

A Pragmatist's Guide to Structuring IT Asset Data

By Scott Parkin, LANDesk ITSM Product Manager

January 2008

At the core of every task is relevant data. To effectively plan, execute, and report on critical business activities you need quick and effective access to the right key facts.

This is a challenge for any business manager, but is especially difficult for IT asset managers where key asset data is spread across multiple applications, departments, disciplines, and sources. The IT asset manager needs to aggregate, analyze, and act on data from Purchasing, Finance, IT, Service Desk, Facilities, Security, Operations, Human Resources and others, and may be pulling data from spreadsheets, expert financial systems, word processing documents, PDFs, drawing or modeling tools, and even handwritten notes.

That's a vast and complex stew of data, and attempting to order that data is a daunting task. The key is to start with a few key facts for each asset and to work forward from there, expanding as needed from a strong foundation.

I call it the KOALA factor—Key costs, Ownership, Accountability, Lifecycle status, and Assignment. If you can track these core facts for your IT assets, you can provide an at least rudimentary response to the vast majority of the planning, compliance, and procurement tasks in the short term, and that data can give you the foundations for extended service delivery and support (CMDB) going forward.

- **Key costs**—acquisition, maintenance, and replacement/retirement. This is the most time- and effort-intensive element of IT asset management, and will require the most resource to implement.
- **Track initial acquisition costs**, including asset purchase, required peripheral or supporting devices, operating system and software (as needed), and service contracts.

Most of this data will come from purchase orders; some will need to be calculated as a pro-rata share of a bulk purchase or license agreement.

For new purchases, update your purchasing process to include calculating and tracking this data in your asset record; for existing assets you will need to create a project to go back and aggregate/calculate this information and add it to your asset records.

- **Track ongoing maintenance costs**, including annual service contracts, upgrade or replacement parts, and the costs associated with Service Desk incidents for each device.

Ideally this information is collected at the time of purchase/service and is immediately attached to the asset's service history record as a function of your established process. You should update your Incident management process to support this, whether you update the asset record manually or through automated technology.

This can be the single most daunting task in the mix—extracting and aggregating historical data for existing assets is a gargantuan task. Many organizations choose to simply start tracking this data as of a specific date and leave existing data unstructured. This is a good method for those organizations that are resource constrained and willing to wait for highly qualified data.

- **Identify replacement costs** for hardware, software, and infrastructure elements. Remember to include both disposal costs for existing assets and install/deployment costs for new assets.

For commodity items such as end user hardware (desktop, laptop) and software, these costs should be predictable within a range and will tend to be updated once a year as new contracts are negotiated.

For high-impact or high-value items the cost of purchase may only be a small part of the total costs, and those costs may be difficult to estimate. This data is intended for planning purposes and should be reviewed at the time of planning, so supply a best estimate with supporting documentation to be used as a starting point for further research, not as an authoritative declaration.

The key benefit here is being able to quickly view approximate costs for individual assets, to aggregate that data by department or cost center, and to use that data in research and planning efforts.

These key costs are supplemental to the detailed cost accounting performed by the Finance team, and are intended to inform purchase, resource, and budget planning—not to provide detailed cost data to financial auditors. Understanding this intended use for IT asset cost data will help you reduce the complexity of your asset repository and keep expectations clear.

- **Ownership**—whose books carry the costs; usually a department or cost center as opposed to an individual or a signing manager. For shared or infrastructure assets there may be more than one owner, with a percentage of ownership assigned to different departments.

The primary goal for this ownership data is to enable simple accountability for an asset's use in providing value to the organization, to support approvals and decision making processes, and to enable simple cost aggregation for planning and budgeting purposes.

In conjunction with Accountability data, Ownership enables IT asset managers to support both compliance audit and strategic planning efforts by providing easy lookup of the high level group an asset belongs to. This also supports internal change control and provides insight for change advisory board membership for critical IT assets.

- **Accountability**—who is responsible to ensure that the asset is functional and providing the value for which it was purchased.

For infrastructure elements there will typically be several accountable people. For example, a database server might include the following accountabilities depending on functional role:

- **Device maintenance**—IT administrator(s) responsible for the physical maintenance of the server hardware. This person may also be responsible to configure that server with the core database application.
- **DBA**—one or more people responsible to create and maintain the actual databases. This might include access control, table creation and maintenance, software updates, and general database engine maintenance.
- **Data owners**—the individual contributors responsible to ensure that each database contains the right information for their respective purposes.
- **Continuity/Disaster recovery**—person responsible to ensure that database files are backed up and a plan is in place to restore or recover from unexpected loss.

The goal here is to provide quick and easy lookup of accountable people for both audit and business management purposes. Simple analysis enables asset managers to identify gaps in coverage and ensure input to asset decisions by key stakeholders.

For end user devices or software, there may only be a single IT accountability—or the assignee and the accountable person may be the same. The goal here is flexibility to track any and all people who may be accountable for content, configuration, or maintenance of the asset.

- **Lifecycle status**—where in its functional lifecycle a particular asset is at the moment, and whether it's capable of providing its intended value. This is the foundation datum for reconciling the asset's planned use versus actual use.

Oddly, this is both the most important and the most neglected asset data point. If you know the current lifecycle state of an asset at any moment in time you can intelligently plan IT update/replacement, budget, IMAC (install, move, add, change), and procurement activities.

For example, if you know that an asset is available but not assigned, you can manage internal stores and plan inventory levels—or identify key assets that are not providing direct value. If you know as asset is ordered but not received, you may need to track a shipment status. If you know that an asset is retired, you can begin physical recovery and disposal activities.

- **Assignment**—who physically possesses the asset.

This is distinctly different from ownership (financial burden) or accountability (who answers for asset integrity). Assignment tracks the actual possession—and presumable use—of the asset.

As obvious as this seems, many organizations can't physically verify either the presence or use of many key assets. In conjunction with lifecycle status, assignment data gives the organization the information needed to physically account for critical assets and ensure effective use.

For active commodity assets accountability and assignment may be to the same person. For active service or network infrastructure assets they will tend to be different. For inactive assets accountability may be the asset team and assignment may be a store room. Having the data to physically locate an asset closes the loop on accountability and many regulatory requirements.

The key issue here is to resist the urge to track too much asset information.

Starting with the Koala factor will provide the core data most organizations need to demonstrate immediate and significant value to both IT and the business. Start small and track a few key elements, then expand asset data only to meet specific needs tied to specific accountabilities.

That will help tame the vast stew of available data and make it specifically and pragmatically useful. ■