



IT Asset Management: *Key Considerations in the Application of Automatic Identification Technology for IT Assets*

April, 2010

**By
James Clark
Chief Operating Officer
XIO Strategies, Inc.**

Today's organizations are faced with an array of challenges associated with identifying, locating, tracking, maintaining, and replacing their Information Technology (IT) assets. This paper will discuss a number of prevalent issues, and offer insight into industry best practices related to Information Technology Asset Management (ITAM) that produce tangible benefits for organizational operations. As part of the discussion, we will focus on the role of Automatic Identification Technology (AIT), which can be used to identify assets, streamline business processes, and improve data accuracy, while considering the use of AIT within IT operations.

This white paper will provide an overview of ITAM and look at both the physical and electronic identification processes, with the implications of AIT addressed throughout the document.

Section I: IT Asset Management - Overview

IT Asset Management encompasses the practices and procedures for controlling assets used within IT operations. In the broadest sense, “assets” can include hardware, software, and other peripherals, in addition to other less tangible components such as storage capacity and software licenses. For the purposes of this paper, we are concerned with the physical assets, which include desktops, laptops, communication devices, printers, servers, disk drives, data storage devices, and other hardware.

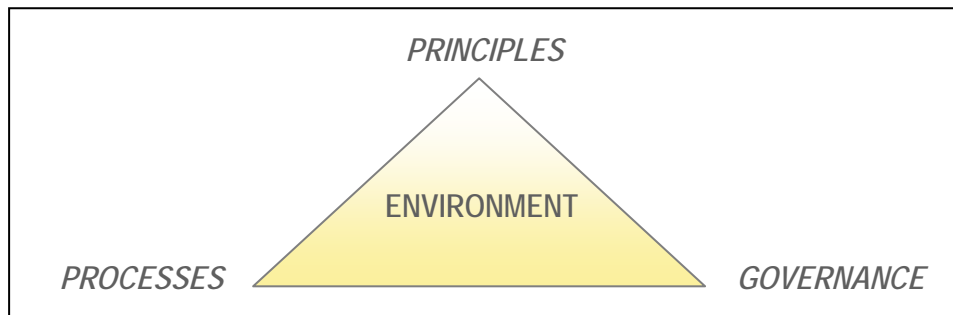
Principles

A 2005 article in *Information Technology Asset Knowledge* provided a good overview of the principles surrounding successful ITAM implementation and execution.* These strategic principles can help provide clear guidance and direction. The article advised organizations to:

- 1) Define “asset management” up front.
- 2) Define goals and align to value.
- 3) Understand the need for data accuracy, but be realistic.
- 4) Develop a total cost of ownership baseline.
- 5) Define a three-way match reconciliation methodology, but let the infrastructure manage IT asset management.
- 6) Maintain integration as a key goal of an IT asset management initiative.
- 7) Define business intelligence and analytic deliverables up front.

A few of the principles are worth expanding upon. First, understanding the total cost of ownership (TCO) is critical to assessing the cost of IT operations. Lifecycle events, including acquisition, delivery, installation, moves and changes, payment, maintenance, replacement, and disposal must be factored into the equation. These processes must be clearly understood in order to minimize unanticipated and undesired effort. Additionally, performance and process improvement cannot be measured unless a baseline is established.

TCO also relates to the third principle above, understanding the need for data accuracy. Without accurate data, existing processes will take longer, supplemental processes will be used in reaction to data errors or missing data, and effort will be expended to correct errors. These all increase the total cost of ownership, regardless of whether the IT network is managed in-house or outsourced, as is common practice today. For these relationships, minimizing the asset management costs is key to both parties.



*Mallet, Roger (2005), “Asset Management: Finding Success Where Others Have Failed,” *Information Technology Asset Knowledge*, 2 (1): 9-14.

