is the first two letters of the customer name.

**Remediable\*** - True/False

**PolicyClass\*** - exposure, behavioral, network\_protection, privileged\_activity\_monitoring

**API Name\*\*** - Cloud API used by the policy RQL, for build policies - Category

**Description\*** - Policy Description

**Recommendation\*** - Remediation recommendation

**Remediation\*** - Remediation steps and cli commands

**Policy RQL\*** - Policy RQL query

**LastModifiedBy\*** - Last policy change author

**LastModifiedOn\*** - Last policy change date

**Policy UPI\*** - Current Policy Index, plus updated with with added \_Checkov\_ID for build and build, run policies, and Custom - for Custom policies

**PolicyCategory\*** - risk/incident

**AccountGroups\* -** Alert rules details with notification channel and AccountGroups that include this policy

**SystemDefault\*** - Default OOTB Prisma Policy status

**PolicyID\*** - Policy ID, for custom policies - for custom policies - updated by the script after successful policy creation

**search\_id\*** - Policy RQL search ID, for custom policies - for custom policies - updated by the script after successful custom policy creation

**savedSearch\*** - Using Policy RQL saved search status, for custom policies - updated by the script after successful custom policy creation

**Reason\*\***- Status for For policy update (Included - YES), Custom policy RQL validation status for (Included - MAYBE) Custom policies, updated data from policies in Prisma Cloud, new and deleted policies

# 

# Python Automation Scripts to manage Compliance standard and policies

Step 1: Run Compliance-All-Policies-excel.py to collect policies data, select your compliance standard from the list of available standards.

Step2: Edit the generated compliance standard policies spreadsheet - make changes to any existing policies with values for: **Included** Status, **SectionOption** or manually add a new Custom Policy (all fields) rows.

Step 3: Run the Compliance-Policies-Update.py script to update the to include specific policies modified in the spreadsheet in the selected standard, create new custom policies if added.

New spreadsheet updated - compliance\_all\_policies\_<customer\_name>\_<compliance\_standard\_name>\_latest.xlsx

Step 4: Repeat 2, 3, review new discovered policies

**Script input parameters:**

**<standard\_id>**- select from the list of custom compliance standards present or add static <customer> Compliance standard in the script event

"standard\_id": "a0ea1077-424f-45fd-994e-4caef6d4d9de"

**<customer\_name>** - given <customer\_name> name in the script event

"Customer": "<customer\_name>"

**<bucket\_name>** - folder to save output to, data by default

**<​​filename> -** default to compliance\_all\_policies

## Policies data collection

### Compliance-All-Policies-excel.py

* Requires access to Prisma Cloud APIs

Retrieve all existing policies by selecting a compliance standard from the list of available standards, to be used as the initial input for the update script.   
All existing policies data is retrieved from the Prisma Cloud instance.

Performs automatic labels mapping, Policy RQL, API used and Cloud Service provider Service name extraction

Output:

* **compliance\_all\_policies\_<customer\_name>\_<compliance\_standard\_name>\_latest.xlsx**

## Policy Updates

### Compliance-Policies-Update.py

Use this script to perform automated policies updates from the compliance standard policy register spreadsheet.  
The compliance standard needs to be the same as the one selected in step 1.

You can edit multiple standards policies by selecting relevant standard to work with during the script run.

Automatically generated Reference csv with the relevant compliance standard requirements/sections/assigned policies definitions details.

After making changes to the spreadsheet and running the script again,  
This script will add/remove policies to the compliance standard and update labels for policies with status set to Included=YES after manual changes to the policies spreadsheet.   
Newly discovered policies added to the compliance standard.

Editing policies set to YES/REMOVE in the spreadsheet to be enabled, labels updated and policy changed to be included in the <customer\_name> compliance standard.

Spreadsheet update for the affected policies with the Compliance Standard, Include=<customer\_name> and the Policy update status. REMOVE will remove the policy from the compliance standard and the relevant labels, but will not disable (or delete) it.  
The script will **ONLY update any policy with Included=YES/REMOVE with enabled status, specific labels and compliance from the spreadsheet**.

All existing policies data is retrieved from the Prisma Cloud instance.

The script also collects information on new added policies (NEW-RUN, NEW-BUILD, etc) and adds them to the spreadsheet.

