Preparing for Service Asset and Configuration Management

CMDB Considerations

Wade Palmer, Director IT Services

Introduction

Often an afterthought or neglected when implementing Business Service Management and IT Service Management (ITSM) Systems and Processes; Service Asset and Configuration Management (SACM) and Configuration Management Database (CMDB) good practices should be considered key components in an effective ITSM strategy. Getting a clear view of the hardware and software assets owned by your organization will give you an understanding of the impact and value of the investments you've made throughout their lifecycle.

Accurate data within the CMDB, including relationships and dependency mappings, add a high degree of effectiveness to related processes, enterprise architecture and strategy, and reduce risks associated with Change and Configuration Management activities. ALL major operational and transitional ITSM activities (Incident, Problem, Change etc) should feed and utilize an accurate CMDB.

Key CMDB Data Elements

The IT Infrastructure Library (ITIL) provides guidance on key and essential data elements for a CMDB:

- Asset Registration and Lifecycle Status
- Relationships and Dependencies (Key to Change Impact Analysis and Service Mappings)
- Documentation (Vendor Warranties and Maintenance Agreements, Security Templates, Configuration Templates and related Processes)
- Service Level Agreements
- Service Catalogs
- Knowledge

Key IT Change Management Considerations

The CMDB provides reliable, quick and easy access to accurate configuration information to enable stakeholders and staff to assess the impact of proposed changes and to track the change's work-flow. This information enables the correct asset and service component versions to be released to the appropriate party or into the correct environment. As changes are implemented, the Configuration Management information should be updated, either manually, or automatically (preferred, in a closed loop change management system). The CMDB should also identify related CI/assets that will be affected by the change, but not included in the original request, or in fact similar CI/assets that would benefit from similar change.

Dependencies and Service Mappings

A key component or characteristic of a CMDB is how it relates each of the CIs to one another. These relationships are what differentiate standard Asset Management processes to the more robust ITIL good practices for SACM. In order for IT organizations to continuously improve services by adopting and improving upon best practices, an accurate, efficient and effective SACM system is crucial.

Discovery

As good as Senior IT technicians are, they will never be able to effectively maintain an accurate inventory of the infrastructure without automatic discovery. An effective discovery tool should, at a minimum, support or provide:

- Discovery of all IT assets — mainframe, distributed, and virtual
- Data reconciliation, software title normalization, and rules-based software license compliance
- License harvesting through effective software license management
- Elimination of the need to invest in integrations between IT asset and service support repositories
- A flexible architecture to quickly extend and adapt out-of-the-box workflows and data model, without programming to account for Business and Custom Application discovery

This assists in:

- Proactive contract management
- Gaining visibility into asset costs
- Executing intelligent IT change decisions
- Reducing out “shelf-ware”
- Lowering software license compliance penalties
- Driving problem management practices through accurate and current configuration data

Initial SACM and CMDB Good Practice Considerations

Develop and follow standard ITIL guided processes that initially include:

1. Document and make policy; methods to support the enforcement of standardized SACM procedures across the enterprise (People, Process, Technology) for the entire

Asset Lifecycle. Processes should include changing, updating, recording, tracking and verifying CIs and eliminating invalid and unauthorized changes

2. Determine required metadata, roles, and access restrictions to support the processes defined above
3. Populating all of the Physical Infrastructure (Discovery)
4. Populating key (if not all) relationships for the physical infrastructure (Discovery - Automated)
5. Populating COTS SW (Discovery)
6. Populating Business and Custom Applications