



KOALA in Depth: Accountability—Foundation for Stakeholder Engagement

This is the third in a series expanding on the principles of the KOALA Factor, first introduced in “A Pragmatists Guide to Structuring IT Asset Data.” The KOALA Factor is—Key costs, Ownership, Accountability, Lifecycle status, and Assignment. The premise is that if you can track these core facts for your IT assets, you can provide at least a 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.

Asset accountability is more than simple assignment tracking—it’s going to the effort to understand who the key stakeholders for an asset or service are, then maintaining the discipline to include the right people in relevant maintenance, change/update, strategic deployment, and other planning activities and IT management processes.

The specific value of asset accountability tracking is risk mitigation and operational efficiency management. By engaging the right people in pre-planning or strategy sessions you can identify and resolve potential conflicts or dependencies before they have an impact on purchasing, budgets, or service levels.

Similarly, informing stakeholders of decisions, plans, and milestones that affect the assets under their purview helps ensure effective forward planning and daily operational response.

This is the essence of successful IT governance—to engage the right stakeholders at the right time to help increase efficiency (budget, allocation, and operational) and reduce risk.

Distinguishing Accountability from Ownership and Assignment

The fact is that most organizations have not spent the time or effort to identify who the relevant stakeholders for an asset are—at best we tend to track current assignment and original ownership and consider our work done.

Unfortunately, that leaves out both operational maintenance and overall strategic context for the asset, and as a result robs planners on both sides of valuable knowledge already captured within the organization. Too often, high-level planners have little understanding of operational—with the reverse being equally true.

While ownership focuses on high-level business value and low-

level cost accounting, accountability deals more directly with operational planning, process control, and risk mitigation. Similarly, accountability focuses on contextualized value of an asset, where assignment deals more directly with immediate use and tangible control.

Together, these three categories define the distinct roles necessary for overall process control and value management, and help distinguish the processes needed to fulfill the responsibilities inherent in those roles. That’s why the KOALA model recommends that you track ownership, accountability, and asset assignment as three separate facts—even when the roles overlap.

Understand Current Accountabilities

Accountability is tracked at two primary levels—operational accountability for the underlying components, and strategic accountability for the business services derived from those components.

These are entirely different types of stakeholder, but each is equally important. Inefficiencies and functional collisions occur when operational maintenance is disconnected from strategic service delivery. The first step is to track both categories within your asset repository.

This is a key consideration—your asset repository should track not only the component assets, but also the services derived from them. This enables you to independently track the unique accountabilities associated with each element.

Underlying Components—Operational Accountability

At the very least you should track accountability for infrastructure assets which historically bear a greater share of cost burdens. Start with key assets—the servers, databases, applications, and network components that underlie your primary business services. This includes both tangible and virtual machines, as well as logical assets and software licenses.

If it makes sense for your organization you may choose to extend accountability tracking to workgroup assets (printers, office equipment, etc.) and end user assets (desktops, laptops, cell phones, etc.) as needed to meet your internal goals.

Virtual assets are often misunderstood as simple software

applications. The fact is that virtual assets are often more difficult to account for than physical assets precisely because they are not immediately tangible—which makes managing that accountability even more critical.

Consider the example of a single server that hosts multiple virtual servers. There is the host server device and its applications, as well as the guest virtual servers and their applications—as well as the data generated at both the host and guest level. Each machine (real or virtual) may be controlled by a different group in the organization, and with modern VM steering and consolidation utilities the location of any single virtual server could change dynamically.

The matrix of accountability can become quite complex if you attempt to take it as a single management exercise. This is precisely why it's crucial to track not only the logical aggregate asset, but each component asset as an independent entity within the same asset repository. The ability to relate asset and their individual accountabilities within the same object repository is what enables proper risk management and operational planning.

With the emergence and commonality of virtualization technologies into both the desktop and datacenter environment, this trend shows no evidence of slowing.

You should track each accountable stakeholder by name and role so you can quickly distinguish who can respond to a specific inquiry.

For tangible assets, accountability tends to be very straight-forward:

- *Physical / facilities*—who is responsible to plan and provide power, cooling, rack or floor space, and connectivity. This may be one or several people, including datacenter facilities and/or network technicians.
- *Configuration maintenance*—who is responsible to ensure that the device is both physically configured and logically configured to meet its primary intent. In many cases this is the same as the assignee, but separate tracking is useful—especially in the datacenter where each device may have a separate administrator.
- *Application maintenance*—who is responsible for the individual applications running on the device. Accountable stakeholders could include application administrators, database administrators, and individual service consumers.
- *Data owners*—who is responsible for the security and integrity of the data itself. This can be a little trickier to track, but ultimately the reason for all other components is to produce and manipulate the data itself, so understanding who has accountability for the data housed in an infrastructure components will directly feed impact analysis activities.

