Avoid Common Mistakes in an Internal Audit
Introduction

We have already spoken and heard volumes on how the widespread usage of technology has made the world a better place for everyone concerned. Also, there is no need to further expound on the fact that businesses of today, and certainly those of tomorrow, are increasingly relying on digital assets for their day-to-day operations. Everybody knows we can’t do without our devices these days. Connectivity has become the watchword of current times, and information technology has us clearly enmeshed in itself. Hopefully for the better.

What is overlooked, however, is how vulnerable these devices actually leave us. While the judicious and knowledgeable use of digital assets can certainly be beneficial to the operating effectiveness of an organization, at the same time it must be remembered that improper usage of digital assets can surely and certainly lead a business on the path to immediate ruin.

Information Technology (IT) is vast. It is essentially an umbrella term that incorporates any technological innovation that enables communication and the dissemination of information in digital or analog format. And because such a wide number of technologies are incorporated into its fold, IT has become a behemoth that is almost impossible to fully comprehend.

It is this very complexity of information technology that unscrupulous elements are leveraging to find chinks in the IT security armor. Data is the currency that runs the world in current times, and information is the translation of data in useable, applicable formats. As the majority of the world’s data is stored in digital form, such data, which includes valuable and business critical information items, are at risk of being violated by digital delinquents.

Incidents of hacking, malware attacks and holding critical data hostage through use of ransomware have ballooned in recent times. While it is true that technological complexity often plays an enabling role in easing the job of hackers and the like, nevertheless, most security breaches occur due to laxity on the part of an organization in adequately and effectively assessing, scrutinizing and documenting the threats to their digital assets. Only through a systematic process of repeatable assessment can we truly ensure the security of our IT systems.

This is exactly the need fulfilled by an IT audit. IT audits effectively fulfil the role of a guardian when it comes to determining the safety as well as operating efficiency of the digital assets of an organization. Yet the sad truth is, IT audits are often seen in a negative light. Upper management, which is mostly concerned with improving the bottom line, sees IT audits as costly and time-consuming interventions that serve very little purpose other than disrupt the day to day operation of the organization.

Nothing could be further from the truth.

While it is true that IT audits do take up a significant amount of time and resources in their execution, and it is certainly true that those resources could have been used for improving profits and other essential functions of the business, nonetheless it should also be remembered that
ensuring the smooth and unhindered operation of the IT infrastructure is one of the essential components of guaranteeing the proper functioning of an organization’s business processes.

In spite of the above, most organizations still view IT audits as a nuisance. They consider regulatory compliance issues to be too complex to navigate, and instead of taking the help of experts to overcome the barriers to IT audits lean towards avoiding them altogether.

This can become a quick recipe for disaster.

It is of prime importance that organizations carry out periodic audits to ensure the safety and security of their digital assets. Yet the process to completing a successful IT audit is easier said than done.

While it is true that if executed correctly IT audits can reveal vital insights regarding the safety and security of the digital assets of any organization, yet here the operating phrase is *if executed correctly*. For just as a successful IT audit can go a long way towards ensuring the well-functioning of your digital infrastructure, an ill-executed one can lead to disaster faster than an actual cyber-attack. So, while on the one hand it is of vital importance that IT audits be held, it is perhaps of greater significance that they be implemented in the right manner, without any mistakes.

Yet mistakes are a part of human nature, and in spite of taking all possible care they may creep in and ruin your day. So, to help you in this regard, this guide is going to talk you through the common mistakes that you need to avoid while performing an internal IT audit.

But wait, did we just mention *Internal IT audits*? What is that? And how is it different from an external one? In order to get a clear idea of the mistakes to avoid during an *internal* audit you first need to know what it actually is.

**What an Internal IT Audit is**

Going by the formal definition of an *Internal Audit*, it is one in which the IT audit is carried out by auditors who are themselves a part of the organization where the audit is taking place. In this case, the auditors are liable to report their findings to the management of the company.

This is in contrast to *External Audits*, in which the auditing is carried out by external agents such as government agencies, in order to determine compliance with rules and regulations. External auditors are in no way beholden to the company management.

Successfully conducting an internal audit is a proven way of making sure that your organization is protected against data breaches and other IT security threats that may severely damage your organization both in financial as well as reputability terms.
Security audits surely need a lot of resources and time to complete, yet they are absolutely necessary to the well-being of your IT infrastructure. An internal security audit can play a critical role in improving the security of the organization and can also provide actionable insights that contribute towards improving the company defenses.

