

Mitigating Risk through IT Asset Management

Uncovering meaningful information to manage infrastructure assets throughout their lifecycle—and minimize business risks



White Paper



Table of Contents

Executive Summary	3
Automated IT Asset Management Is a Must	3
Where IT Asset Management Stands Today	3
Building the Case for IT Asset Management	3
Regulatory Compliance	4
Software License Compliance Audits	4
Security	5
Vendor Changes	5
Operational Risk	6
Financial Risk	6
Timely IT Solutions to Help Mitigate Risk	6
Conclusion	7
References	7

This document contains confidential and proprietary information of LANDesk Software, Inc. and its affiliates (collectively "LANDesk") and is provided in connection with the identified LANDesk® product(s). No part of this document may be disclosed or copied without the prior written consent of LANDesk. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in LANDesk's terms and conditions of the license of such products, LANDesk assumes no liability whatsoever. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. LANDesk does not warrant that this material is error-free, and LANDesk reserves the right to update, correct or modify this material, including any specifications and product descriptions, at any time, without notice.

Copyright © 2006, LANDesk Software Ltd. All rights reserved.

LANDesk® is a trademark or registered trademark of LANDesk in the United States and other countries. Other brands and names may be claimed as the property of others.

LSI-0461 0206 JBB/KL

Executive Summary

Business risks are growing in number and seriousness every day. Yet while most companies know there are ways to reduce their exposure, many still don't take the appropriate measures to do so. And that can be a huge mistake, potentially threatening the very success of these companies.

This white paper examines some of the primary risks that companies face today and discusses ways to mitigate them through IT asset management. The paper also looks at where companies are today in their adoption of IT asset management solutions. And finally, it presents an overview of several solutions for managing IT assets throughout their lifecycle to both enable operations and mitigate risk in its various forms.

Automated IT Asset Management Is a Must

Gone are the days when IT asset management was a nicety—an optional exercise that yielded interesting bits of information to the accounting department but offered little real business value. Today, asset management is a mandate. Enterprises depend on it to provide meaningful information for managing infrastructure assets throughout their lifecycle—and mitigating enormous business risks.

Gone also are the days of manually keeping score—walking from desk to desk, taking inventory and affixing asset tags. The modern IT environment is in a near constant state of change. Users continually download and install software from the Web. Operating systems, browsers, anti-virus programs and other applications update themselves on a regular basis. Then there is always the game of musical offices, equipment and peripherals to contend with, to say nothing of the proliferation of mobile devices. By the time an IT department could possibly complete a manual inventory these days, the information would be hopelessly out of date and of little to no value.

For these reasons, many companies are adopting automated solutions for managing their IT assets. Armed with complete, accurate data and the analysis tools to convert it into actionable knowledge, these businesses can better plan, maintain, upgrade and retire their IT assets—to help meet operational requirements while mitigating risks. And that is vitally important, as there are a number of serious risks that threaten today's businesses.

Building the Case for IT Asset Management

It seems there are as many types of risk as there are reasons for using IT asset management tools to mitigate them. To mitigate risk in all its forms, Gartner researcher Jack Heine recommends that, “businesses need to develop a practical blueprint to improve controls over hardware and software assets, as well as a game plan that they can execute to leverage the full value of assets across the enterprise.”¹

That blueprint should detail solutions for handling these risks in particular:

- Regulatory compliance
- Software license compliance audits
- Security
- Vendor changes
- Operational risk
- Financial risk

Let's take a brief look at each of these risks and see how businesses can better protect themselves by effectively managing both their IT and non-IT assets.

Where IT Asset Management Stands Today

In a 2006 study commissioned by LANDesk Software, Inc. (“LANDesk”), UK-based research firm Dynamic Markets interviewed 500 enterprise IT managers across the U.S., UK, Germany and France. The results of the survey were no less than shocking:

- Some 64% of respondents are not entirely confident that their record of IT assets is accurate and up-to-date.
- However, when it comes to software, 85% claim that all applications used internally and remotely are fully licensed.
- Nevertheless, when it comes to testing out that confidence, less than half (approximately 48%) would confidently welcome an audit from Microsoft.
- Manual methods of tracking IT assets are still most commonly used.
- Approximately 31% keep a register for health and safety reasons, and 32% make a log of items as they are purchased. Only 28% use a single management tool to automate the process.

Regulatory Compliance

In an information society like today's, businesses depend on data—accurate data. Without it, profitability, customer service and public accountability are all in jeopardy. Hence the proliferation of new legislation and government regulations aimed at ensuring the integrity of both data and data handling processes in recent years. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA) and Notification of Risk to Personal Data Act (NORPDA) are just a few you may have heard of. Other new regulations are emerging as well, promising to protect copyright and intellectual property rights. And these regulations have teeth. Violators face significant penalties, including large fines and even prosecution for senior management.