Processes

The processes for asset management in the IT arena are very similar to the asset management processes in industrial operations. Assets must be identified in order to distinguish different instances of similar items (serial numbers), identify specific production runs (lot or batch numbers), or identify specific form, fit, or function attributes (part numbers). Item-level identification also needs to be accessible for multiple purposes (e.g., procurement, inventory, order fulfillment, assignment, and authorization).

In addition to identifying assets, data about those assets must be integrated to support business and operational functions. Proper accounting and financial management is supported through fixed asset accounting, procurement, maintenance, upgrade, and disposition processes. High operational performance is achieved by having the right assets in the right place, at the right time. These same processes — procurement, delivery, inventory, etc. — apply to IT assets.

Governance

The primary goals for information technology governance are to: 1) ensure that the investments in IT generate business or operational value, and 2) mitigate the risks that are associated with IT. These can be achieved by implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, infrastructure, etc.

The greatest challenge in meeting the strategic goals is finding appropriate metrics that truly reflect progress toward the goals while not imposing an undue burden in their collection. Once the metrics have been defined, data can be collected automatically with identification and monitoring technologies such as serialization, Item Unique Identification (IUID), Radio Frequency Identification (RFID), and network management systems. Automating the data collection should occur in conjunction with process review or reengineering to standardize the processes that collect, review, and use the underlying data.

Environment

A number of environmental factors influence the complexity of IT asset management. The size and complexity of the organization, frequency with which assets are moved, environmental conditions the assets will be used in or moved through, and security requirements are just some of the factors that will impact an organization's ability to effectively execute IT asset management. Different environments may drive an organization to select different technologies to support the IT business processes.

Section II: Physical IT Asset Management

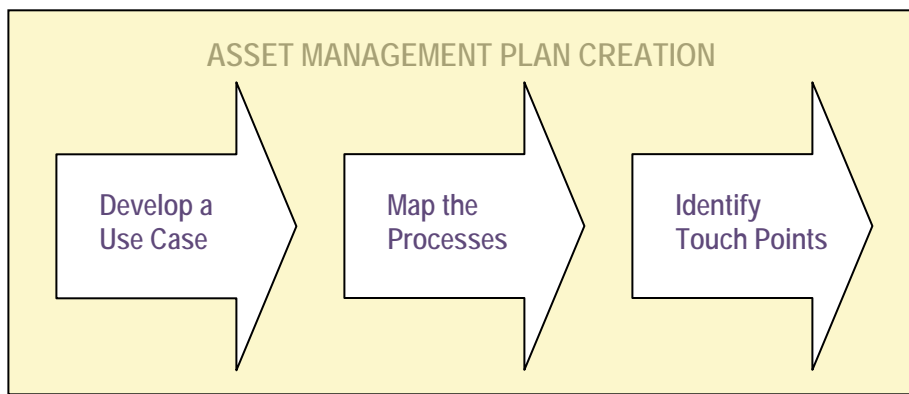
The goal of an IT Asset Management program is to determine the following about any given asset: its *identity*, its *location*, and its *condition*. The way in which management prioritizes these will dictate the requirements of the specific program. Regardless of the degree to which an asset is to be physically marked, the components of a Physical IT asset management system include the following:

- A **unique identifier**. For a Physical IT asset management system to be successful, a unique identifier must be assigned to each physical asset that is to be managed. In most cases this will be the item's serial number. However some asset management initiatives such as the Department of Defense's (DoD) Item Unique Identification mandates are augmenting the item serial number with data elements such as enterprise identifier and in some cases part, batch, or lot number, to provide a truly unique identifier. Also, some organizations will assign an internal identifier to the asset (an asset ID). In this case, it is important that all unique identifiers are linked in the system of record.

- A **physical mark** on the asset “labeling” it with the unique identifier. Ideally the physical mark will include both human and machine readable formats (barcode, RFID, etc.) to facilitate automated data collection.
- A **data collection device**. Depending upon the technology used for the physical marking (barcode, RFID, etc.) a device is required to capture and decode the machine readable data.
- A **system of record**. The asset data need to reside somewhere.