So now that you have a clear idea about what an internal audit is, let’s find out some simple steps in which one can be easily carried out.

**The Five Step Guideline to Performing an Internal Audit**

Internal audits can be tricky to implement the right way; however, by sticking to the five-step guideline mentioned below you can easily ensure that your audit takes the right route to success.

**Scope Out Your Audit**

The very first step that you should follow while carrying out an internal audit is, with the help of your team, make a clear inventory of all your digital assets. This should range from physical devices such as computers and networking equipment to intangible assets such as software and digital data.

Once you have successfully completed taking stock of your digital assets you now need to define the scope of your audit. Certainly, the first mistake you can make here is to try and include every asset for your audit. Nothing could be more wrong. While performing the audit it is not expected that you can cover all aspects of your IT infrastructure.

The scope of your audit should be determined by the final goals that you wish to achieve through the audit process. Once you have your goals established you can easily define which parts of your infrastructure you need to include in the audit, and which parts you should leave for a subsequent audit.

**Perform a Threat Analysis**

Once you have scoped out your assets, now it’s time to match them with any potential risk factors that may seek to harm them. This can range from cyber-attacks such as ransomware to physical hazards such as a fire or a natural disaster. As long as the threat can cause damage to any part of your infrastructure, be sure to document it carefully.

**Evaluate Existing Security Measures**

After successfully completing your relevant threat analysis you need to perform a thorough evaluation of your existing security practices and measures. Be advised, this is an area where you are essentially evaluating your own performance. Hence biases are liable to creep in.
It is essential that you do not allow this to happen. Block out any emotional attachment that you or your team members may have towards your existing security system. Remember, personal views and egoistic concerns have no place here. Be critical, be logical and above all, don’t be afraid to question your own ideas.

Score Your Risks

Now that you are done evaluating the threats and security measures, it’s time to assign a risk score to the threats that you enumerated in step two. In this step you need to compare the possibility of a particular threat to the actual damage that can result if the threat becomes a reality. Based on this you need to assign a priority score to each threat. After doing this successfully arrange the threats decreasing order of risk score. This will enable you to deal with the threats that carry a greater risk first, while leaving low risk ones for later handling.

Create Security Solutions…and Implement Them

The final step here is actually very straightforward, though not as simple as it may seem. After you have arrived at your list of prioritized threats, then you need to devise security protocols and take steps that negate each of those risks. This can range from setting up security improvements to ensuring that employees follow security best practices while handling digital assets.

However, the task does not end simply by putting the measures in place. You need to be diligent and vigilant to make sure that your security measures are being properly implemented. Also bear in mind that a security audit is not a one-off process and should be repeated periodically to ensure continued protection of your digital infrastructure. Further, your first security audit should be used as a standard against which you should measure the performance and results of your future IT audits.

This will allow you to develop an iterative assessment process that can lead to continuing improvement of your security measures. By sticking to a fixed yet flexible audit regime, you can guarantee that your IT infrastructure is in a safe condition.

Common Internal IT Audit Mistakes and How to Avoid Them

The above process is one of the ways of ensuring that your internal audit is carried out without a hitch. Yet the truth is mistakes do happen, and even well-intentioned audits can quickly spiral into disaster. The following is a list of the most common mistakes that auditors may fall prey to during an internal IT audit. Also provided are some methods of avoiding and recovering from such mistakes in case they do start to creep into your audit process.
**Getting Overwhelmed by Complexity**

Audit regulations and compliance rules are often complex and require a deep professional understanding of the process that can only come from extensive experience. Often this is exactly where organizations tend to trip. IT being the vast field that it is, most organizations face problems regarding which method to adopt for beginning their internal audit. Many organizations even have problems deciding from which part of the system they should actually begin their audit process.

Getting confused and overwhelmed by the complexity of the audit ahead of you is one of the greatest missteps that you can make. So, if you feel you are being flooded by contradictory views and opinions its best to hire professional help to make the process easier for you. Experienced professionals who are well equipped to carry out such audits can be a lifesaver for your organization.

**Lack of an Asset Database**

Another deadly mistake that organizations are often plagued by is the lack of a well-documented asset list. Remember the first step in our five-step process to carry out an internal audit? It involved creating an inventory of all your IT assets. In small organizations this may be easier to implement as the number of digital devices and associated articles are limited in number.

