

A Configuration Management Database: Your First Line of Defense in an IT Audit

This article appeared in *“INNOVATION: The Convergence of Information Technology and Business,”* published by BMC Software.



To receive a copy of *INNOVATION: The Convergence of Information Technology and Business*, go to www.bmc.com/innovation.



A Configuration Management Database: Your First Line of Defense in an IT Audit

By Cindy Sterling

Program Executive for Compliance, BMC Software

Many forces are converging to increase the burden and cost of doing business. IT organizations must deal with complex regulatory requirements, international standards, industry frameworks, and codes of good corporate practices. They also have to grapple with internal policies needed to manage business processes. IT must not only achieve compliance with the requirements set forth in these regulations, standards, and policies, but also be able to demonstrate compliance well after the activities have been completed.

Since most of today's business processes are supported by IT, much of the compliance burden falls on IT to achieve the level of compliance required in an effective, efficient, and sustainable manner. That's why effective controls need to be established and records retained for possible examination by regulators and auditors well into the future.

When auditors knock on company doors, they come not just to evaluate whether an overall business process meets regulatory requirements. They are also interested in determining the integrity of the configuration data of the individual IT processes that support business processes. What's more, they will want to know that the actual asset configurations continue to match the baselines on record.

As a result, IT must understand and be able to show the relationships of the components of the IT environment (people, processes, and technology) to the business processes they support. IT must also be able to produce records about the configuration of these assets. This presents IT with a challenge due to the continually changing nature of the environment. Consequently, the lack of integrity of configuration data can result in significant compliance issues for the organization. In addition, it can also mean that the IT infrastructure, resources, and capabilities are not being used in an optimal manner.

Who's Your Friend?

IT professionals are turning to a well-architected configuration management database (CMDB) as a repository for the information that is critical for reliable computer operations and that can make compliance processes easier to manage and track. Also growing in popularity are standardized industry frameworks that enable companies to achieve regulatory compliance and transition to a more business-oriented approach to IT management.

Since most of today's business processes are supported by IT, much of the compliance burden falls on IT to achieve the level of compliance required in an effective, efficient, and sustainable manner.

Two important standardized frameworks play key roles. The IT Infrastructure Library (ITIL®) offers best practices in service management, while Control Objectives for Information and related Technology (COBIT) provides controls for compliance. A CMDB, in turn, provides the foundation for implementing both the ITIL and COBIT frameworks.

The CMDB offers immediate access to information about the configuration of the IT environment and changes that have been made. It is a source of reliable, detailed, current, and historic data about your business. If properly federated, a CMDB can accurately substantiate your business practices against regulatory controls, so you can breathe easy during audit times. A federated CMDB is an approach that features a centralized database linked to other



data stores with a common data model that carries information from one point to another, without the need to rewrite code.

CMDB as Facilitator

To meet regulatory compliance for auditing, IT needs to manage and track the technology, people, and processes in the IT environment from a business process perspective. A CMDB ideally facilitates this activity.

Think of a CMDB as the central repository through which IT management processes in your IT infrastructure can exchange information. The CMDB is a place where disparate sources provide information about changes, releases, configuration, assets, incidents, and so on. A CMDB should hold important information that helps IT understand the relationships of the components in the IT environment to the business processes they support. It should identify a set of configuration items and maintain all IT resources — technology assets, processes, and people — as configuration items. The CMDB should also maintain important details about those items and their relationships and facilitate two major compliance requirements:

- > Tracking and reporting
- > Configuration control and verification

To meet regulatory compliance for auditing, IT needs to manage and track the technology, people, and processes in the IT environment from a business process perspective. A CMDB ideally facilitates this activity.

Tracking and Reporting

A major compliance requirement is that all activity in the IT environment that affects business processes must be tracked and reported, creating an audit trail of activity. Tracking and reporting must be done from the perspective of the business process, and in a holistic fashion that ties together all the IT processes that support the business processes.

Many organizations create compliance reports using processes laden with manual procedures. The IT staff gathers data manually from a number of sources scattered across the enterprise, manually consolidates the data, and then manually correlates the data to business processes. This approach is time-consuming, labor-intensive, error-prone, and expensive.

The CMDB, in contrast, provides a single, comprehensive, and easily accessible source of tracking information for reporting purposes, eliminating the need for manual data gathering and consolidation. By providing automatic tracking of pertinent IT processes, and by mapping the IT processes to business processes, the CMDB ensures data integrity and facilitates significant cost reductions in compliance reporting.

CMDB — Your Single Source of Truth

Through the information maintained in the CMDB, IT can understand the impact of IT processes on business processes with respect to compliance. For example, it can facilitate answering the following questions:

- > Was compliance impacted when data used by a specific business process was migrated to another data storage device?
- > Has compliance of a specific business process been impacted by incidents and problems that have occurred? If so, what was the outcome?
- > Has compliance of a specific business process been affected by changes made to the IT infrastructure?
- > Does a specific business process meet compliance with respect to data backup procedures?

Configuration Control and Verification

Unauthorized changes expose the organization to noncompliance. For example, the deployment of an untested patch to a server operating system opens up a security hole in a financial reporting application, which results in a noncompliance status. That's why it's critical to ensure that all changes are carefully controlled through best-practice change management processes.

Here's how the CMDB can help. The CMDB can be configured to maintain:

- > A list of authorized configurations for all IT technology assets
- > A list of all people authorized to approve changes and what types of changes each person is authorized to approve
- > A list of all people authorized to implement changes and what types of changes each person is authorized to implement



Your change management application can use this data to ensure that only authorized people are approving and making changes, and that they are implementing only those changes they are authorized to implement. Autodiscovery capabilities can be added to the environment and used to continuously monitor the IT infrastructure, updating the configuration information maintained in the CMDB and automatically recording all changes, both planned and unplanned.

The CMDB maintains a mapping of IT resources to business processes. This mapping information can be used by compliance analysis and reporting mechanisms to automatically correlate events to business processes.

The configuration management application can be used to monitor the data in the CMDB to detect any changes, therefore helping to identify whether a change has resulted in an unauthorized configuration, and if so, what business processes are affected by the changes. This continual update of the CMDB provides two important functions for compliance:

- > An early warning of unauthorized change
- > An audit trail of all changes, both planned and unplanned

If it detects an unauthorized configuration that results from a change, the configuration management application can restore the offending resource to an authorized configuration and record an audit trail of this restoration in the CMDB.

Finally, and perhaps most importantly, the CMDB maintains a mapping of IT resources to business processes. This mapping information can be used by compliance analysis and reporting mechanisms to automatically correlate events to business processes. It permits tracking and reporting of the overall business process, automatically tying together the multiple IT processes involved in the overall business process.

By putting in place a CMDB and leveraging that foundation with IT service management applications that support ITIL best practices and COBIT controls, organizations can reduce the cost and effort of achieving and demonstrating compliance with government regulations, industry standards, and internal policies. What's more, compliance efforts can act as a catalyst and provide a foundation for the initiatives that align IT even more closely with the business.

For more information, visit www.bmc.com/cmdb.



About the Author

Cindy Sterling joined BMC in 1993 and has been responsible for the execution of compliance initiatives. She has held technical and management positions at BMC, supporting various product lines that include job scheduling, output management, storage, application management, and identity management.