Why your business needs an IT audit

Every business manages and processes data with a system of computers. A failure within this system can have significant consequences such as inaccurate billing, inability to retrieve data, or release of confidential information. Getting the system back in shape can be expensive, lost data may never be recovered, and data breaches expose the business to third party liability.

IT evolves at a much faster pace than practically any other field. Rapid evolution and complexity mean that most businesses hire specialists fairly early, and as the business grows management depends more and more on IT experts.

Recent cases of data breaches and system failures highlight how critical it is to have a robust and continuously updated IT system. Every year the number of incidents costing the company more than a million dollars has increased.

All of these factors – rapid evolution, highly technical and specialized subject matter, and an elevated cost of failure -- mean that it has become industry standard to engage in third party audits of IT systems, much as third party auditing of financial statements is common.

What is an IT audit?

An IT audit is an examination conducted by an independent third party in which the company's hardware, protocols, risk map, software, mitigation plan, and other IT related aspects of the business are evaluated. The goal is to collaborate with senior management and IT personnel in order to make the system more robust. Just like the financial auditor, the IT auditor will issue a report indicating areas of concern along with recommended remedial measures.

Auditors work closely with your CIO, IT administrator, internal IT audit team and HR in order to protect your business from loss or liability caused by a system or human failure. The auditor must be completely independent of all of the other IT professionals, and report directly to senior management. Also, the auditor should only do external audit work for the business and leave systems design, updating and remediation work to others in order for the auditor to maintain its independence.

IT auditing is more than disaster planning and threat protection. It also requires taking into account human behavior that can undermine the security of an IT system. For instance, it is human nature to believe that things are generally good and will remain that way, and that most risk lands on other people. This makes it easy for daily users to overlook potential risks in the IT infrastructure. Without independent, third party auditing it is a near certainty that some vulnerabilities will go undiscovered.

TEKMAR SOLUTIONS, INC.

1830 Banking St.
Greensboro, NC 27408
336.373.1105p
info@tekuser.com
www.tekuser.com

In addition to network security, IT auditing provides protection from liability in the event of a successful attack or a breach.   Should sensitive data be compromised, plaintiffs' lawyers will closely scrutinize the preventative measures in place before the event and compare them with industry standards. Those IT managers who can argue that they did everything possible to anticipate and mitigate a cyberattack, including performance of an IT audit, will be in a much better position to reduce financial exposure than those who did not.

Improving Customer Experience

It can be very difficult to see your web presence from a customer's point of view. It is human nature to assume that everyone else thinks the way we do. It is also common for people to stop noticing the familiar and well known. These two biases can make it hard to notice when links aren't intuitive, customers react differently to an interface than expected, or some other aspect of the customer experience with the website is not optimized. Your auditor will use the website as a customer would and provide valuable, independent insight into how it feels and will have the expertise necessary to suggest solutions. And a better customer experience makes it more likely that visitors will be converted to buyers.

How big does my business need to be to benefit from an IT audit?

The need for an audit does not depend upon the size of the company. Since mishandling of software or data can happen in firms of any size, the need for an IT audit is instead predicated upon the potential harm that a system failure can cause. If your sensitive data is compromised, how likely are you to be sued and what would it cost to get it back? If your website goes dark, how much would it cost to recover and what would be the effect on revenue? How much are inefficiencies and dated technology costing the business?

What is the difference between an internal IT audit and an external one?

Internal audits are a protocol businesses have in place to ensure information security and compliance and to properly manage risk. An anti-virus program is a simple example of an internal auditing protocol. This work is often contracted out to third parties, but is still considered internal because the third party provider may be involved in the IT system design and often suggests and implements solutions when a problem is discovered.

External audits are performed by companies that have no financial interest in providing solutions and that have played no part in designing or implementing the IT infrastructure in the first place. This allows maximum independence and protects against human biases to the greatest degree practical.