Generates a totals summary for the policies included in the standard and all other policies.

* Requires access to latest policies CSV file
* Requires access to Prisma Cloud APIs to make changes to the updated policies (SystemAdmin is needed to make changes to the Prisma Cloud default policies)

Input/Output:

* **compliance\_all\_policies\_<customer\_name>\_<compliance\_standard\_name>\_latest.xlsx**
* **compliance\_all\_policies\_\_<customer\_name>\_<compliance\_standard\_name>\_data\_totals\_%Y%m%d%H%M'.csv**
* **compliance\_all\_policies\_<customer\_name>\_<compliance\_standard\_name>\_Reference\_latest.xlsx**

Backup:

* **compliance\_all\_policies\_<customer\_name>\_<compliance\_standard\_name>\_%Y%m%d%H%M'.xlsx**

Private Github repository - <https://github.com/okostine-panw/compliance_policies>

## Other

**Compliance-Policy-Delete**

* Requires access to Prisma Cloud APIs

### Deletes policies created by specific user - (sysadmin or user who created policies permissions required)

## Authentication

### Local credentials API Configuration

The script uses a local API\_config.ini configuration file (API\_config.ini) to manage credentials securely. Make sure to update the file with your Prisma Cloud API details. Optional AWS Secret code is included in the script comments

Example API\_config.ini:

[URL]

BaseURL = https://your.prismacloud.api

[AUTHENTICATION]

ACCESS\_KEY\_ID = your\_access\_key\_id

SECRET\_KEY = your\_secret\_key

### (Optional) AWS Secret format to access Prisma Cloud API

**baseurl**: https://apix.prismacloud.io

**access\_key\_id**: <your access id>

**secret\_key**: <your secret key>

For OOTB Prisma Cloud policies updates requires SystemAdmin role, otherwise can only update policies created by the relevant user/service account API key only

# 

# Next Actions Plan:

1. Redefine <customer\_name> Compliance Standard structure and policies labels - <customer\_name> input into definitions of each Compliance Requirements sections for the new <customer\_name> v2 Standard (this document) - Include existing <customer\_name> compliance policies into <customer\_name> v2 Standard - **<customer\_name> field - YES/NO/REVIEW**
2. Identify Prisma Cloud policies that are in the CIS v2/3,CIS Controls v8, Azure BenchmarkAzure Security Benchmark (v3), GDPR, NIST CSF 2.0, PCI DSS v4.0 standards by default and add them to the <customer\_name> v2 Standard compliance standard.
3. Identify Prisma Cloud policies that are not in any standard by default (latest policies) and add them to the <customer\_name> v2 Standard compliance standard.
4. Update existing custom policies with relevant compliance section labels
5. <customer\_name> - from the list of candidate policies to select applicable policies to be included in the the new <customer\_name> v2 Standard **(update <customer\_name> field - YES/NO/REVIEW) , <customer\_name> to review latest version of policies spreadsheet**
6. Where selected existing policies do not match <customer\_name> requirements - <customer\_name> to edit specific compliance standard requirement and sections with use cases as part of this document for custom policies where appropriate - **<customer\_name> CUSTOM POLICY SELECTION , <customer\_name> to review current compliance sections mapping to policies in the policies spreadsheet**
7. Create custom policies for specific <customer\_name> controls that currently do not have platform OoTB policies for AWS/GCP/Azure/OCI - **<customer\_name> to review latest version of policies spreadsheet**

# 

## 

# 

# CIS based Example Compliance Standard Requirements and Sections mapping

New Compliance Standard name - <customer\_name> Standard

To simplify policies and labels management, each compliance section label will be updated by the scripts to include relevant Cloud Service Provider prefix - eg. CU\_**AWS\_**IAM-

## Threat Detection - PolicyLabel: CU\_THREAT-ANOMALY-

This section contains recommendations for Threat detection and anomaly policies

### THREAT-ANOMALY-UEBA Anomaly UEBA events

* Currently THREAT-ANOMALY section only
* Policies:
  + Account hijacking attempts
  + Unusual user activity
  + Excessive login failures

### THREAT-ANOMALY-NET Anomaly network events

* Currently THREAT-ANOMALY section only
* Policies:
  + Port Scan attempt from inside monitored cloud accounts
  + Port Sweep attempt from inside monitored cloud accounts

## 

## Identity and Access Management - PolicyLabel: CU\_IAM-

This section contains recommendations for configuring identity and access management related options.

