# AWS-Tagging-Standards

## Why do we need tags?

Tags help application and operations teams:

- Understand what components in an application are doing and what apps they belong to.
- Understand who is accountable for resources.
- Understand who is accountable for cost.
- Understand criticality of assets to better protect them.
- Understand compliance concerns that may be on data.

## IAM Tagging Standards

### IAM User and Role Type Descriptions

The highest usage risk should be considered when classifying the type. We anticipate different controls based on user type and the inherent risk (example: more frequent key rotation for “vendor” and “service” user types)

| TagType | IdentityType | Description |
|---|---|---|
| user | IAM User | An account a GP employee is using to access AWS resources from a workstation |

| | | |
|---|---|---|
| service | IAM User or IAM Role | An account a Koch application or Koch company is using for processing data on resources in a Koch controlled AWS account. No data leaves Koch |
| vendor | IAM User or IAM Role | A non-Koch person or entity accessing or transferring data to or from a non-Koch owned environment or for vendor access to Koch owned cloud accounts or resources |
| deployment | IAM Role | Roles used by CICD and for deploying infrastructure. |
| support | IAM Role | Roles used to support infrastructure deployed via CICD. |
| consumer | IAM Role | Roles that consume resources deployed via CICD. |

## Role Tagging Standard

| TagKey | Description | Required |
|---|---|---|
| owner | This identifies who has decision rights about this IAM role and is accountable for any questions regarding the role. This must be a valid user email address (not a distribution list) and in email format (myemail@gapac.com). | Required |
| owneralternate | An additional contact provided who can authorize changes to a role or can be a point of contact. The value must be an email address | Required if ticketgroup is empty |

| | | |
|---|---|---|
| | (mydl@gapac.com) and should be distribution list. | |
| ticketgroup | A ServiceNow assignment group where a ticket can be dispatched to for changes to an IAM role and can act as a contact point. | Required if owneralternate is empty |
| description | What the role is being used for. | Required |
| type | Type of role being deployed. | Required - see definitions in section "IAM User and Role Type Descriptions" |

## User Tagging Standard

| TagKey | Description | Required |
|---|---|---|
| owner | This identifies who has decision rights about this IAM user and is accountable for any questions regarding the user. This must be a valid user email address (not a distribution list) and in email format (myemail@gapac.com).  This is the person who new IAM keys will be given to when key rotation is performed. | Required |
| owneralternate | An additional contact  provided who can authorize changes to a user or can be a point of contact.  The value must be an email address (mydl@gapac.com) and should be distribution list. | Required if ticketgroup is empty |
| ticketgroup | A ServiceNow assignment group where a ticket can be dispatched to for changes to an IAM user and can act as a contact point. | Required if owneralternate is empty |
| description | What the user is being used for. | Required |

| | | |
|---|---|---|
| type | type of user is being deployed. | Required - see definitions in section "IAM User and Role Type Descriptions" |

## Resource Tagging Standards

All resources capable of being tagged outside IAM resources (refer to IAM tagging standards above) should adhere to the following tags.

| TagKey | Description | Required | Expected Values |
|---|---|---|---|
| blc | buyer ledger code. Defines the company the resource will be billed to | Required | 1460 |
| costcenter | defines the project or department the resources will be billed to. | Required | format NNNNNNNNNN<br>Approved Cost Center List |
| itemid | unique identifier that can group resources together for more detailed billing. | Required | varies |
| owner | This identifies who has decision rights about the resources and is accountable for any questions regarding them.  This must be a valid user email address or a distribution list and in email format | Required | myemail@gapac.com or mydl@gapac.com |

| | | | |
|---|---|---|---|
| | (myemail@gapac.com or mydl@gapac.com). | | |
| owneralternate | An additional contact can be provided who can authorize changes to a resource or can be a point of contact. The value must be an email address (mydl@gapac.com) and should be distribution list. | Required if ticketgroup is empty | mydl@gapac.com |
| ticketgroup | A ServiceNow assignment group where a ticket can be dispatched to for changes to a resource and can act as a contact point. | Required if owneralternate is empty | service now assignment group name |
| description | What the resource is being used for. | Required | varies |
| segment | Segment the resource belongs to. | Required | See Cloud Strategy Team Leads List |
| org | Business asset belongs to. | Required | See Cloud Strategy Team Leads List |
| dr | Used to identify resources considered business critical. | Required | values should be 1,2 3.<br>Definition:<br>• 1- Most Critical - 1 day RTO<br>• 2 - Moderate Criticality - 7 day RTO<br>• 3 - Least Critical - 7+ day RTO |

| | | | |
|---|---|---|---|
| dataclassification | Used to indicate data that is sensitive to ensure proper controls are implemented. | Required | values should be Highly Confidential, Confidential, General, Public. See here for description of each type. |
| Name | Used to provide a name for services with a name in the console. | Required - For services with name tag in the AWS console. Required for **running containers** | varies |
| team | used to segment access to resources in the same account. | Optional - Used for segmentation of resources in same accounts. | varies |
| subsegment | tag for further segmentation based on team associated with resource. | Optional | varies |
| compliance | Used to identify workload that need to meet a specific compliance or regulatory requirement | Optional | values should be HIPAA, PCI, GDPR, ISO. |
| version | Used to indicate a version of a deployment. | Optional | varies |
| application | Used for enhanced billing reporting on resources | Required | varies |

12 people liked this    Comment    5025 Views    Save for later

## Comments