Planning

Whether IT operations are managed internally or through outsourcing arrangements, oversight of the purchase, installation, maintenance, management, and disposal processes and the physical infrastructure and network architecture must be provided. Therefore it is important that a solid physical Asset Management plan be created.



Good planning begins with developing a *use case* or concept of operations. The use case will assist in organizing the requirements, defining the user interactions and identifying the data flow for an asset management system. The first step in the development of the use case is to clearly define stakeholders and expectations. This prevents any potential miscommunication and provides an opportunity to measure the success of the asset management implementation.

The second step is to *map the processes*. In the case of asset management, this includes the processes surrounding the major milestones in the life of the asset: delivery, inventory, maintenance, and disposal and replacement.

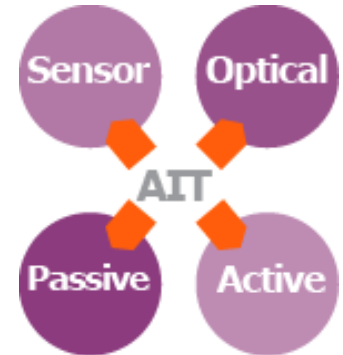
The next step is to identify the choke and touch points for the asset. A *choke point* is any point in the process through which all of the assets will flow. If the initial delivery process flows through one location every time, this is a choke point. A *touch point* is any time in the process in which a human may physically interact with the asset. Performing a periodic inventory or maintenance on an asset can be considered a touch point. Both choke and touch points are good candidates for data collection on the asset.

Identification

An essential component to managing assets is the ability to identify each particular asset. In the physical environment, this is usually done through part marking, during which a part number or serial number is applied. Part numbers distinguish the class or type of item, while a serial number distinguishes each individual instance of the item. Not every item will be identified by a serial number, but if some level of tracking or management at the individual item level is desired, a serial number is required.

A critical attribute for identification is uniqueness. In order to avoid duplication, controls need to be established that ensure each serial number is unique within some bounded environment. Examples of bounded environments include part numbers, production lots, manufacturing plants, business units, corporations, industry groups, and the global arena. *Note: The smaller the bounded environment in which the serialization is conducted, the greater the probability of duplicating a serial number in any larger environment.*

Machine readable technologies, referred to as Automatic Identification Technologies (AIT), facilitate easy and accurate data collection. 2D barcodes and RFID are just two of the more recent technologies applied to identifying assets. The ability to capture data electronically is usually quicker than by manual methods and reduces the errors associated with manual data capture and entry. Guidance from the DoD suggest the use of primary and backup AIT is a sound strategy when considering physical parts marking.[†]



Tracking/Traceability in Supply Chain (Delivery, Inventory, Shipment)

As physical assets are identified, particularly through machine-readable tags or markings, the ability to track and trace them through the supply chain improves. Marked assets facilitate the automatic detection of assets as they are delivered, enter inventory, and are shipped out. For typical order-deliver operations, automatic identification can be coupled with advance ship notices to plan, receive, and confirm delivery of assets. Other automatic processes such as RFID and Real Time Location Systems (RTLs) can support tracking assets as they move within and between locations. The reasons for tracking are varied but all relate to saving either time or money in support of improved operations.

The ability to effectively, efficiently, and accurately track and trace assets is an increasing desire and requirement. The Sarbanes-Oxley Act of 2002 provided significant wide range reform for standards of U.S. public company boards, management, and public accounting firms. One of the key aspects of this legislation included the requirement of public companies to evaluate and disclose the effectiveness of internal controls regarding financial reporting. The relationship of asset management and corresponding finances are directly related. The more accurate the data regarding asset location and management the less likely there will be additional spending on assets that cannot be identified and located; the main function of tracking and traceability.