Detailed policies in the policies spreadsheet.

### CU\_IAM-ROLE Role-based access control - IAM Policies specific to permissions (OoTB policies for risky permissions available)

* + Using RBAC allows specifying granular access permission privileges at various levels.  
    Access to any resource needs to be assigned based on groups (dynamic groups are preferred) with the minimum required access.
  + The information security principle of least privilege asserts that users and resources should be granted access only to the data and operations they require to perform their actions.   
    Access to all resources needs to be assigned with least privilege principle in mind.
  + Permission to change any network related settings or configuration will be done only by corporate system or ITE teams.

### CU\_IAM-ROOT Root User Account

* + The root user account will have no access keys associated with it - **default access keys must be deleted**.
  + The root user account will have MFA with a virtual MFA device (not connected to Azure AD).
  + Any login of the root user will be alerted to the SOC - must be verified with the account owner.

### CU\_IAM-PASS Password policy - Password policies for AWS/GCP/Azure

* + The password policy will be configured the same as Service Users in Password Policy:
    - Minimum Password Length: 20
    - At least one of the following characters: Uppercase letter, Lowercase letter, Number, Non-alphanumeric character.
    - Allow users to change their own passwords.
    - Prevention of reused 24 last passwords

### CU\_IAM-USER IAM configuration changes - resource IAM config policies for AWS/GCP/Azure

* + Any change to the IAM configuration (e.g. Password policy change, New IAM user, New Policies, New Roles) will be alerted to the SOC.
* **Automated Service Users - API keys - CodeSecurity policies, IAM config policies for AWS/GCP/Azure**
  + **Until Vault implementation**, Automated service users will be configured as IAM users with API keys which will be rotated regularly.
  + Credentials to automated service users must be kept off the codebase (i.e. GitHub, Stash, SVN).
  + Service users must **not have access to the web console.**
  + All service users will have a policy allowing access only from a specific set of <customer\_name> corporate IP addresses.
  + Any new service user requires approval from the security team and an alert should be raised.
  + These users will be tagged with the following tags:
    - **UserType:Service**
    - **Owner:[username]@<customer\_name>.com**
    - **OwnerGUID:[GUID]  
      Note:** You may use the following script to get the ObjectGUID value of a user from Active Directory.
* **Human Users - All Audit logging is monitored by Prisma Cloud and Anomalous User behavior is detected.**
  + All user access to the AWS console must be done via SSO **Entra ID** ([myapps.microsoft.com](https://myapps.microsoft.com/)).
  + A user will have permissions based on the AD group to which they belong.

### CU\_IAM-BREAKGLASS Breakglass IAM users - Custom IAM Config policies

* Any login to a Breakglass user will be alerted to the SOC - must be verified with the account owner.
* Breakglass users are specific individual employees, part of the ITE group or otherwise the main technical group in charge of the tenant.
* Each tenant will be allowed a small number of IAM Breakglass users.
* These users must have virtual MFA enabled.
* These users will have access to the web console only. **No Access Keys!**
* Breakglass account username should be the user <customer\_name> email address
* These users will be tagged with the following tags
  + **UserType:Breakglass**
  + **Owner:[username]@<customer\_name>.com**
  + **OwnerGUID:[GUID]  
    Note:** You may use the following script to get the ObjectGUID value of a user from Active Directory.

