Key Issues for Implementing Configuration Management

Liu Ying¹, Xue Lijun¹, Su Wei²
¹Teachers’ College of Beijing Union University, Beijing, China
²Automation College of Beijing Union University, Beijing, China
liuying@buu.edu.cn, zdhtsuwei@buu.edu.cn

Abstract — Configuration Management is the key for an IT organization to transform from a technology provider to a service provider. In this paper, key considerations for designing and implementing Configuration Management are summarized. Some important policies, roles, RACI Matrix and leveraging technologies proposed in this paper will be valuable guidelines for IT Service Management practitioners.

Index Terms—ITIL (IT Infrastructure Library), Configuration Items, Database, RACI Matrix (Responsible, Accountable, Consult-before, Inform-after)

I. INTRODUCTION

Effective, reliable and flexible IT services are more and more critical to the success of business initiatives today. Enterprises are increasingly seeking to transform IT from a traditional technology provider to a reliable, low-cost IT service provider. How can an enterprise safely transform its IT organization? Many IT organizations are turning to IT Service Management (ITSM) for answers. ITSM focuses on delivering and supporting IT services that are appropriate to the business requirements of the organization, and it achieves this by leveraging IT Infrastructure Library (ITIL)-based best practices that promote business effectiveness and efficiency.

However, ITIL practices are only guidelines to help people to understand the core processes, while leaving the implementation issues to the practitioners. Most of these issues will include process policies, roles and responsibilities, technology leverage, etc. Because implementation will demand far-reaching changes that affect people, processes, and technology.

To help ITSM practitioners move forward with greater ease and confidence, this paper will take one important process in ITIL – IT Infrastructure Library. Typical disciplines include incident management, problem management, change management, capacity management, service level management, availability management, and so on (refer to [1]). Configuration Management is a specialized discipline as defined in ITIL. The primary objective of Configuration Management is to provide a basic and logical model of the enterprise’s IT infrastructure by identifying, controlling, maintaining and verifying the status and versions of Configuration Items (CIs) in the IT environment.

Why do the authors take Configuration Management as illustration in this paper? When we have conversation with IT directors or managers who are preparing to implement ITIL in their enterprises, they are more conscious at functional processes, such as incident management, problem management, and availability management, etc., while putting less focus on the configuration data management. Those remind us managing basic data while implementing ERP (Enterprise Resources Management). Many enterprises ignored managing data, such as items, bill of materials, routing, since they thought those issues had no technical difficulties.

Configuration Management has tight relationship with all other ITIL processes, shown as Fig. 1. All ITIL processes will access the infrastructure configuration data.

II. CONFIGURATION MANAGEMENT

There are five service supporting processes plus service desk function, and five service providing processes in the beginning version of ITIL – IT Infrastructure Library. Typical disciplines include incident management, problem management, change management, capacity management, service level management, availability management, and so on (refer to [1]). Configuration Management is a specialized discipline as defined in ITIL. The primary objective of Configuration Management is to provide a basic and logical model of the enterprise’s IT infrastructure by identifying, controlling, maintaining and verifying the status and versions of Configuration Items (CIs) in the IT environment.

Why do the authors take Configuration Management as illustration in this paper? When we have conversation with IT directors or managers who are preparing to implement ITIL in their enterprises, they are more conscious at functional processes, such as incident management, problem management, and availability management, etc., while putting less focus on the configuration data management. Those remind us managing basic data while implementing ERP (Enterprise Resources Management). Many enterprises ignored managing data, such as items, bill of materials, routing, since they thought those issues had no technical difficulties.

Configuration Management has tight relationship with all other ITIL processes, shown as Fig. 1. All ITIL processes will access the infrastructure configuration data.

Figure 1. Configuration Management
Wrong configuration data will lead to wrong decision in problem solving, capacity planning and availability design, resulting in lower service level than agreed with customers, or higher service cost.

