

Chapter 4

CONFIGURATION AND ASSET MANAGEMENT

Configuration management is the process of monitoring and reviewing approved product configurations periodically while the IT tool is in production to ensure configurations are in compliance with design standards. Each IT product has a specific set of configurations (i.e., hardware or software settings). Consequently, the design should specify how the IT product will be configured to meet business requirements as any configuration changes could have a significant impact on business operations.

The product's configuration may consist of dozens, and sometimes hundreds, of different items to be set up in the system. Although in an ideal world every configuration is monitored, IT departments must manage resource costs with product efficiency by focusing their work on critical configurations only (i.e., configurations that impact the entire system, disabling the product from functioning as intended or from functioning altogether).

Other configurations considered critical include those that have a major business impact, even though they are not systemic. An example is a stock trading application that transfers data feeds to and from another system. Although

the configuration is not systemic, an error in the data feed configuration could cost the organization millions of dollars per second. Hence, the configuration is considered critical.

Sources for critical configuration

The engineering group should include a list of critical configurations to be monitored and significant, technical, and business items for periodic monitoring in the product's design.

The list is part of the design information that will be reviewed by the operations group. After the design has been discussed, the engineering group should release a final agreed list.

Note: product updates or fixes from the engineering group should include critical configuration information, including new items or updates to existing items.

Configuration monitoring method

The engineering group should also specify how critical configurations will be monitored. Use of configuration management software for automation is the preferred monitoring method as the software allows the entry of standard settings for different product components. These entries could be file versions, registry settings, database objects, or file modification dates. The software pulls the settings from the product, compares them to the standards specified by the operations group in its database, and reports any noncompliance issues.

Although an automated control is preferred, sometimes a manual control has to be used. This is often the case in small organizations where purchasing a configuration management

software is not feasible or in environments where a configuration management software does not work with the IT product in use. An example of a manual control is the engineering group's identification of critical text or editable files. After the IT product is in production, a screen shot of the file's content is taken that is stored in an electronic library. Periodic screen shots are then taken and compared to the original library copy.

Configuration review frequency

The engineering group should specify if critical configurations need to be monitored in real time or periodically (e.g., weekly or monthly). Configuration review frequencies should be discussed with the operations group during the design review phase to balance existing resources and costs properly.

Reconciliation process

The compliance report should be reviewed, and non-compliance items must be reconciled, by querying the product support team on items that do not match approved standards. Below is a list of sample reconciliation process questions:

1. Was a new authorized update installed on the product?
2. Has the configuration on the product server changed?
Was this an authorized change?
3. If an authorized change took place, did the engineer forget to update the configuration process?
4. Do all product servers have the same configuration?
5. If a noncompliance item is discovered in the staging phase, is a current staging test taking place?

Integration into PLCM process

Configuration management should be a part of all PLCM processes affecting the IT product's configuration, such as product testing and implementation. In addition, a test run for new critical configurations should take place during the testing stage. For instance, can a new critical configuration be monitored by the existing configuration management process? If so, a test should be performed to verify that monitoring is taking place.

Furthermore, if a change is made to an existing critical configuration item, testing should take place to verify that the compliance report is updated correctly. If new hardware infrastructure has to be added, the new object must be incorporated into the configuration management process to determine whether it is configured as expected. During the decommission phase, the object that is being phased out must be removed from the configuration management process.

Asset management

Asset management is closely related to product configuration management. Key considerations for asset management activities include product licensing and inventory reconciliation.

Product licensing. A product may have a vendor license or use a component that requires licensing. Licensing information is part of the product's configuration and should be part of the engineering group's released product design. If a product component does not have a license, the component is in noncompliance with design standards. Licensing information should be included in the configuration and asset document.

The document should specify when the vendor will end support of the product version in use and whether there is an option for extended support.

The engineering and operations groups should do a periodic review of all licensing requirements. If a date is specified pertaining to when vendor support will be discontinued, the engineering group must plan design updates for a replacement product, which may consist of a newer product version or an entirely new application.

Inventory reconciliation. The product design should specify the infrastructure and hardware needed for the product.

The operations group should conduct periodic inventory reconciliations to verify that infrastructure components specified in the design are active and in production. The product inventory report should be included in the configuration management document.

Configuration and asset management document

The operations group should create a configuration and asset management document that includes the following sections:

1. Critical configuration sources.
2. Configuration monitoring method.
3. Configuration review frequency.
4. Reconciliation process.
5. Product inventory reconciliation.
6. Product licensing.

For special consideration

Many organizations spend time and money on anti-virus, anti-spam, and anti-spyware programs to secure their network. As important as these kinds of software are, organizations also must focus as much attention on the configuration management process for their IT products. Consequently, a configuration management process should be in place before the product is implemented in production. This will provide greater assurance about the product's functionality.