As these regulations necessitate a certain level of asset tracking to handle data security and privacy issues, companies are changing the way they conduct business to ensure accurate and timely compliance. Fortunately, there is plenty of help to be had. These new regulations have ignited the widespread development of new asset management tools and fueled the enhancement of existing solutions. In addition, standards like the new IT Infrastructure Library (ITIL) are helping businesses integrate best practices and standardize their IT asset management, while IT governance frameworks like Control Objectives for Information and related Technology (COBIT) are allowing managers to bridge the gaps between control requirements, technical issues and business risks.

The key to meeting regulatory compliance of any kind is understanding what IT assets a business has, what information is stored on those assets and who has access to that information. Once a company knows all that, only then can it begin the task of ensuring that its data is safe and its stewardship responsibilities are met. And that brings us to asset management.

When searching for an IT asset management solution, a company needs to look for one that helps it achieve full accountability over its business assets. This means finding a solution that is capable of inventorying and reporting on servers, desktops, mobile devices, peripherals and all software in use, regardless of operating system, location or system state. A company has to have the ability to generate such reports before it can begin meeting the terms of a regulatory compliance audit. Having an automated solution to do the heavy lifting can save a business significant time and money—and ensure that the data is available the moment it is needed.

Software License Compliance Audits

Another form of compliance that is of notable concern to companies these days relates to software licenses. Due to widespread piracy, software license revenues continue to decline. The Business Software Alliance, the voice of the world's commercial software industry, estimates that 35% of the software installed on computers in 2004 was pirated.² That equates to approximately \$33 billion in lost revenue for software developers that year—up from \$29 billion the year before. As this trend continues, software vendors will be forced to seek additional revenues from customers through more frequent software audits.

Those companies without an IT asset management solution in place are at the greatest risk—and they probably don't even know it. According to industry expert Gartner, enterprises without an asset management or software licensing group have a high probability of being audited within the next two years, with unfavorable results. Gartner goes on to predict, "Through 2006, 40 percent of mid-size and large enterprises can expect an external software licensing audit (0.7 probability)."³

Obviously, a comprehensive, automated IT asset management solution would be of immense value during such an audit—a solution that features fast, accurate and extensible software inventory querying and reporting in support of both internal and external audits. While external audits are the subject at hand, internal audits are important for preventing pirated software from creeping into the environment in the first place, putting the business at risk.

However, the benefits of implementing such an asset management program extend far beyond simply fairing well during an audit by a software vendor. With detailed software usage monitoring and alerting, a company can better police its license agreements, more effectively plan for future purchases and even reclaim expenditures for unused software.

Security

It isn't enough for a business just to have a handle on its software licenses to avoid risk anymore. With the threat of security attacks rising, it is becoming increasingly important to know exactly what hardware and software is installed and where it is located in order to safeguard it. That task, however, is becoming more and more difficult with the number of mobile devices used in companies increasing so rapidly. Yankee Group Research, Inc. reports that mobile computing is growing steadily, with the number of employees with remote access increasing from 25 percent in 2003 to 34 percent in 2004.⁴

So the first step in the process of securing a company's infrastructure becomes information gathering. In addition to knowing everything about the internal computing infrastructure, the company also needs to know everything about mobile devices that try to connect to it: system information, installed applications, security tools in place and their status. Only when all of that information is known can the company then take the steps necessary to ensure corporate network protection.

For example, let's say a company's security policy requires its mobile workers to have the latest virus definition files installed on their notebook PCs. Not an unusual requirement. With a functional IT asset management solution in place, the authenticating server can query a remote device that is attempting to gain network access. In real time, it can determine the make and model of the device, its hardware profile, installed anti-virus software and the date of its last set of virus definition files—among other things. If the remote device is determined to be up-to-date and meets the company's security requirements, and if the user has the proper credentials, then the authenticating server grants the device network access. If the remote device doesn't meet the company's security standards, it can be quarantined on a subnet where it can be properly updated and later granted network access. The key takeaway here is that this process begins with gathering information about the remote device—and that is something automated IT asset management is ideally suited for.

“Nearly 90 percent of U.S. businesses suffered from a computer virus, spyware or other online attack in 2004 or 2005 despite widespread use of security software, according to the FBI. Though 98 percent of respondents said they used antivirus software, nearly 84 percent said they had suffered a virus attack in the 12-month period.”

– ZDNet Research,
January 20, 2006

Vendor Changes

Another current area of risk to companies is vendor change. At first glance, this might not seem like a serious hazard. But consider that vendors are going to come onto the landscape, consolidate with other vendors, and may ultimately disappear. Their customers could be left holding the proverbial bag. For a business to fare well in this environment, it needs to maximize its IT spending through competitive negotiation and contracting. The business also needs to manage its vendors to ensure it receives everything it bargained for.

