A Service-aware IT Configuration Library

With so much of the modern enterprise powered by IT, visibility into IT infrastructure is mission critical. But as IT infrastructure continues to grow and become more complex due to multi-cloud environments, serverless compute, and containerization, visibility into infrastructure is like tracking a moving target.

For IT to gain visibility, it faces the challenge of consolidating, maintaining, and understanding complex configuration data. Often this data is found in many different repositories, making it even harder for IT to find business service issues arising as a result of infrastructure changes.

But there’s a better way to solve these challenges. A CMDB is a purpose-built system for storing your IT infrastructure and its relationship to each other. But the CMDB doesn’t just contain information about your IT environment. It also puts business context around it and helps IT organization become service oriented. Incident management, problem management, and change management are core functions in IT service management (ITSM).

The configuration management database (CMDB) consolidates disparate IT management systems into a single system of action.

Unfortunately, many companies have struggled with CMDB projects and failed to realize the value it can provide.
They have a reputation for failed starts, lengthy implementations, and ongoing maintenance challenges. This whitepaper provides you with the fundamentals to help ensure your configuration data management project with CMDB is a success.

**Opening new value stream with CMDB**

Enterprises use CMDB as a foundation for IT service management but the value does not end there. CMDB is the foundation for IT Operational Management, Asset Management, Security Operation Management, providing Audit/Compliance capabilities.

When CMDB becomes the configuration system of record, organizations see benefits such as:

- Reduced incident volume
- Reduced number of system outages
- Improved vulnerability response
- Increased automation to respond to issues faster

Increasingly, CMDB is evolving from being applicable for ITIL to now being relevant for DevOps. IDC sees that 48% of organizations with DevOps deployed will release new code monthly or weekly. These activities are powered by Kubernetes and other container orchestration engines on PaaS or public cloud environments. A healthy CMDB is the foundation to manage changes in these dynamic environments. It also allows you to also understand the complex relationships among this infrastructure supporting critical business services.

Let’s take a detailed look at some of the leading IT organization use cases where CMDB improves existing processes and unlocks new value streams for the business.

**Experian’s CMDB success**

Experian is a global company with thousands of employees in many countries. In 2016 they began their Service Central CMDB journey with a migration from an existing primary technology asset repository to ServiceNow CMDB. They leveraged service automation and orchestration opportunities using the platform. They expanded the reach of CMDB by building an automated federated model, sourcing data from Qualys, Tanium, FireEye, and other authoritative sources. Next they leveraged CMDB to build robust and automated business service maps to further facilitate impact.
and risk assessment for internal and client facing products. Next came development of an automated method of identifying and eliminating duplicate configuration records to help further reduce manual processes. Finally, they added cloud management with support for account inventory management, along with normalization of discovery approach.

Any organization’s IT functions can benefit from adopting CMDB. Some of the primary use cases include:

• IT service management is more efficient with CMDB. Configuration Items (CIs) mapped to business services will improve the service desk readiness and resolve issues faster. When this mapping is in place, both IT and business partners are on the same page about tracking issues in impacted services. With service maps, you know which business services are affected and can plan accordingly. As a result, IT can launch or resolve incidents rapidly since they have better visibility of the infrastructure changes.

• Manage system outages in a better way. Being proactive in stopping business service outages before they start is important in improving service availability, but it also reduces the run-rate workload for IT operations teams. These teams spend huge amounts of time trying to make sense of events from their monitoring systems. Often, the first time that IT operations knows about a business service outage is when end users complain. By integrating an event management solution with your CMDB, you can tackle this problem head-on.

Event management combined with your service maps make diagnosing service outages much simpler because you can see how issues are propagating across the business service. By linking remediation actions to CIs, you don’t just diagnose service outages faster — you fix them faster.

Save more with software asset management. Asset management is usually considered a financial function. A configuration management platform can be used to track physical assets, software assets, and consumables. What if you can have software asset data in the same place where you manage IT? This way IT teams can track where are all the installed assets and their utilization in a single platform.
• Respond to security vulnerabilities faster. A single source of truth — the CMDB — is likewise a valuable tool for security management teams. The CMDB offers easy access to data, which is useful to security management. Security teams can leverage the CMDB to map threats, security incidents, and discover vulnerabilities in your IT infrastructure.

Meet compliance requirements with ease. Practically every organization in every industry today is subject to various regulatory requirements such as Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS). Additionally, many organizations are subject to federal government regulations and certification programs. Although these various regulations differ in their requirements, they all share the common goal of ensuring that sensitive data and systems are appropriately secured, and proper governance and accountability is established. The CMDB is an essential tool to help organizations meet their audit and compliance needs.