But for an organization of significant scope, accomplishing this task can well become something of a Herculean task. Taking stock of all digital assets of an organization is by no means a simple task that can be completed at the drop of a hat. However, for obtaining the best results from your IT audit you need to have a systematic process of documenting, identifying and tracking your entire IT infrastructure.

The best way to do this is to maintain a database of all your IT assets from the very inception of your organization. This way you can keep on adding new items and removing old ones as and when they enter or leave your infrastructure. This way you stand to create a dynamic, updated inventory that guarantees that all your digital assets are adequately and systematically documented. So, the next time you need to face an internal audit you’ll be a step ahead.

**Inadequate Staff Training**

As mentioned in the very definition, an internal audit is usually carried out by auditors who are employed in your organization. This means that you are responsible for the training of the auditors. However, many organizations overlook this very important aspect.

Unless your internal auditors are adequately acquainted with the latest industry trends, tools and practices they will certainly not be able to carry out the audit process to their full capacity. This will ultimately lead to an audit that is done in a slip-shod manner, which is bound to give less than ideal results.
To ensure that your staff is properly trained, consider investing in training. Yes, the upfront cost may be a bit high, but it pays off in the long run by improving the quality of their work and giving you stellar results from your internal audit.

**Self-Serving Biases**

We’ve already mentioned this point before but seeing as it’s one of the most common pitfalls that many auditors fall in, we deem it prudent to stress it again. An internal audit is a dangerous job for the simple fact that you are auditing yourself. This can open the doors to multiple biases and inherent slip-ups. As the auditors—and authority—they will be reporting to are internal to the organization there can be a temptation to gloss over small inefficiencies or overlook certain mistakes.

This can cost you dearly in terms of data breaches and associated security lapses. The very essence of auditing yourself means that the auditors must be extra careful in their assessment of your internal systems. And just in case you feel that your auditors can’t carry out the task in an entirely unbiased manner, consider hiring external help to aid you in the audit process. Self-serving biases can be serious roadblocks on the path to a successful audit, so make sure you do not fall into that trap.

**Lack of a Proper Audit Plan**

Planning is one of the essential steps to achieving the perfect results from any task. Without the proper plan, a job is bound to become botched due to improper execution. The same is the case with internal auditing. Without a proper auditing plan, auditors can scarcely hope to get the proper insights from their audit.

Yet this is what many inexperienced auditors tend to do. Getting started on the audit without a proper plan would essentially be the same as going on a road trip without a map. Lack of a proper audit plan can lead the auditors astray, and waste valuable time, money and company resources that go into the audit.

Therefore, it is of vital importance that you have a proper plan in place for your internal audit. Be advised that there is no one size fits all approach here. Every organization, and for that matter every audit has distinct needs and goals. Be sure to frame your audit plan in line with your organizational goals and infrastructural requirements. For a starting point, you can always use our five-step audit plan (as outlined above) as a framework on which you can build your own audit strategy.

**Manual Processes as Opposed to Automated Solutions**

Even in 2019, many organizations rely on manual tools such as spreadsheets and in-person tracking to keep tabs on the auditing process. This can be a quick route to ruin; if you are not
using automation tools to help your auditors (and yourself) you are actually setting yourself up for a spectacular failure.

To overcome these pitfalls consider investing in automation tools for internal auditing. Also, you can employ the help of external experts who are adept in using automated tools for generating instant reports and customized result sheets for you to use. Automation tools are also a great way to ensure that your auditing process is completed on time and within the assigned budget.

*Losing Track of the Big Picture*

During an audit, the auditors have to deal with a considerable amount of numerical information such as network statistics, risk scores and numerous other data items. Often in the middle of such convoluted numbers it is easy to lose track of the final objective: ensuring the safety and security of the organizational assets from threats.

Auditors must take extra care to ensure that every step they take is geared towards the realization of the company goals regarding IT and information security. Keeping this in mind every step of the way can guide auditors to drive the internal audit process in the right direction.

*Improper Documentation*

A common mistake that plagues many internal audits is the lack of proper documentation. In many instances, the reports of previous audits, along with asset documents and associated papers are not provided to the auditors.

This can severely curtail the effectiveness of the auditors. Another documentation mistake that can occur is failure to record the findings of the audit in a consistent manner. Unless relevant reports are generated at every stage of the audit, the method becomes self-defeating. Hence it is of utmost importance that proper attention is paid to documentation.