### CU\_IAM-SAML Cross-Account Roles - Between <customer\_name> accounts - IAM Config policies

* + Cross account role delegation requires the approval of the security team via JIRA approval ticket **Information Security (SEC)**.
    - Tickets must include the details of the 2 accounts, what data is being shared, what resources require access.
  + Cross account role delegation must have external ID in place, default form of external ID is UUID4 - <https://www.uuidgenerator.net/>
  + These roles will be tagged with the following tag:
    - **RoleType:InternalCrossAccount**
* **Cross-Account Roles -** Between a <customer\_name> account & 3rd Party account - **Custom IAM Config policies**
  + Cross account role delegation requires the approval of the security team via JIRA approval ticket **Information Security (SEC)**.
    - Tickets must include the details of the 3rd party, what data is being shared, what resources require access.
  + Data sharing, if required, will be done according to the legally-approved agreement between <customer\_name> and the 3rd party.
  + Cross account role delegation must have external ID in place, default form of external ID is UUID4 - <https://www.uuidgenerator.net/>
  + Permissions will be based on least privilege.
  + Any 3rd party cross-account role delegation will be configured with a 12 month expiration date (using IAM time conditions)
  + These roles will be tagged with the following tags:
    - **RoleType:ExternalCrossAccount**
    - **Vendor:[Vendor Name]**
    - **Owner:[username]@<customer\_name>.com**
    - **OwnerGUID:[GUID]**  
      **Note:** You may use the following script to get the ObjectGUID value of a user from Active Directory.

## Logging - PolicyLabel: CU\_LOG-

This section contains recommendations for configuring logging features.

Detailed policies in the policies spreadsheet.

### CU\_LOG-TRAIL Audit Logs - CloudTrail

* + All CloudTrail **read & *write*** Logs will be saved in a central S3 bucket for all regions in the account - **<customer\_name>-sec-longterm**
  + CloudTrail logs will be searched for problematic, and abnormal behavior
* **Audit Logs - Config** **- Prisma Cloud performs Confg Audit logging for all onboarded cloud resources**
  + Config must be configured in all regions (even regions without resources) and send all logs to a central S3 bucket - **<customer\_name>-sec-longterm**
  + Global resources will be monitored from the **us-east-1** region only

### CU\_LOG-FLOW Flow Logs - AWS Level 2 Logging 3.9

* + All VPC Flow Logs will be logged to CloudWatch logs and will be retained for 14 days
    - This will allow any system to search the flow logs for malicious or suspicious traffic using the Palo Alto Prisma Cloud system.

## Monitoring - PolicyLabel: CU\_LOG-

This section contains recommendations for configuring AWS to assist with monitoring and responding to account activities. Metric filter-related recommendations in this section are dependent on the Ensure CloudTrail is enabled in all regions and Ensure CloudTrail trails are integrated with CloudWatch Logs recommendation in the "Logging" section.

Detailed policies in the policies spreadsheet.

## Compute workloads, OS & Application Security PolicyLabel: CU\_COMPUTE-WORKLOADS-

Detailed policies in the policies spreadsheet.

### CU\_COMPUTE-WORKLOADS Compute workloads

* **Custom tagging policy - AWS EC2 instance not labeled with Owner**  
  Any kind of compute element needs to be tagged with the following tags:
  + **Owner:[username]@<customer\_name>.com**
  + **OwnerGUID:[GUID]**

**Note:** You may use the following script to get the ObjectGUID value of a user from Active Directory.

### CU\_COMPUTE-WORKLOADS Vulnerability & Asset Management - Workload Vulnerability Management Process

All Assets should be patched regularly based on <customer\_name> Security Patch Management

Critical / High Vulnerabilities should be reported as they occur and should be patched based on the SLA defined on <customer\_name> Security Patch Management

* **Golden AMI** - **Workload Deployment Management Process**
  + All instances will be created using a predefined AMI (Application Machine Image) - One for each OS type - that will be cleared for security vulnerabilities and pre-provisioned with security tooling.
* **Endpoint Threat Detection & Logging - Diagnostic and logging Config policies for VMs**
  + All Linux servers must be configured with <customer\_name>'s **audit.d configuration**, and log to a central logging service.
  + All Windows servers must be installed with **SentinelOne EDR**.
* **Vulnerability & Asset Management - Diagnostic and logging Config policies for VMs, Workload Vulnerability Management Process**
  + Using a vulnerability scanner, all workloads will be scanned for known vulnerabilities. Any vulnerabilities found will be resolved according to a predefined SLA.
  + All instances will be managed by SSM for patch management and software asset management.

## Networking - PolicyLabel: CU\_NET-

This section contains recommendations for configuring security-related aspects of Networking config and exposure policies. Please Note - network exposure policies can not be assigned to a compliance standard.

Detailed policies in the policies spreadsheet.

### CU\_NET-TOPOLOGY Network Topology - Networking config and exposure policies

* + Each VPC will be configured with IP addresses according to <customer\_name>'s IP addressing scheme
  + IPSec VPNs will be established to <customer\_name> <customer\_name> Gateways data centers and branch offices only!
  + Network access should be limited only to the minimum required access.
  + All peering (BGP) / direct connect (ISP) / transitive connections will be done to <customer\_name>'s networks only.