All CIs are registered, tracked and monitored in the Configuration Management Database (CMDB), which represents the current known functional status of the IT environment. IT organizations need to have a controlled Configuration Management environment that enables the tracking, recording, and reporting of elements (i.e., Configuration Items or CIs) in their IT infrastructure. In the early years of IT, the process to keep this information current and accessible was simple. Today’s IT organizations need to manage complex technologies across multiple domains. The ability to collect and present infrastructure data is challenging. Organizations’ top concerns in this area are the ability to:

- Assess the impact of a service failure quickly.
- Identify the components that make up a service so that Service Level can be agreed with the clients and availability measurements can be identified.
- Assess the risk associated with the implementation of a change to the production environment.
- Cost and price IT services accurately.

The Configuration Management process, with the aid of related business processes, enables organizations to address these concerns effectively.

III. PROCESS POLICIES, ROLES AND RESPONSIBILITIES

The high-level activities of Configuration Management process are:

A. Planning the Configuration Management
   - Defining the scope, purpose, objectives, policies, roles and responsibilities and the process for Configuration Management.

B. Identification of Configuration Items (CIs),
   - Identifying and labeling, defining the sources for gathering and maintaining CI data in CMDB.

C. Monitor, Control and Maintain CMDB
   - Monitor for unauthorized changes to CIs and CI data in CMDB.
   - Control CI changes through Change Management. Update and maintain CI data to ensure accuracy.

D. Verification and Audit
   - Verify CI with CI data recorded in CMDB.

E. Report Metrics and Evaluate
   - Define and review metrics and targets.
   - Monitor, measure and report on metrics achievement.
   - Regular review and evaluation of process for improvement.

The detailed process activities can be obtained from ITIL Guideline for Configuration Management, refer to [2]. Besides the activities, process policies are also very important to drive the process design, as well as the roles and responsibility assignment. The policies provide a significant foundation for managing the expectations within the IT organization. The ground rules of a policy are:

- Clearly States a Fundamental Belief of the Organization
- Simply Stated and Understandable
- Supporting Principles Need to be Rationalized Using Business-Related Factors where Possible
- Implications of Adopting Principles should be Identified

Some policies are listed below.

- Policy 1: The Configuration Management process will track and manage Configuration Items (CIs) required to provide an agreed IT service.
- Policy 2: The Configuration Management Database (CMDB) represents the current known-state of the IT environment.
- Policy 3: Each CI must have an owner who is responsible for keeping the information accurate and current for CI.
- Policy 4: All CMDB changes must be authorized and implemented only by assigned personnel.
- Policy 5: Changes to CI records in the CMDB must adhere to the Change Management Process through work orders.
- Policy 6: Each CI in the CMDB shall be identifiable by its location and name.
- Policy 7: Regular exception reporting should be performed and reviewed. A formal CMDB audit should be conducted at least once a year.

Process has roles and responsibilities associated to design, develop, execute, and manage. A role within a process can be defined as a set of responsibilities. In an organization, one person can take on multiple roles, as per the requirements specific to the organization. The process accountability remains with the process owner. The Roles in the configuration management function are:

- Configuration Manager: Overall responsible for designing CMDB, Owns the implementation and execution of the Configuration Management process within the function.
- Configuration Management Process Owner: Overall responsible for the process. Monitors and reviews process performance metrics and evaluates process for improvement.
- Configuration Coordinator: Performs the CI registration and data maintenance for the CMDB.
- Configuration Item Owner: Overall responsible for their CI data quality and completeness in the CMDB.

In order to achieve high data quality and completeness in the CMDB, Configuration Item Owners are empowered to make changes to the CMDB data. Use of automated discovery tools also helps to maintain the CMDB data. Here we suggest a centralized configuration management function in order to support and maintain an enterprise-wide CMDB so that the CMDB contains all the information about the IT environment and be as accurate as it can be.

The enterprise wide CMDB can be implemented as a single physical instance for the organization, or it can be a
single logical instance that consists of several physical instances which are connected through data exchange.

The centralized configuration management function reviews and plans for the CMDB architecture and direction, implementation of tooling and automation to support the configuration management activities. The configuration management function also sets the standards, policies and processes for CIs and data under configuration management control.

Activities (tasks), roles and activities are basic elements of a process. Linking them together can be very meaningful by RACI matrix, which defines Responsible, Accountable, Consult-before, and Inform-after. A sample of RACI is shown in Table 1.