*Preparing Reports in a Routine and Disengaged Manner*

It is no doubt that an internal audit is, at its core, a routine task. The audit is undertaken according to the company routine; there is a routine process of carrying out the audit, and what’s more there is even a routine format for the creation of the final audit report. All this is done to maintain standardization in the auditing process.

And while standardization is undoubtedly a desirable quality of any audit, often the auditors make the mistake of confusing routine with run-of-the-mill. By allowing a sense of monotony to creep into their reporting, they convert the very essence of the report into a set of routine observations that often fail to capture the true purpose behind the audit process.

This should be avoided at all costs. Allowing the report to become a set of disengaged statements defeats the very objective of the audit, which is to capture the dynamic nature of the security landscape of the organization’s IT assets. Auditors should take extra care to ensure that they do
not fall into this very common trap. Reporting should be done in a routine format, not in a routine tone.

**Creating a Massive Report**

Just as damaging as a routine report, overly complicated and detailed reports can lead to confusion among executives. No one nowadays has the time to go through massive documents that entail hours of intense concentration.

Instead, consider creating concise and to the point reports using automated tools. The best method is to prepare customized dashboards that detail all relevant points in an easy-to-digest format.

**Failure to Act**

Even if all goes well with the audit process, chances remain that you’ll find some issues during your auditing that need to be addressed. These can range from potential security loopholes to serious vulnerabilities that must be immediately plugged.

One of the greatest mistakes you can make in an internal audit is failing to act upon the findings of your audit process. Your auditors will surely follow up with you regarding their findings, and would expect you to take action in order to address the issues that have been discovered. In this case, it is best to take act quickly and not procrastinate.

Remember, a stitch in time saves nine. Timely action on your audit findings can help save your organization both in terms of time, money and resources. So be sure to take immediate action in case you are faced with security issues in the course of your audit.

**Neglecting to Maintain Continuous Communication**

Your internal audit team is a part of your organization. However, often they are seen as special operators who only need to come in during the audit process, relay their findings to the reporting authority and then fade into the background. This is not the ideal way to deal with your auditors.

Being a part of the organization, you should ensure that your audit team is involved in regular communication with the rest of your staff, especially your IT and InfoSec departments. Lack of proper communication with the auditors can result in information gaps that may severely affect the final outcome of the audit.

To ensure that your audit team is on the same page as the rest of your stakeholders, include them in major decision-making processes. This will enable them to remain up to date on any system changes and major overhauls that are being implemented. And will go a long way towards ensuring the veracity of your next internal audit.
Inadequate Staff Preparation

While not maintaining proper communication with the audit team can be a serious impediment to a successful audit, the other side of the coin must also be examined. Without proper preparation and a sense of adequate direction, an internal audit can quickly become a harrowing experience for the rest of your staff.

Internal audits are integral to the success of the organization. This should be clearly explained to the staff so that they realize the need for the audit. After all, it is your staff who are the prime users of your IT infrastructure; hence their adequate participation in the audit process is absolutely essential to ensuring its success.

Without the support of experienced staff members, the audit team would have a hard time carrying out their job efficiently and effectively. Further, tenured employees can play the role of guides for new entrants and explain the audit mechanism to them. To ensure that the audit process unfolds smoothly, take care to encourage active participation of the staff in your audit process.

Viewing Auditors as Critics

Many organizations make the mistake of treating internal auditors as an adversarial unit that is out to find faults with the way digital assets are being maintained. Nothing could be further from the truth.

Your auditors are perhaps your greatest well-wishers, and their job is not fault-finding but rather fault remediation. And auditor is simply another stakeholder in your business and should be viewed and treated as such.

Auditors help to compare existing processes with established standards in a bid to evaluate the level of security that your IT assets currently possess. Such assessment not only validates your existing measures but also contributes towards improving them. Your auditors are your partners who are working with you for the development of the business; they should be treated as such.

Patchy Security Policies

Every business that deals with IT assets (which is almost all businesses these days) need to have a sound security policy in place. This not only helps the auditors take stock of your protection policies but also guides the staff in their day-to-day operations.