Building a Configuration Management Database (CMDB) for the Modern Enterprise

The fundamental building block of a CMDB is the CI (configuration item). A CI represents an item under configuration management, such as a router, a server, an application, or even a logical construct such as a business service.

CMDB manages data for on-premises and cloud environments. For example, it can store data from cloud resources such as virtual machines, containers, or cloud datacenters. This is to accommodate for the complex environments of today's IT operations. A properly maintained CMDB allows IT to have insight into the critical business services that run on the IT infrastructure. This allows organizations to better engage customers, drive revenues, increase efficiency, and create new business insights. Service maps give IT this visibility. They visualize the CIs that support a particular business service and how these CIs are related to improve visibility of your products and services. These service maps are derived from CIs held directly in your CMDB, connecting your business services to your infrastructure. Then you can use AI processes such as machine learning, advanced analytics,
and actionable intelligence to benefit from this visibility of your business services.

Manually entering information about CIs is time-consuming and can be error-prone. Even in a small organization, too many changes take place and manual entry cannot be depended on for very long. Yet, many organizations start out using this method to establish their CMDB before automated processes are created.

Automated technologies that can discover CIs are the most efficient, repeatable, and accurate method for populating the CMDB. The CMDB will ensure the most recent and accurate profile of the CI is loaded. Mature automated technologies also can map the relationship between business services and underlying infrastructure.

Some data cannot be gathered automatically, such as business and organizational information. Information about people cannot be gathered by a scan of the network and must be entered manually. Depending on your organization, you may have a number of other business strategic information that will require manual input, too.

Your configuration management platform should have the capability to regularly poll for or receive events from cloud resources, to automatically create CIs, and manage their life cycles as appropriate.

Keeping the Database Healthy and Trusted
Change is a major cause of service outages and yet change is an everyday part of IT infrastructures. With a healthy CMDB you can evaluate the impact of these daily changes and respond to them properly to quickly fix or prevent service outages.

Most organizations face difficult challenges when implementing a CMDB. A configuration item (CI) is the fundamental structural management unit of the CMDB. Everything IT supports is ultimately expressed in terms of CIs. Thus, the quality of CI data will be an essential tenet of your ability to effectively communicate the current state of items powering your services.

The configuration management team should be relentless in challenging the IT organization to improve CI data quality. You need to put technology and processes in place to ensure that the data within your CMDB remains accurate.
Addressing the challenge of keeping the CMDB healthy is vital. Preventing bad data is your first line of defense. This involves creating identification rules for CI and attribute population and reviewing every automation method that updates the CMDB. The second line of defense is having regular reports run of the data looking for CI issues and bringing them to the attention of the configuration management team. Common CI issues include duplicate CIs, CMDB de-duplication process can identify and reconcile duplicate CI records to improve CMDB health. Finally, regular data quality procedures must be implemented to look for defective data.

An open channel must exist between the users and the configuration management team to communicate defective CI data. A process (preferably automated) must exist to handle such defects. Most important, you don’t want to just fix the defects — you need to fix the process that allowed the defects to occur in the first place.

Many processes and people downstream of the CMDB depend on the quality and accuracy of the data in the CMDB to do their jobs. When inaccurate data affects the success of those processes, those people lose trust in the CMDB and the configuration management team.

Configuration management is an ongoing discipline in any organization. Changes come from the evolution of corporate strategies that are then translated into technology decisions that then need to be implemented.

It’s important to regularly measure your effectiveness and benefit to the organization. You should collect metrics on the following:

- How many configuration management requests are fulfilled
- CMDB defects identified and fixed
- Number of CIs missing key attributes
- Size of CMDB (only for the classes being managed in the data dictionary)
- Number of incidents and changes placed on items where there is no corresponding CI
- Number of reports designed and run
- List of IT use cases for which the CMDB is being utilized with detailed metrics on each (for example, number and type of reports produced)

When you have the tools and processes in place for a healthy CMDB, you need to keep it healthy and resolve issues as they arise. The best way to do this is to
monitor your CMDB using a CMDB health dashboard. With it you can monitor key CMDB key performance indicators (KPIs), including completeness, compliance, and correctness. In addition to aggregate scorecards, you can also drill into CMDB details for specific business services, and individual CIs allowing you to pinpoint CMDB problems and request corrective action. The CMDB health benchmarks can measure your CMDB health relative to other ServiceNow customers and industry standards.

With a healthy and service-aware CMDB, you have better capability to diagnose service issues, detect root cause problems quickly, and find resolution with reduced mean time to resolve. For example, real-world enterprises have seen results such as:

- Over 50% reduction in major incidents in spite of huge IT growth
- A decrease of 30% in false positive incidents
- 22% fewer major outages

To learn more about Configuration Management and ServiceNow CMDB, visit servicenow.com to read Configuration Management and CMDB For Dummies, ServiceNow Special Edition.