<table>
<thead>
<tr>
<th>Process Activity</th>
<th>Conf Mgr</th>
<th>Conf Cord.</th>
<th>CI Own</th>
<th>Chg Mgr</th>
<th>CAB</th>
<th>Pro Mgr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning Implement</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Identification</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Monitor/Verify CMDB</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Maintain CMDB</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify/Audit</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Report Metrics</td>
<td>A</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate Process</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
</tbody>
</table>

Table 1 Sample RACI Matrix

Figure 2 shows a possible implementation model of the Configuration Management function.

IV. TECHNOLOGY CONSIDERATIONS

Though good process design and modeling are the very basis for sound Configuration Management, process-supporting technology is necessary for implementation of the process. Some state-of-the-art technologies and software tools shall be adopted when planning and implementing enterprises IT Configuration Management.

A. Automatic CI detection technology

Automatic CI detection technology should provide the following functionality or features:

- Automatically discover IT configuration items with predetermined characteristics either periodically or upon occurrence of a defined event.
- The list of discovered CIs can be used as an audit comparison to ensure all CIs are owned and managed and to verify the limits of the production environment.
- Automatically establish all relationships with other CIs when new CIs are added to the IT infrastructure.

B. CMDB management system

As a key to the successful implementation of the logical Configuration Management database, the CMDB management system provides the glue for distributed data repositories of IT service and production environment information. Features of the CMDB management system should include the following:

- Allow definition of various levels and characteristics of configuration items and relationships within the design.
- Define the boundaries of the CMDB (i.e., what’s in, what’s out).
- Provide the ability to automatically inventory CIs, performing an initial load or verifying existing data.
- Provide a data dictionary identifying the available data, from what source it was obtained, and to who needs it.
- Provide tracking, archival, backup, and other typical database management system capabilities.
- Provide a logical database structure tied to the physical repositories.
- Provide security and audit capabilities.
- Provide the ability to interface, as appropriate, with a customer’s corporate asset management system.

C. CMDB data entry tool

The CMDB data entry tool should provide the following features:

- Permit entry of CI registration data.
- Permit batch uploads from other systems.
- Allow review of existing CMDB data based on key (e.g., CI name, work order number, RFC number, etc.).
- Update only changed data, leaving unchanged data as is.
- Require entry of and consistency in context-dependent data.
- Apply changes to all physical repositories of data referred to by the logical CMDB entry.
- Provide automatic validation of input data.

D. CMDB query tool

Ideally found in an online tool, query capability should provide authorized retrieval of Configuration Management Database (CMDB) data by various key items. CMDB data includes:
• Configuration item (CI) records (includes entries for hardware, software, documents—including the physical documents, and change, incident, and problem records)
• CI attributes and relationships (name, model, version, location, owner, status, cost, configuration parameters, and hierarchical relationships with other CIs)
• Service performance data (component usage data, resource performance data, cost data, and service metric data) that needs to be queried by cost centers (e.g., business unit)

Since CMDB data are dispersed among many repositories, the query tool must have the following capabilities:
• Locate requested data.
• Ensure the requestor is authorized to access the data.
• Retrieve requested data.
• Organize the data (e.g., sort, tally, group, etc.).
• Package data as requested (e.g., report format, data dump, hardcopy, electronic files, etc.).
• Place query results in a location specified as part of the query.

V. SUMMARY

Implementing configuration management will provide a sound basis for getting other ITIL processes work. The scope, breadth and depth of the CMDB needs to be defined step by step as other ITIL processes being implemented and applied.

• **Scope** of the CMDB deals with what type of CIs (e.g., Server, Software, Documents, etc.) would be registered in the CMDB and when do you start tracking them (e.g., when ordered or being built.)

• **Breadth** of the CMDB refers to what type of information or characteristics would be tracked for each CI. This is commonly known as CI Attributes. Examples are Total Disk Space, IP Address, Location of CI, etc.

• **Depth** of the CMDB means how deep or number of layers of CI relationship do we maintain in the CMDB. For example, do we track the Server and right down to each Network Interface Card installed? Do we track the mouse and keyboard installed?

With the key issues and considerations in the paper, IT organizations’ leaders will find a roadmap to transform IT services successfully.

REFERENCES