However, many organizations make the mistake of creating security policies that are patchy at best. They have an exception to every rule, a loophole to every clause; this creates a shaky framework on which sound security practices cannot be built. Further, a less-than-adequate security policy makes things more difficult for your auditors.
To ensure that the internal audit goes unhindered and your business gets the best results from your audit, make sure to invest time and resources in framing a solid security document. If required, consider hiring external help to aid the process. Often, experts can bring a considerable amount of domain knowledge to the table that can go a long way towards guaranteeing audit success.

**Trying to Micromanage it All**

This can be one of the greatest mistakes to commit during the internal audit process. As the internal auditors are usually employees of your organization often this results in higher management trying to dictate them every step of the way.

This can only hinder the process. By trying to direct the auditors in every aspect of their work, you might just be proving to be a greater impediment than anything else.

Allow the auditors to work as per their code of conduct, and the results will automatically follow. This of course does not mean you will not be a part of the process. Bringing your own valuable insights to the table and aiding the auditors in carrying out their job is the best way to facilitate the internal audit.

**Lack of a Contingency Plan**

IT audits are a technical process, and things can go wrong in any number of ways. If you do not have a contingency plan in place to ensure that you can effectively handle any untoward situation, then this can create a sense of urgency and breed confusion among staff members.

Therefore, it is essential to have backup plans in case something goes amiss during the internal audit. This will help your auditors to complete the audit in a timely and effective manner and will also ensure that your day-to-day operations remain undisturbed.

We’ve covered the bases on all common mistakes that can take place during an internal audit. While some of these mistakes are procedural and can be overcome through standardization techniques, many involve simple human oversight which need to be carefully curtailed in order to ensure that the audit process goes smoothly.

Most of this piece has dealt with how to avoid mistakes in internal audits. While the mistakes and redress mechanisms mentioned here apply specifically to internal audits, external auditors too can keep them in mind in order to ensure they are not repeated in any way in the external audit process.
The Fundamental Goals of an Internal Audit

Many organizations are of the view that repeated internal audits are a problematic element. While it cannot be denied that internal audits do affect the usual operations of the organization to some extent, nevertheless the effectiveness of audits in ensuring the safety of the organization’s IT infrastructure cannot be denied. The following are some of the fundamental goals of the internal audit.

- They ensure the adequate protection of company data.
- They help to determine whether the hardware resources available to the organization are up-to-date and sufficient to fulfill the goals of the business.
- They guarantee that all stakeholders are involved in the IT security process.
- Audits provide the necessary tools to staff so that they can carry out their respective functions without hindrance.

To Wrap It All Up

If there is one thing that has been made clear from the above discussion, it’s this: internal audits are an unavoidable part of ensuring the safety, security in continued operation of your IT assets. They not only help to maintain the integrity of the digital assets that businesses are commonly reliant on, they also serve to provide the template for safe IT practices and help to maintain digital discipline.

Internal audits can also serve as a launchpad for any future audits, provided the findings are recorded and implemented systematically. Audits are also important steppingstones for achieving compliance requirements.

As mentioned before, information technology and security compliance can be a difficult job, and often companies find it difficult to decide how to begin. In such situations, professional help should be sought to resolve any challenges.

Expert help can enable organizations to be ready for IT audits and avoid financial penalties resulting from non-compliance issues. Further, automated tools used by professionals can generate instant reports which help to eliminate many of the mistakes that usually may occur during the implementation of an internal audit.

Internal audits are an important part of the IT infrastructure maintenance process for any business. They provide ample scope for bringing forward the visibility of security and compliance risks. Internal audits also enable effective enforcement of security policies. Overall, it can be said that internal audits form the backbone for the information and IT security policy of any organization.
It is of utmost importance that this very crucial process is carried out with utter carefulness. Mistakes are a part of life, but with diligent care and a little bit of resourcefulness they can be minimized to a large extent. By automating internal audits and assessment workflows, professional auditors can help to carry out the task effectively.

Whether this is the first time you are going to have an internal IT audit, or your business is an experienced one with many past brushes with the process, keeping the above mistakes and their avoidance policies in mind can help you to minimize risks in your internal audit and ensure the unhindered execution of the task.

This has indeed been a long exposition, but before we wrap up, a final word: one of the gravest errors you can make in the process of an internal audit is not learning from past mistakes. Errors happen as a part of human nature, but there is wisdom in learning from them and moving forward so that they are never repeated. Keep the above points in mind during your next audit.

…and don’t let the same fire burn you twice.
Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com