# Service Asset and Configuration Management

## Principles

The following are the first-class principles influencing the design considerations of the Software / Data - Asset Management capability

- Compliance
- Security
- Monitoring
- Cost Optimization
- Infrastructure as code

## Purpose

Service Asset and Configuration Management, or SACM, according to ITIL is described as:

> The process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.

The SACM capability can be thought of as two separate, but tightly coupled processes:

> **(i) Asset Management:** This process addresses those assets you use to deliver IT services.
>
> **(ii) Configuration Management:** This process tracks the configurations and relationships between various components (configuration items or CIs) of your various IT services

Together these processes are responsible for maintaining an up-to-date and verified database of all Assets and Configuration Items (CIs) throughout the IT Service Management Lifecycle. The primary objective of SACM is to identify, document and administrate all the Configuration Items (CIs) required for delivering IT services, including their relationships and dependencies. It is done in a way so that updated data can be made instantly available to other service management processes whenever needed.

## Cloud Considerations

- Resource Access
  - May not have the authorization to tweak the cloud provider's pre-packaged stack
- Security
- Monitoring
- Data Protection
- Performance
- Cost Management
  - Virtualized environments can be left running empty, representing significant cost with no business value.
  - There is no additional charge for AWS License Manager itself
- In a traditional IT setup, the goals of establishing a CMDB are met through the process of:
  - Discovery tools used to create a record of existing Configuration Items (CI)
  - Comprehensive change management processes to keep track of creation and updates to CIs
  - Integration of incident and problem management data with impacted CIs with ITSM workflow tools like BMC, Hewlett-Packard, or ServiceNow
- Challenges to creating a CMDB for cloud resources due to:
  - The inherently dynamic nature of cloud resource provisioning, where resources can be created or terminated through predefined business policies or application architecture elements like auto-scaling
  - The difficulty of capturing cloud resources data in a format that can be imported and maintained in a single system of record for all enterprise CIs
  - A prevalence of shadow IT organizations that make information sharing and even manual consolidation of enterprise IT assets and CIs difficult

## Risks

- Commercial of the shelf (COTS) Licensing Overages
- Vulnerability Management
- Incident Management
- Change Management
- Service Delivery Impact Analysis
- Resource Over/Under Utilization
- Reliance on license servers

### Dependencies

- Account Management
- Compute Instances/images
- Cloud Resource Modeling and Provisioning
- Cloud Resource Configuration Management

### Architecture Decisions

1. Leverage Eracent agents for commercial of the shelf software deployed asset reconciliation for Virtual Machine resources (IaaS)?
2. Leverage ServiceNow CMDB as a federated source of truth for Configuration Items (CIs) deployed to USAA chosen cloud service providers (CSP)?
3. Leverage ServiceNow Discovery Probes to fill metadata gaps with CIs deployed on a the client's chosen CSP?

### Architecture Artifacts

- ServiceNow CMDB
- ServiceNow CMDB Architecture
- ServiceNow CMDB Identification & Reconciliation
- ServiceNow CMDB Integrations
- ServiceNow CMDB Integrations - Turbot
- Enterprise Software Asset Management (ESAM)
- ESAM Architecture

### Guidance

1. Configuration items (CIs) must be consumed by our enterprise CMDB as it is the federated source of truth.
    a. This is a mandatory requirement by our regulators
2. Configuration Items must provide the following metadata
    a. Virtual Machine & Appliances (IaaS)
        i. IP Address
        ii. Hostname
        iii. Owner
        iv. Support Group
        v. Network Security Zone
        vi. Subnet
        vii. Purpose
        viii. Status
        ix. Virtual Status
        x. Critical Infrastructure
        xi. Data Sensitivity
        xii. Operating System
        xiii. Security Baseline
        xiv. End of Security Life
        xv. End of Life
        xvi. Logical Location
    b. Software (IaaS)
        i. Software Title
        ii. Version
        iii. Purpose
        iv. Application Owner
        v. Application Owner Delegate
        vi. Hosts/Device/Resource Installed On
        vii. Status
        viii. End of Security Life
        ix. End of Life
        x. Installation Date
3. All configuration items must be tagged with the TPM Application ID.
4. CIs need to be tagged. Tags help to classify, filter and define the CIs in the cloud.
5. To mitigate licensing risks and liability consider open-source OS, instead of licensed OSs e.g. Redhat

### Enablement

Since enablement is tied to specific cloud implementation, this section tries to list out the minimum features that need to be implemented as part of the safe landing, cloud enablement initiative.

1. CMDB

    a. At a minimum, a CMDB contains the following:
        i. Configuration item (CI) records with all associated attributes captured
        ii. A relationship model between different CIs
        iii. A history of all service impacts in the form of incidents, changes, and problems
    b. AWS Config helps customers manage their CIs in the cloud. AWS Config provides a detailed view of the configuration of AWS resources in an AWS account. With AWS Config, customers can do the following:
        - Get a snapshot of all the supported resources associated with an AWS account at any point in time
        - Retrieve the configurations of the resources
        - Retrieve historical configurations of the resources
        - Receive a notification whenever a resource is created, modified, or deleted
        - View relationships between resources

2. Licensing
    a. AWS License Manager
        i. Features
            1. Set license terms as rules
            2. License tracking enforcement
            3. Proactively limit non-compliance
            4. Application Discovery
            5. Centralized license management and reporting
            6. Integrates with: EC2, Systems Manager, Organizations, Service Catalog, Marketplace

Footnotes:

1: https://aws.amazon.com/license-manager/

2: https://www.snowsoftware.com/sites/default/files/documents/cloud_iaas_optimization_for_aws_en_screen_0.pdf

3: https://d1.awsstatic.com/whitepapers/AWS_Asset_Config_Management.pdf

4: https://www.certguidance.com/service-asset-configuration-management-itil/