

## In This Issue:

Guest Authors  
Provide Their  
Experience:

- CMDBs for IT Asset Managers
- Technology escrow for Software Asset Managers

**Industry Event: The Annual Conference of IT Asset Managers, November 7-9, 2007 Palm Springs, CA**

## About the Author

Krzysztof (Chris) Baczkiewicz is Eracent's IT Standards Support Manager. Chris actively works with customers, ISO/IEC and other groups to promulgate best practices for the business of IT.

## Contact Eracent

Jenny.Schuchert@eracent.com

+1.412.221.1398

Sales@eracent.com

+1.908.537.6520

www.eracent.com

## What Every IT Asset Manager Should Know about CMDBs

*Guest Author Krzysztof (Chris) Baczkiewicz, Eracent*

The frequently used abbreviation CMDB stands for Configuration Management Database. In the ITIL (IT Infrastructure Library) guidelines, a CMDB is any database that is part of configuration management. That means the CMDB contains information about IT service configurations. ITIL is, after all, a service management model for IT.



Let's review some basic concepts that can help explain the role of the CMDB. A configuration item or CI is simply the elements that comprise a specific technology grouping that is needed by a user. In order to use this specific technology grouping and to offer it as a service to users, the additional components necessary to deliver that service must be identified. The term IT service configuration is used to describe everything that influences the ability to deliver the service with the configured item.

An IT service may include hardware, the software installed on the hardware, and the information about how the components relate to each other and the users. With ITIL v 3, the model now includes a service lifecycle that helps identify the steps necessary to build and maintain these services.

Selecting the data to be placed in the CMDB can be one of the most difficult aspects of implementing configuration management as part of service management. Because of the different informational needs associated with services, there is no one right answer. An example of a responsibility defined as a service is the requirement to maintain the enterprise's desktop hardware with the technical specifications necessary to enable the CIO's strategic direction. This service contains information about the hardware elements of the desktops and the status of those computers, along with information about the CIO's strategic direction. In this case, the CI does not include the software that is installed on the hardware.

Bottom line, IT Asset Managers are responsible for information about every hardware and software element. The relationships between these elements from an operational, financial and contractual perspective are also part of the information that IT asset management collects. It is a logical leap to consider an IT asset management repository as a CMDB. Additional service attribute data that makes a service unique can be linked with the IT asset management data to build a robust basis for service management.

Data from other sources can also be linked such as the incidents related to a CI. The CMDB can contain the CI to incident relationship and perhaps even details about the incident. It is clear that services dictate what data is needed for a particular service and determining the "right content" for the CMDB is a difficult task.

## For More Information on These Topics:

More information on the business of managing IT, use the Eracent Information Center. Free access is available via a password. To access or register, go to [www.eracent.com](http://www.eracent.com) and click on Info Center.

Eracent provides solutions to manage the business of IT. To improve the breadth and accuracy of asset inventory, software compliance management or attain value from lifecycle management of assets, contact Eracent.

## About the Author

Saul Marcus is a product manager at Iron Mountain's Digital division. For more information on technology escrow services from Iron Mountain, visit [ironmountain.com/ipm](http://ironmountain.com/ipm)

[saul.marcus@ironmountain.com](mailto:saul.marcus@ironmountain.com)

Organizations with IT asset management business practices and automation to support those processes have great capability to build and maintain service lifecycles that are accurate and deliverable.

## Is Your Business Vulnerable? Why Software Asset Managers Should Prioritize Escrow

*Guest Author Saul Marcus, Iron Mountain*



Every company, in every industry, has software applications that are absolutely critical to the business. While the value of protecting these intellectual property assets is widely recognized, most companies are still at risk of suffering serious losses in revenue or productivity if their mission-critical software vendor goes out of business, is acquired or is unable to continue supporting the software.

Technology escrow is the safety net that assures access to source code and other proprietary information if needed — but only if executed correctly.

Technology escrow is an established part of vendor management and business continuity best practices. The escrow management role is now expanding to include the challenges presented by compliance regulations. With escrow now part of the corporate compliance strategy, it directly impacts Software Asset Managers, particularly if your organization is:

- Traded publicly
- In a regulated industry
- Dependent on mission critical third party software
- Required to have certain automation in place

Too many companies manage escrow on an ad hoc basis, without formal processes and without adequate risk analysis. Over time, most have no way of determining whether vendors are in compliance with escrow terms and conditions in the software agreements. Software Asset Managers must inquire:

- How do I know which of my applications are at risk because of inadequate escrow enforcement?
- Are there risk assessment tools that can help me make better decisions about software escrow protection?
- How can I best leverage technology escrow and software asset management processes, automation and data?

Working with a vendor to perform a comprehensive, integrated escrow audit measures the level of risk enterprise-wide, identifies gaps to be closed and establishes a consistent, repeatable escrow process. Software Asset Managers, already well-aware of the power of asset information and the importance of proactive audits have a complementary ally with escrow management for software.