ITIL® Poster Series #39

CMS and DML

Good e-Learning

Introduction

Software asset management is an important responsibility for any organisation. Failure to manage these assets may result in the organisation over-spending by buying licences that are not required, or operating illegally, by using software without the required licence. The IT service provider must be able to provide evidence that the software they use is legal. Ideally, these will be compliant with the international standard for SAM, ISO/IEC 19770.

Effective SAM is dependent on use of appropriate tools, including a Configuration Management System (CMS) and a definitive media library (DML). Here we examine how these tools are used, and the relationship between them, to ensure effective software asset management.

The CMS and DML

The management of software assets presents challenge that service providers must meet to both remain legal, and avoid unnecessary expenditure. There are risks involved with software that do not apply to other asset types, specifically the potential for the illegal use of software where the licences have not been purchased, and the risk of not being able to prove that a licence has been purchased, forcing the purchase of another licence. There is also a risk that money will be wasted by purchasing more licences than are required, due to an inability to track the use of the software. To address these concerns, organisations should implement a software asset management (SAM) process to track the software in use, and the software licences and activation codes.

ITIL recommends the use of the secure libraries and stores to protect these assets. A secure library is a collection of software, electronic or document CIs of known type and status, with access restricted so that copies of these are only released in accordance with the agreed process. Every software asset purchased should have been recorded in the CMS; the DML provides the location for the storage of the master copies of software items themselves, and enforces controls around their release, by requiring change management approval whenever items are to be moved into or out of them. In practice this media library may consist of one or more storage areas for the electronic copies, and a physical store to hold any physical master copies, such as disks, in a fireproof safe.

The DML should include definitive copies of purchased software (along with licence documents or information), as well as software developed on site. Master copies of controlled documentation for a system are also stored in the DML in electronic form.

The DML is a foundation for release and deployment management. Electronic assets in the DML are held within the SKMS, and every item in the DML is a CI. The diagrams below shows the relationship between the DML and a CMDB in the CMS, and how copies of the software are released following the appropriate authorisation.

THE RELATIONSHIP BETWEEN THE CMS AND THE DML

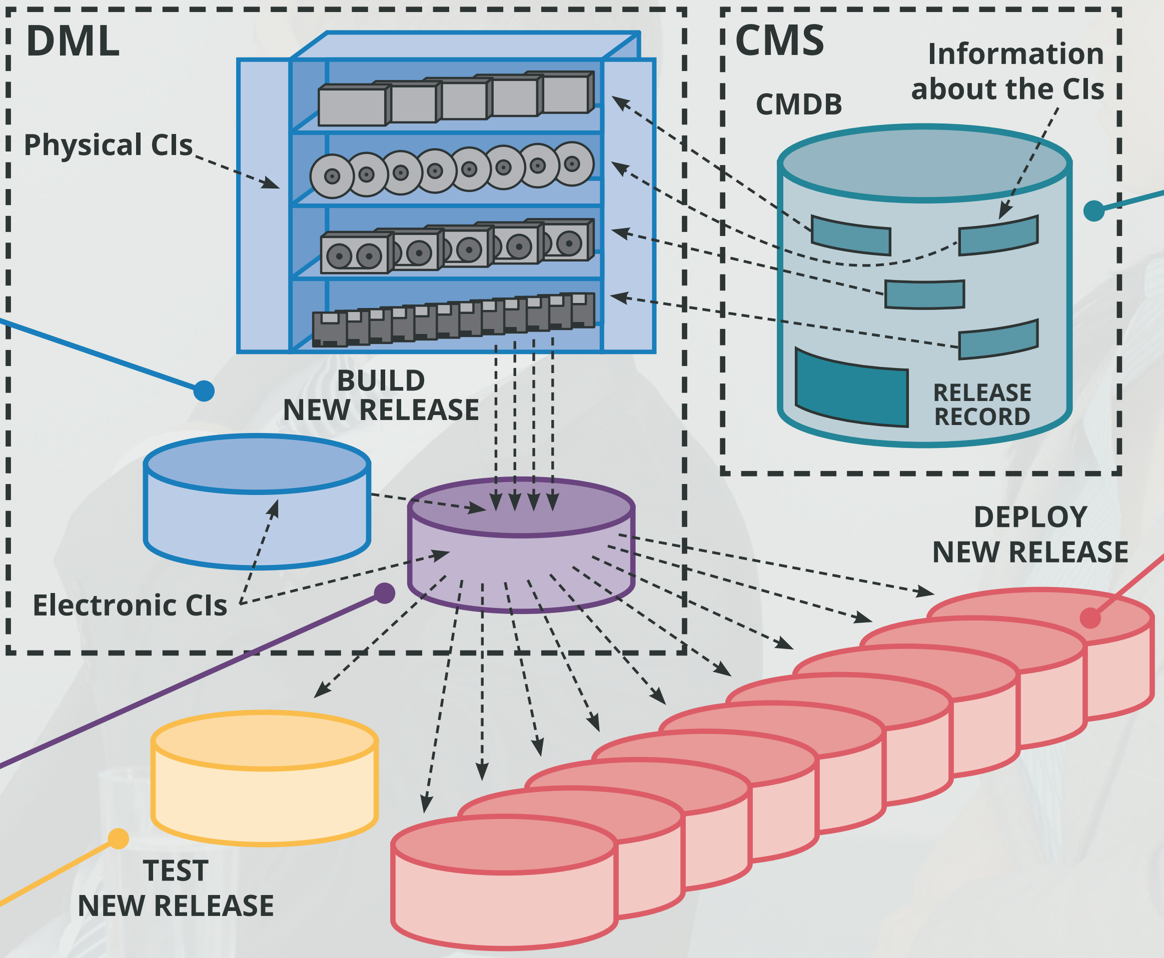
The Definitive Media Library will consist of an electronic store, for electronic versions of the software and licences, and a secure safe containing the disks or other physical media, and any physical licence documents.

Each software asset in the DML will have a corresponding CI record in the CMS.

Following authorisation from change management, the DML provides copies of the software that is to be released (ensuring that sufficient licences are available, and reducing the available licence count).

The new release is build.

The new release is treated



Here we can see hoe the CMS holds information regarding assets (in this case software assets) within a CMDB.

When software is to be released into the live environment, a Release record will detail which software CIs are to be included.

The release is deployed.

The CMS is updated and the Change closed, following evaluation.

NOTE: Definitive spares

In addition to the definitive library used for software asset management, ITIL guidance also recommends that an area should be set aside for the secure storage of definitive hardware spares.

Ensuring that the service provider has access to examples of the hardware in use in the live environment, provides assurance that should the operational hardware fail, the service can be restored by employing these spares. It is important that the equipment held in the definitive hardware store is an exact match in terms of configuration, build levels etc. for the devices in live use. They can then be used in a controlled manner as required.

When the requirement has passed (for example when the failing device has been repaired or replaced) the items are returned to the spares store. Details of these components should be recorded in the CMS; their deployment into the live environment, and return to the definitive store when no longer required should be under the control of change management.