



## Why do an IT Audit?

One common misunderstanding is that an audit is purely of financial kind. Let us firstly understand the definition of an audit prior discussing its purpose.

The term "audit" originated from the Latin root *auditus*, which means "a hearing." An audit (financial or non-financial) therefore indicates detailed examination and verification of an account, a situation or a state.

Given this definition, the application of an audit varies from financial audits to marketing audits; from fire safety audits to Information Technology audits.

The purpose of carrying out an audit is to verify and examine in detail if there is accuracy in information. However, the type of audit being carried out may have a deeper purpose that is being addressed.

Areas covered and graded by Keene Controls IT Audit.

### Section A: Asset Management

Asset management at its most basic description means simply keeping track of all of your "fixed assets". Fixed assets are real property that your business owns, and is designed to help businesses lower their daily operations costs. Properly used, this is possible in many ways.

#### **Purchasing**

Cost savings in purchasing break down into a few ways:

**How can you know what to purchase if you do not know what you currently have:** Being able to quickly search through your asset database allows you to view assets for the entire company, by department, etc to determine which assets are getting old and are up for replacement.

**Software License compliance:** This is becoming a major problem for organizations that do not keep track of their licenses. You can be fined for installing software on computers than you have not paid licenses.

**Keep track of purchasing information:** Asset records can be generated from purchase orders, or you can explicitly put purchase price information into the system. This can be a quick lookup for you to recall how much you have paid for assets in the past, and in the case of evaluating new vendors, comparing prices.



## **Accountability**

It is in the best interests of your company to know who has which assets and make employees aware that they are accountable for their assets. Doing this allows companies to monitor their assets and should something turn up missing, they know who was responsible for the asset. With the proper use of an asset management system computer and software, assets would be show up in your queries and cannot be forgotten. Your accounting departments will love this since they need information like this to depreciate and/or dispose of assets that are no longer useful.

## **Contracts and Warranty Information**

Most things you purchase come with a limited warranty... but how many of you actually keep those warranty insert cards? Now the few of you that do, how quickly could you pull that card out of filing if you needed information off it? Most companies have service agreements with local repair firms. Do you know the terms of those agreements off the top of your head? Do you know which assets are covered by the agreement? Are you notified when warranties or service contracts are running out?

Bottom line is that repairing an asset once it is out of warranty is very expensive. So tracking this information properly allows you to monitor this information and never be caught with a broken asset with an expired service contract.

## **Track Maintenance Costs (ROI)**

ROI is one of those MBA terms that means, "Return on Investment". To break this concept down simply, think of your office printer. If you paid \$500 for the printer, you could estimate just about how much benefit (\$) you get from running print jobs. What most organizations do not track, however, is the costs associated with maintaining that printer. Printers break, they jam, you have to call in service techs. If you are not keeping track of the time you are spending doing this, how can you know whether keeping that printer is a good investment?

**Should I replace an asset:** In the case of the printer above, lets say you have a cost associated with tech work of \$100/hr. Over the last 6 months, you have had to have the techs fix the printer four times, at an average of 2 hours per support ticket. That is 8 hours of support at \$100/hr, or \$800. So guess what? You have been spending more than 50% of what the printer was originally worth. You should get rid of it and purchase a more reliable printer! Having these numbers in your hand tell the business that even if you spent \$1340 on a better printer, you would break even as far as your costs. Those of you out there who complain about having poor equipment in the office... hard data like this can convince your superiors to buy a better product.



**Dealing with vendors:** When that printer vendor comes calling trying to sell you more equipment, slap them with the above data. You have evidence that their product was a poor purchase decision and this gives you power over the vendor. Make them give you a better service contract if you can show that their product is troublesome, find a new vendor if not. Information is power!

**Staff Training:** What if you find that the vast majority of your helpdesk tickets are your office people having trouble with a certain software package? By being able to track and run reports on where most of your problems are coming from you can draw conclusions about where better training for your end users will be more cost effective than the time you are spending handling their support tickets.

### **Insurance Savings**

Collecting insurance in case of a disaster can be quite a trying process. The insurance provider will want model numbers, serial numbers, purchase information, photographs... generally the more information you can provide the insurance provider about your assets the more likely you are to be reimbursed for that asset. A good asset management system is a great "cover your butt" investment.

Therefore, as you can see, when properly used there are many ways that you can lower the costs of doing business. Proper asset management can more than pay for itself over time.

### **Section B: Security**

There are hundreds--if not thousands--of techniques used to compromise both Windows and Unix-based systems. Malicious code and new exploit scripts are released on a daily basis, and each evolution becomes more and more sophisticated. Keeping up with the myriad of systems used by hackers in the wild is a formidable task, and scrambling to patch every potential vulnerability and addressing each new attack one-by-one is a bit like emptying the Atlantic Ocean with a paper cup. The pressure is on to defend your systems from attack, but short of devoting your life to becoming a security expert, what can you do to ensure the safety of your mission critical systems?