Data Management

While asset identification alone may lead to improved efficiencies, greater benefits come from capturing, aggregating, and managing data about the item over the life of the asset. It is also important to determine how often data updates will be required and the type of data collected at each event or touch point. For example, climate-sensitive items that require climate control would need to provide temperature updates at regular intervals to ensure the proper functioning of the item. The method of data collection is also a factor; will the data be collected remotely by a system or with human interaction? In order to do this, accurate asset records must be established, and updates must be timely and accurate. Updates should occur at pre-determined events identified by the organization during the planning process. These can include reassignments, replacements, movement, maintenance, and disposition of assets.

[†] United States Transportation Command (USTRANSCOM), DoD Automatic Identification Technology Concept of Operations (CONOPS) for Supply and Distribution Operations, June 2007.

By answering the questions in the planning process, the type of data management system and corresponding tags/markings may be influenced. The different scenarios provide guidance or “what if” responses that help the development of business processes.

Benefits

The benefits of managing physical IT assets fall into two major categories:

- ***Minimizing costs through inventory reduction***
- ***Improving operations with streamlined processes and increased asset visibility***

Proper ITAM reduces inventory by ensuring all assets are identified and located where needed. ITAM also focuses on streamlined processes and internal controls to ensure that what is ordered, what is delivered, and what is paid for are in agreement, with minimal intervention required for confirmation and reconciliation. ITAM also addresses cannibalization of assets, often by linking information with Configuration Management Databases. The frequent cannibalization of equipment has a direct effect on items requiring configuration management and those that have associated warranties or leases.

With an increase in asset visibility, AIT also serves as a theft deterrent, both physical and the information about the assets. By knowing the location of the asset, it is easier to determine when that particular asset became “offline.” Sensors or readers can also help determine if an asset passes into, through, or out of an area it should not.

Section III: Electronic Asset Management

In addition to physically locating assets, electronic capabilities exist on networks to identify the assets present.

Identification

Network-derived asset information can be collected by standard network management suites and systems management agents located on desktop computers, laptops, and other IT assets. Data relevant to desktop computers including Basic Input Output System (BIOS) and machine configuration down to jumper configurations can be collected in real-time across the network. Information relevant to software loaded on assets, hardware configuration, current operating status, and usage logs can be collected and delivered via reports or data feeds into intermediate databases. This is possible in most cases, but in the instances where assets are deployed remotely or to an employee’s home (as with a laptop), electronic identification is not possible unless the user is logged onto the network.

Discovery/Traceability

Standard network management processes include real-time detection of devices that are introduced onto the network and traceability back to the devices physical location. One challenge lies in the mobility of users. Traceability is more complex for roaming devices such as laptops with wireless connections and portable devices (e.g. cell phones and personal digital assistants (PDAs)). In these cases, organizations need to allow for ambiguity in device location and use non-positional references, such as machine name and designated owner (e.g., John Smith’s Laptop). Another approach is to partition the data into fixed assets and mobile assets making it easier to make sensible queries on the data.

Data Management

Data collected from multiple devices can be staged for near real-time evaluation or for forensic studies of significant events. Data can be collected from devices in real-time over the network; however, there will be an impact on network performance if the collection process is not managed. Using previously collected data for overview information and real-time collection of data for details on a single device would address most situations.

A critical aspect of data management is access to the data. Appropriate controls should be in place such that users that need information on the assets have the ability to see the data they require, while safeguarding the integrity of the data stored in the system and limiting the exposure of information to non-authorized personnel.

Benefits

Electronic collection of asset data can be combined with AIT to:

- ***Provide a real-time, accurate view of the status of IT investments***
- ***Observe the impact of changes to business processes***
- ***Improve processes for technology replacement and upgrades***
- ***Enable improved sourcing decisions***

Electronically identifying the presence and identity of assets associated with the recorded inventory (or services ordered in the case of outsourced IT services) can feed directly into inventory, property, and/or billing systems. In a static environment of desktops this is fairly straightforward. With a mobile workforce using laptops that are frequently deployed, electronic identification may not capture all devices if they are not attached to the network for prolonged periods of time. Therefore, other processes would need to supplement the electronic identification, such as AIT to capture movement away from current location, help desk data capture associated with service calls, and periodic inventory. The key factor is to establish clean and valid data and then be able to update and maintain the data with consistency and accuracy.