For example, many companies lease hardware to control costs. The leases for this hardware need to be managed for the business to capitalize on them. That means tracking vendor data, lease terms, maintenance agreements, service histories and lease expirations for each piece of equipment in the environment—and doing so each time new hardware is brought in. Any IT asset management solution under consideration should be robust enough to handle such duties. Because with negotiated three-year lease terms, the IT department will be exchanging approximately one-third of its hardware each year. If a company returns leased equipment late, the vendor could impose financial penalties.

Operational Risk

An area of concern that deserves particular attention is operational risk. When a company's computing environment is unsecured, unstable or otherwise unreliable, it is vulnerable to operational risk—anything that negatively affects the company's ability to do business. For example, let's look at a company hit with a virus that shuts down its database servers. Like many others, this company depends on those servers to conduct business. And until the database servers are up and running again, operations are at a standstill and the company is losing money. In this case, the company should have put measures in place to prevent the virus from getting into the network and attacking the database servers. These measures could have included blocking the installation and execution of applications that are known to be a risk for introducing viruses, such as file-sharing utilities and media players. Other measures could have been disabling certain device ports or drives.

Taking a proactive approach to IT asset management is a must for any company interested in minimizing its operational risk. By implementing the right solution, a company can continually collect meaningful information about its computing infrastructure and rapidly respond when threats arise or business requirements simply change. Consider the example of a company planning a major expansion. Using an automated IT asset management solution that actively tracks computing infrastructure information, managers at the company can view the infrastructure's current capabilities at any time and plan the improvements that are necessary to facilitate the expansion.

Financial Risk

The umbrella or catchall category for business risk is financial risk, as every type of risk holds possible financial consequences. In addition, a company that runs afoul of regulatory compliance, fails a software license audit, suffers a headline-grabbing security breach or otherwise tarnishes its public image may irreparably damage its brand, causing customers to defect. And that can have devastating financial repercussions.

However, beyond mitigating these risks, companies have long used asset management to reduce costs simply through better IT planning, financial accounting and lifecycle management. In fact, according to Gartner, "Enterprises that systematically manage the lifecycle of their IT assets will reduce the cost per asset by as much as 30 percent in the first year, and between 5 percent and 10 percent annually in the next five years (0.8 probability)."⁵

Timely IT Solutions to Help Mitigate Risk

Business risks will continue to grow in number and seriousness. To mitigate such risks, a company would be well served to look into automated IT asset management solutions, such as those offered by LANDesk. Inventory management is built into the entire LANDesk product line to provide extensive knowledge about IT assets, including system hardware, software, configuration and performance.

LANDesk® Asset Manager extends the power of LANDesk Management Suite and LANDesk Inventory Manager, enabling companies to view and track both their IT and non-IT resources—office equipment, associated users, contracts, maintenance agreements and more—throughout their lifecycle.

Key features of LANDesk Asset Manager that help a company mitigate its risks include:

- Asset tracking capabilities that enable a company to track its physical, contractual and financial assets using data stored in a single asset repository. This data may be obtained through import utilities, keyed input into customizable templates and software usage monitoring—across Windows, NetWare, Macintosh, Linux, UNIX and handheld operating systems.
- Efficient access and administration tools that give business managers, financial employees and IT staff access to data entry, administration, alerting and asset tracking tools through a single unified interface. Definable, role-based accounts ensure each worker has access to only the features and information they need to do their job.
- Complete reporting and analysis tools that enable a company to export data in a standardized format and flexibly use its own task-optimized tools and methods. Predefined business intelligence reports and customizable reporting options let managers extract just the data they need and present it just the way they want.

Conclusion

When a company is able to effectively manage its IT assets, it is better able to optimize their use, adapt to change and mitigate risks in all forms. Implementing the appropriate IT asset management solutions enables organizations to discover networked computing devices and known and unknown applications, automatically maintain detailed hardware and software inventories, monitor software usage to reduce licensing costs, and maintain compliance, ultimately resulting in reduced risk, exposure and threats to business success.

References

- 1 "What You Need to Know to Take IT Asset Management to the Next Level," Gartner, December 2005.
- 2 "Global Software Piracy Study," Business Software Alliance, 2004.
- 3 "Why IT Asset Management Is Important Now," Gartner, June 2004.
- 4 "Surviving the Endpoint Security Policy Enforcement Melee," Jim Slaby, Senior Analyst, Security Solutions & Services, Yankee Group, May 1, 2005.
- 5 "Use IT Asset Management to Mitigate Enterprise Risks," Gartner, June 2004.