Using the steps delineated by professional security analysts and consultants to identify and assess risks, *The Keene Controls* offers an efficient testing model that you can adopt, refine, and reuse to create proactive defensive strategies to protect your systems from the threats that are out there, as well as those still being developed. This thorough offensive strategy helps design and deploys a barrier to assure your network is immune to offensive exploits, tools, and scripts. If you agree,



you need to develop and implement a security program you will find everything you are looking for in our proven, expert-tested comprehensive program.

### **Section C: Software Compliance**

There was a newspaper article written not too long ago about a brand-new CIO of a large financial services organization, on the job for less than a week, being contacted by a major software vendor and being handed a bill for unauthorized software usage to the tune of \$1 million. By contract, the burden of proof fell to the organization, which was expected to pay up or prove that it was in compliance. This is not an isolated incident. Software vendors and trade associations are aggressively auditing organizations with little advance warning, often resulting in heavy fines. Industry watchdog groups such as the Business Software Alliance (BSA) that represent software manufacturers took in piracy settlements of \$12 million in 2002, and they say they catch an organization that is out of compliance every working day. Gartner Inc. estimates that the probability of an audit for a midsize to large organization is 40% over the next two years and that it will increase by 20% each year. Today, software vendors continue to generate significant revenues from zealous auditing, and there is no end in sight. The BSA estimates that 25% of organizations that do business in the U.S. have some form of noncompliance, resulting in an estimated \$6 billion in lost revenues to software manufacturers.

#### **How Do Organizations Fall Out of Compliance?**

While some organizations choose to take their chances, most do not knowingly put themselves at risk for being out of compliance. Software license noncompliance can occur for a variety of reasons:

Lack of an asset management system

Misuse of MSDN media and licenses

Re-imaging of systems

Assumption that vendor records are accurate

Failure to perform periodic software audits

Poor contract record-keeping

Lack of understanding of software rights as granted in license (such as dual-use conditions) or changed licensing terms

Overbuying server licenses but under buying client licenses



Lack of centralized or consistent procurement policies

Compliance is not easy and you may fall out of compliance without even realizing it. However, as hard as it is to stay in compliance, it is even more difficult to face the consequences that can result from noncompliance. Organizations need to take proactive steps to protect themselves from potential damage. Unfortunately, many organizations are still in reactive mode and seriously address software compliance only when confronted with an audit or a bill from a manufacturer or watchdog group.

Organizations must first determine what is actually running in their environments. However, just because software is installed does not mean that the organization has the right to use it. To truly understand if it is in compliance, an organization needs not only a baseline comparison, but also a view of the software it has purchased, has installed and is using. It has to prove ownership, which requires matching actual inventory with internal contracts and manufacturers' records. This information can be used as protection against fines, fees and penalties. Once organizations reconcile all the necessary information from various sources, they then need to take steps to ensure software compliance. These steps can include renegotiating contracts, removing licenses that are no longer needed or used, or purchasing additional licenses.

## **Section D: Disaster Recovery**

Sometimes referred to as a business continuity plan (BCP) or business process contingency plan (BPCP) - describes how an organization is to deal with potential disasters. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimized and the organization will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.

Disaster recovery is becoming an increasingly important aspect of computing. As devices, systems, and networks become ever more complex, there are simply more things that can go wrong. Consequently, recovery plans have also become more complex.

Appropriate plans vary from one company to another, depending on variables such as the type of business, the processes involved, and the level of security needed. Disaster recovery planning may be developed within an organization or purchased as a software application or a service. It is not unusual for an enterprise to spend 25% of its information technology budget on disaster recovery.

Nevertheless, the consensus within the disaster recovery industry is that most enterprises are still ill prepared for a disaster. The Disaster Recovery web site states that, "Despite the number of



very public disasters since 9/11, still only about 50 percent of companies report having a disaster recovery plan. Of those that do, nearly half have never tested their plan, which is tantamount to not having one at all."

## **Section E: Network Reliability**

There continues to be intense interest on the how to improve the level of reliability and the techniques to improve the reliability of internal networks

The Keene Controls Audit answers two simple but important questions:

*What is the reliability level of your networks?*

*How can I make my network more responsive?*

The methodology employed by Keene Controls is to employ network tools designed to empirically measure critical metrics of your network reliability. The information uncovered from the use of these probes will be discussed with you so we can develop an action plan to correct or enhance any particular area of interest.

## **Section F: VoIP Readiness**

If you are considering an IP Telephony solution, but are not sure whether your current network infrastructure can support your requirements, Keene Controls can help. Across your local area network or even a wide area network, our IP Telephony Readiness Assessment will help you understand the current state of your network, and its ability to support a converged IP telephony (IPT) environment. The readiness assessment provides an invaluable way for you to evaluate your existing network infrastructure and applications to verify that you are ready for an IP telephony solution, which aligns appropriately with your business and network requirements.

The Benefits of this approach:

Provides capacity and performance information on your network

Measures quality of service (QoS) to ensure excellent voice quality

Recommendations on the most appropriate IP solution

Recommendations on the most appropriate network solution

What happens if everything looks good? You can be comfortable that your network is stable and meets or exceeds the minimum requirements for IP telephony. What happens if your network fails? No problem, we will now have enough information to guide us in the right direction.



Keene Controls has the skills and ability to advise and implement the most appropriate solution to suit your business requirements.