An additional benefit that visibility provides is improved technology refresh. Accurate identification and location of IT assets enables a more optimized process for replacing and upgrading assets at scheduled or ad hoc intervals.

For data centers with large numbers of IT assets on hand, location and performance metrics associated with asset identification enable improved sourcing decisions as well. Bad actors are more easily identified and warranties are more fully applied through accurate data.

Section IV: Challenges

This section discusses a number of specific operational challenges related to ITAM that can be addressed with AIT.

1. Delivery Confirmation

In typical shipping/receiving operations, best practices require an acknowledgement of the delivery. Scanning an asset tag can provide quick, accurate information that can feed the inventory, property, and finance systems, as well as initiate receipt confirmation processes.

2. Service Confirmation

The provision of assets in support of performance-based services creates a specific challenge for asset management. Within this environment, services are ordered by the customer but the assets are owned and controlled by the service provider who bills the customer for the services provided. In cases that the service includes the placement of an asset, reconciling the asset to the billed service is a challenge. The physical assets provided are typically assigned with asset identifiers by the supplier; this is in addition to the manufacturer's serial number.

From the perspective of total cost of ownership (TCO), performance-based contracts do have hidden costs related to asset management. While the supplier may not receive full payment for sub-optimal performance, additional time and effort is spent by the customer in reacting to and trying to rectify poor asset management.

Another impact of multiple identifiers is the effect on help desk or other support operations that require association with the identifiers to track lifecycle history of the assets. In order to record accurate history, all identifiers should be captured.

3. Locating Assets

One of the basic tenets of asset management is to be able to accurately locate assets. This can be a challenge depending on the level of internal controls and the nature of the operating environment. Physical monitoring through visual or AIT scanning and electronic monitoring over the network can assist in locating assets, whether for assignment/usage, inventory, or technology refresh. A corollary to locating an asset is the notification of when an asset disappears - security can be improved with AIT technology to prevent unwarranted removal of IT assets from facilities.[‡] This can also apply to assets electronically leaving a network.

4. Order-to-Delivery Cycle Time

The order-to-delivery cycle time is a performance measure that can be influenced by asset management practices. A number of factors complicate the attainment of high-performing target metrics. As capabilities for customization increase, ensuring what was ordered is what was delivered becomes more crucial. Any data mismatches across the ordering, delivery, and receiving systems create the need for rework and clarification. While commercial best practices have shortened order-to-delivery times by converting to direct delivery, any intermediary assembly or staging activities require asset management to ensure order accuracy.

[‡] Griebenow, Allan (2007), "Hardware Loss Epidemic: New RFID Technology Provides Proven Solution and Even Automates the Inventory," *Information Technology Asset Knowledge*, 2 (4): 32-34.

Section V: Conclusion

AIT can address many of the asset management challenges that today's IT users and managers experience. At the heart of the issue is the manner in which assets are identified, how the identification data are stored across electronic systems, and how that identification is represented on the physical assets. Assets must be properly accounted for by every organization, to ensure both prudent financial management as well as efficient operations.

Accurate identification enables streamlined processes. If the data are questionable, missing, or incorrect, time and effort will be spent reconciling the data, correcting the data, or establishing deviant processes to resolve issues. The automation of processes such as invoicing and payment can be accomplished only if the underlying data are accurate — automating broken processes or continuing processes based on faulty data will not deliver the full benefits of automation.

About XIO Strategies, Inc: *XIO Strategies, a Vienna Virginia-based woman-owned business, specializes in developing and delivering end-to-end supply chain management services and solutions that enable improved asset visibility across the federal government and in commercial organizations. XIO works with its customers to improve business processes, manage technology deployment, conduct research and training, and design and launch marketing and communications programs. Through our work in policy planning, process analysis and deployment of the next generation of AIT tools, the XIO team strives to optimize business processes so they are poised to propel our clients forward.*