### CU\_NET-SG Security Groups - Inbound Rules - Networking config and exposure policies

* + Access to internal services located in the cloud (SSH, RDP, Web, DBs etc.) will be done on **private IP addresses** routed in <customer\_name>'s networks
  + Must contain specific source (not 0.0.0.0/0)
  + Management, DB, Web admin consoles, and file sharing ports must **not be available from public IP** **addresses** (like 0.0.0.0/0)
    - Management Ports: 22-ssh, 3389-rdp, 5900-vnc
    - DB Ports: 1433,1434-mssql, 3306-mysql, 5432,5433-postgresql, 27017-mongodb
    - Web Admin Consoles: 10000-webmin
    - File Sharing Ports: 21-ftp, 445-smb
  + Service ports (443 - SSL, etc.) will only be available from public IP addresses if the service is **related to the relevant game client** (Internal <customer\_name> services not included) and using a Load balancer (ALB, ELB) - not directly to the EC2 instance.
* **Security Groups - Outbound Rules - Internet**
  + All outbound traffic will be inspected by a proxy service, matching the mechanism located in the Data centers.
  + Outbound traffic will be routed via the regional transit gateway in <customer\_name>'s networking account.
* **Security Groups - Outbound Rules - <customer\_name> services**
  + As described in Production Infrastructure Security Policy policies will be applied to control traffic between IaaS and On-Premises workloads.
* **Publicly Available Services** **- Application/Service Config specific policies**
  + All publicly available services - API endpoints, Websites, etc. - will be available via secure protocols, using SSL/TLS or equivalent

**Connectivity to <customer\_name> On-Prem** (to/from DCs, Offices)

* + AWS VPCs must be connected to <customer\_name>’s internal networks and services via **IPSec VPN only**
  + Connectivity to other cloud environments will be done via the regional TGW as depicted in Secure Design - AWS Network Connectivity
  + Connectivity between <customer\_name>’s on-prem and cloud-based services directly over the Internet is prohibited!
* **Connectivity to other <customer\_name> clouds**
  + Connectivity to other cloud environments will be done via the regional TGW as depicted in Secure Design - AWS Network Connectivity
* **WAF** - **Application/Service Config specific policies**
* Each Web application publicly accessible from the Internet will be protected by Akamai WAF solution.

### 

## Data Protection (Storage) - PolicyLabel: CU\_DATA

This section contains recommendations for configuring Storage and Data.

Detailed policies in the policies spreadsheet.

#### CU\_DATA-REST Data At Rest

* **Public S3 buckets - Storage policies, DSPM module**
  + S3 buckets must only be configured as public if the service they provide is related to the relevant game client or public website
  + Public S3 buckets must **not contain any sensitive information** or PII - as defined by <customer\_name> Data Privacy Protocol
  + Public buckets will have a policy that will **allow public clients to only get objects** (listing the buckets and their content is prohibited)
  + Public S3 buckets must be tagged with the **DataSecurity:Public** tag
  + Public S3 buckets will have the following policy:
    - Allow read objects - everyone (unauthenticated)
    - Allow list objects - owner, specific roles
    - Allow write/edit/delete objects - owner, specific roles
  + Any new public S3 bucket must receive the approval of via Jira tickets:
    - Architect in charge
    - Security team
  + These S3 buckets will be tagged with the following tags:
    - **Owner:[username]@<customer\_name>.com**
    - **OwnerGUID:[GUID]**

**Note:** You may use the following script to get the ObjectGUID value of a user from Active Directory.

* **PII in S3 buckets** - **DSPM module**
  + S3 buckets containing sensitive data and PII:
    - Must be tagged as such using the **DataSecurity:PII** tag
    - Must be encrypted using AES-256 with a <customer\_name> managed master key in KMS
    - Must be configured as **not public**
* **Databases** (RDS, RedShift, DynamoDB, ElastiCache, etc.) **- Database Service Config Policies**
  + All databases will utilize server-side encryption at rest.
  + The databases/volumes will be encrypted using AES-256, with a key managed in AWS KMS.
  + No Shared accounts will be used for human access

#### CU\_DATA-TRANSIT Data in Transit

* **Data In Transit - Networking config and exposure policies**

## Existing CIS Standards requirements definitions

The CIS compliance standards requirements definitions below are not being used, <customer\_name> specific compliance standard requirements (and sections) are being used instead.