For virtual machines or for logical assets that consist of a collection

of tangible assets (such as a cluster or SAN), accountability is the same as for tangible assets with the exception that physical/facilities accountability is no longer relevant. Since the host or component devices are each independent assets with their own accountability lists, there's no direct need to redundantly track that information within the virtual or logical asset itself; the focus is on configuration and application maintenance.

For software assets accountability is slightly different. Because a single software license often governs multiple installed instances of that software title, the license itself needs to be an independent asset with its own accountability. In this case the only true accountable person is the license administrator; all other considerations are covered by the application instance maintenance associated with the host device itself.

It's possible to break accountability down into even finer distinctions depending on your specific service management or compliance reporting needs. The goal is to maintain the smallest complete list of accountable stakeholders that you can to minimize maintenance burden.

Derived Services—Strategic Accountability

Ultimately, the purpose of low-level infrastructure components is to enable a high-level business service that provides strategic value to the business itself. As with logical or virtual assets, a strategic service is a collection of those low-level components that inherits those operational accountabilities.

Your asset repository should contain records for these high-level deliverables that aggregate hardware, software, databases, and utilities—and you should track accountable stakeholders for those aggregate services separately from those associated with the individual components. More importantly, both components and derived services should recognize their relationship to the other to enable impact and risk analysis.

Who the accountable stakeholders are will vary widely depending on the service, your business, and your service management framework. Ultimately, this list forms the basis of a change advisory board with responsibility to manage both service availability and continuity for the business.

Typically, you should track:

- *Corporate sponsor*—who interfaces with the business to ensure funding, relevance, and adoption of the service. This is normally a senior executive.
- *Service owner*—who is ultimately responsible for driving definition and creation of this particular service. This is normally a project manager or solutions architect.
- *Service delivery manager*—who is responsible to physically deliver the service. This is normally a high-level IT manager

with direct access to datacenter and network engineers.

- *Service support manager*—who is responsible to identify and resolve problems with the service itself. This is normally a high-level service desk manager.

Again, the goal here is to document who makes decisions around how the service is defined and delivered, as well as the key enablers needed to plan rollout or change.

This data will feed into your service management strategy; the asset repository is a sensible place to store that information not only for service infrastructure but for other key assets as well.

Leverage Accountability to Drive Risk Analysis and Planning

An effective asset repository is a central resource accessible to both service management and IT operations management organizations, and your IT asset management team functions as the common contact point or vector for critical information.

Just as importantly, no single person is required to understand all possible accountabilities—rather, the primary stakeholder for each asset or service maintains the much smaller list of additional accountable stakeholders and lets the asset repository be the integration point.

This use of IT asset management processes and the asset repository can now drive a series of key planning, change, and risk analysis activities for both operations and service management.

- *Risk analysis*—the asset repository comprehends the relationships among asset components and derived services, enabling not just component stakeholders to be consulted, but service stakeholders as well.
- *Scheduled maintenance*—technicians can directly look up component stakeholders and provide proactive notification. Internal processes can then inform additional stakeholders as needed to enable scheduling, impact mitigation, and other activities to ensure service availability and continuity.
- *Refresh/replacement planning*—the component asset record contains an out-of service, warranty expiration, and/or lease return date as well as immediate stakeholders and related service-level stakeholders. This enables a well-defined process to notify top-level accountable stakeholders who can then drive their own planning and budgeting activities.
- *Change planning*—by leveraging risk analysis and accountability data for both components and services, the asset repository can now directly inform the change advisory board as it plans out impact, rollout, and mitigation activities.

By storing simple accountability information at both the component and derived service level in your asset repository, you create the vectors that enable proactive notification and stakeholder involvement for all fundamental processes. The rest is a matter of human discipline by your project teams.

Conclusion: Accountability Enables Active Risk Mitigation

The vast majority of asset, service, and project data exists within your organization; the challenge is to create vectors and an aggregation point to get the right people in contact with each other when operational management events occur.

IT asset management discipline in conjunction with an effective asset repository provides both, and enables your existing processes to execute more effectively and provide greater insight into impacts and risks from those activities. The key is to get the right people involved in the decisions in a timely manner. The KOALA model enables your IT asset management team to add that context data with minimal impact on those processes.

The discipline around Ownership ensures that the asset provides optimal value to the business, and discipline around Accountability ensures that each asset functions according to plan as a component of that business service. While this discipline can have value for any asset, it is especially critical for infrastructure and datacenter assets.

Using a centralized asset repository to track who has direct operational interest in an individual managed asset directly feeds command and control processes and ensures that the right people are consulted when that asset changes status—whether as a result of planned change, or discovered (unplanned) event.

By supporting both process control and tracking discipline, the asset repository can function as the authoritative data source to feed operational management activities, whether from a service management, an operations management, or an IT development standpoint. Making sure that relevant stakeholders are properly involved at moments of change is the critical step to effective IT governance. ■