How to get more out of your internal audit?

Internal IT audit programs are key if you want to make sure all your information assets remain properly secured from any threat. An internal audit provides assurance and helps organizations to manage their risks and controlling their processes effectively. All in order to improve and mature the practices used within the business. An optimally functioning internal audit system starts with an accurate implementation and continuous attention for the organization's hard- and software infrastructure. This whitepaper describes how to get more out of your internal audits by looking at some of the key aspects of IT.

Information security

Traditional IT security was mainly aimed at keeping attackers outside the organization. However, since the introduction of gamechangers like mobile and cloud technology, social media and insider threats it is no longer just about protecting the perimeter. Therefore the risk management approach should also be changed in the face of these new threats. Understanding where your information 'lives' is crucial in protecting your critical assets. The most important IT internal audit consideration related to security is to ensure the information security program is comprehensive enough to include these new threats and is not only implemented within IT but embedded within the entire organization.

With new threats, risk management has become even more important. Always consider how well risks are identified, what is done after they are identified and how well processes are being followed. New risks or significant changes in the risk assessment should always be communicated to the management.

Furthermore, with many new threats posing considerable security challenges it is important to not just look at the vulnerabilities but also consider what controls are in place, how these vulnerabilities might be exploited and what the organization's response is, in case an intrusion is detected. This should always be complemented with regular penetrations tests based on the risks identified by the organization.

Cloud technology
Working in the cloud comes with many benefits. It enables organizations to reduce expenses, become more agile, improve security and introduce pay-as-you-go pricing models. It does however also mean a shift in responsibilities with its own risks and challenges which are not always fully understood. These mainly concern service level agreements (SLA's), legal and compliance considerations and security and privacy risks. From an internal IT audit perspective, it is important for you to understand what the approach of the organization is towards cloud technology.

As part of the change management process when moving workloads to the cloud, ensure there is a comprehensive impact assessment and make sure the security provided by the cloud provider is fully understood.

Also, study the SLA's of the cloud service providers and make sure they are in line with what your business expects from IT. Additional contracts might be needed to ensure your access to data is not impacted when the cloud provider is struck with disaster.

Continuity
One of the aspects of information security is continuity: you want to make sure you are able to recover from both small and large incidents. Continuity management has been growing in importance as organizations got increasingly reliant on IT. In addition the margin for errors has become smaller.

Although continuity management should be part of the broader business continuity plan, the focus actually is mostly on IT. That is why one of the key considerations for an internal IT audit is to ensure the plan is part of a broad business continuity initiative. This can be done by determining to what extend disaster recovery plans are aligned with strategic business functions and if proper testing occurs. One of the most important aspects of continuity management is communication, both internal and external. Therefore, always make sure there is a comprehensive communication plan which is communicated within the organization.

Mobile devices
In most organizations mobile devices have vastly outnumbered local fixed devices like desktop computers. Although mobile devices allow employees to be more productive by having access to their data and business applications from anywhere whenever they want, these devices lead to new threats around loss of devices, data leakage and theft. To manage these risks there needs to be a clear policy on mobile devices. It should be ensured that the internal audit includes policies that include elements concerning the management of lost and stolen devices, security and encryption and overall management around what mobile applications can be used by whom.

Ensure that mobile devices are included in the risks assessment and that threats related to mobile devices are understood and mitigated.

Change and project management
Continuous change has become a fact of life, so you better embrace it. With the increased complexity in IT environments and increased IT spending it is important to have a solid change and project management process in order to adopt new IT technology. This is key if you want to create ew opportunities for the business meeting their objectives.

From an internal IT audit point of view, it's important that you assess if the right processes and controls are in place to manage change throughout the organization. Furthermore, ensure that these processes include impact assessment and risk analysis and they are followed correctly.

IT asset management
Protecting your assets starts with understanding what your critical assets are. This helps organizations with cost reductions and limiting overspending by better using their resources, considering that on average 80% of the IT budget is spend on maintaining existing environments. Also, while companies become more reliant on software solutions it has become more important to be compliant with the terms set by the vendor.

Therefore, understanding the IT asset management process is a critical part of your internal IT audit program. First thing is to check if there is a comprehensive approach towards asset management and what level of maturity this approach has. When the amount of assets within an organization increases it is expected that tools will be implemented in support of the IT asset management process.

With cloud technology emerging rapidly it has become easier to adopt new technologies. This has given room to 'shadow IT' where IT is being purchased by individual employees or units without having the IT department involved. Therefore, make sure all applications encountered are under the control of the IT department.

Identity and access management
Identity and access management has become one of the hottest topics within IT and is all about who has access to what and when. With mobile and cloud there is no clear perimeter anymore and therefore it has become more important to ensure solid controls on identity and access management. When performing the the internal IT audit, make sure to have a clear overview of where identities are stored and in which applications. Make sure there is a segregation of duties implemented where an individual will never be able to control a business process end-to-end. Finally, there always should be logs on who has accessed systems and data.

Data
Data has become one of the most important assets for organizations. Data is also an asset that can be difficult to protect. This is evident from the increasing amount ofdata breaches and data leak incidents where data was leaked, stolen or made unavailable. Data can be subjected to a wide range of incidents. Some happen by accident and are unintentional, others are the result of targeted action. It is of the utmost importance to understand what sensitive data you have, where it resides and how it flows throughout the organization. The internal IT audit can help by looking at these questions and the controls in place to protect data.

Especially when it comes to data ensure the controls are not only in place but also operate well. A backup is useless without the ability to restore and deletions can happen unintentional, so make sure the organization is prepared for these kinds of incidents.

Also, there are many legal requirements around data and privacy, like the GDPR. Make sure the requirements are understood and controls are implemented protecting both data in rest as well as data in transit.