### GCP

BigQuery

This section addresses Google CloudPlatform BigQuery. BigQuery is a serverless, highly-scalable, and cost-effective cloud data warehouse with an in-memory BI Engine and machine learning built in.

Cloud SQL Database Services

This section covers security recommendations to follow to secure Cloud SQL database services. The recommendations in this section on setting up database flags are also present in the CIS Oracle MySQL Community Server 5.7 Benchmarks and in the CIS PostgreSQL 12 Benchmarks. We, nevertheless, include them here as well, the remediation instructions are different on Cloud SQL. Settings of these flags require superuser privileges and can only be configured through GCP controls.

Identity and Access Management

This section covers recommendations addressing Identity and Access Management on Google Cloud Platform.

Logging and Monitoring

This section covers recommendations addressing Logging and Monitoring on Google Cloud Platform.

Networking <customer\_name>\_GCP\_Networking

This section covers recommendations addressing networking on Google Cloud Platform.

Storage

This section covers recommendations addressing storage on Google Cloud Platform.

Virtual Machines

This section covers recommendations addressing virtual machines on Google Cloud Platform

### Azure

AppService

This section covers security recommendations for Azure AppService.

Database Services

This section covers security recommendations to follow to set general database services policies on an Azure Subscription. Subsections will address specific database types.

Identity and Access Management

This section covers security recommendations to set identity and access management policies on an Azure Subscription. Identity and Access Management policies are the first step towards a defense-in-depth approach to securing an Azure Cloud Platform environment.

Key Vault

This section covers security recommendations to follow for the configuration and use of Azure Key Vault.

Logging and Monitoring

This section covers security recommendations to follow to set logging and monitoring policies on an Azure Subscription.

Microsoft Defender

This section covers recommendations to consider for tenant-wide security policies and plans related to Microsoft Defender. Please note that because Microsoft Defender products require additional licensing, all Microsoft Defender plan recommendations in subsection 2.1 are assigned as “Level 2.”

Networking

This section covers security recommendations to follow in order to set networking policies on an Azure subscription.

Storage Accounts

This section covers security recommendations to follow to set storage account policies on an Azure Subscription. An Azure storage account provides a unique namespace to store and access Azure Storage data objects.

Virtual Machines

This section covers security recommendations to follow for the configuration of Virtual Machines on an Azure subscription.

## 

### Mapping of other Standards requirements definitions to <customer\_name> v2 Compliance standard requirements

if included\_value == "YES":

p\_requirement = requirement\_name

else:

if requirement\_name in ["Identity and Access Management", "Key Vault", "Identity Management (IM)", "Privileged Access (PA)"]:

p\_requirement = "Identity and Access Management"

elif requirement\_name in ["Networking", "Network security (NS)"]:

p\_requirement = "Network Security"

elif requirement\_name in ["Storage", "Storage Accounts", "Database Services", "Cloud SQL Database Services", "BigQuery", "Dataproc", "Data Protection (DP)", "CIS Control 3: Data Protection"]:

p\_requirement = "Data Protection"

elif requirement\_name in ["Logging", "Monitoring", "Logging and Monitoring", "Logging and Threat Detection (LT)"]:

p\_requirement = "Logging and Monitoring"

elif requirement\_name in ["Virtual Machines", "AppService", "Microsoft Defender", "Compute","Asset Management (AM)","Endpoint Security (ES)"]:

p\_requirement = "Compute workloads, OS & Application Security"

else:

p\_requirement = ""

# Set p\_requirement based on labels

if "Identity Misconfiguration" in labels:

p\_requirement = "Identity and Access Management"

elif "Network" in labels:

p\_requirement = "Network Security"

elif "AppService" in labels:

p\_requirement = "Compute workloads, OS & Application Security"

if p\_section:

labels += f";CU\_{p\_section}" if labels else f"CU\_{p\_section}"

## Resources

* Production Infrastructure Security Policy
* Secure Design - AWS Network Connectivity
* Customer Data Privacy Protocol