TRANSCENDENT GROUP INSIGHT

Hot Audit Topics for 2023

Transcendent Group recently hosted a webinar on hot audit topics to consider for 2023. The Institute of Internal Auditors (IIA) annually releases a report – Risk in Focus[1]. The report compiles the results through a qualitative survey among Chief Audit Executives (CAEs) across 15 European countries (over 800 responses).

Last year, it was mainly focusing on risks driven by the pandemic whereas this year's report highlights the impact of the war in Ukraine has had on many businesses and its associated risks.

A changing environment

We are living in a world that is riskier and more uncertain than some years ago. A state of crisis is nowadays a normality facing all types of organisations. The world is more digitally connected than ever before. As a result, there are multiple threats in the world such as organised crime, nation-state actors, activism, hackers, and "hacktivism" – combining the words "hack" and "activism" which is an act of misusing a computer system or network for a socially or politically motivated reason.

The organised crime has transformed from bank robberies to cybercrime where new types of cybercrime are constantly emerging. It is a known fact that nation-state actors systematically carry out activities to obtain information from not only authorities but also businesses that might possess valuable information. The aim is not only to obtain information, but also creating uncertainty and mistrust towards organisations.

All of the above can cause various consequences, such as different kind of disruptions, intrusion to publish sensitive information, information theft - used to sell to competitors and ransomware (which has exploded in recent years), and in the long run cause severe reputational risk.

So, what can we as internal auditors do? Well, Transcendent Group have identified five areas that we find are relevant to consider in the upcoming audits for 2023.

[1] https://www.eciia.eu/wp-content/uploads/2022/09/Risk-in-Focus-2023.pdf

Cybersecurity/IT-security

According to Risk in Focus 2023, cybersecurity and data security remain the number one threat for CAEs which is the main reason for internal audit to continuously perform audits within these areas. For example: what types of security measures have been implemented within the organisation and are they adapted based on adequate information classification?

Something we often see in our audits is that organisations normally have good preventative safeguards in place, such as effective fire walls. However, they often lack effective and adequate security monitoring. Organisations need to enhance their detective controls to be as effective as their preventative controls. Hackers and cyber criminals are constantly in search of innovative ways to breach an organisations prevention mechanisms. Internal audit could perform targeted audits where we can focus the audit scope on incident response for example with the objective to evaluate an organisation's ability to detect and mitigate potential real-time threats.

Staff awareness and training is always relevant. Is the organisation appropriately supporting staff to ensure they understand challenges faced by security issues and know how to act in case of any suspicious threat? To keep the business safe, it is essential to educate individuals within an organisation about the role they play.

Social engineering

Human error is a common information security breach. Social engineering attacks is a form of a cyber-attack, where hackers use psychological manipulation to talk employees into revealing specific information. Attackers often target groups that manages sensitive or critical information. Internal audit can assist organisations to simulate tests and thereby providing valuable insights into the organisation's vulnerability to these attacks. The testing will also serve as a security awareness exercise to demonstrate staff awareness maturity. These tests can also be combined with physical security.

Supply chain management

Supply chain disruptions have increased as a result of the pandemic and the ongoing conflict in Europe. In our third-party/outsourcing audits, inadequate monitoring and control of the suppliers is a key issue we normally find. In addition, supply chain attacks have increased lately. A supply chain attack is a cyber-attack that seeks to damage an organisation by targeting less secure elements in the supply chain. Another area within managing third parties is the use of various certifications or third-party statements.

Since the use of suppliers is crucial in many organisations it is likely that internal auditors should focus on third-party risks over the next twelve months. Perhaps as a targeted audit focusing on security aspects or the use of assurance reports?

Business continuity management (BCM) and crisis management

BCM and crisis management are extremely important areas in these times. Even if it is already an area where internal audit spends much time and effort on, it is expected to continue to do so in the next couple of years, mainly impacted by the war in Ukraine.

Although crisis management and business continuity are closely related, there are distinctions between them. For example, BCM is proactive while crisis management is reactive. Business continuity focuses on a set of plans and procedures to ensure that an organisation is resilient. It involves planning for any potential disaster by identifying potential threats and analysing their impact on the organisations day-to-day operations. Crisis management is complementary to business continuity and is the process of managing and dealing with crisis.

Effective BCM, based on international best-practice standards such as ISO 22301, can protect organisations from widespread business disruption in the event of a successful cyber-attack.

Human capital

The human capital is the most important asset in many organisations and have become a key area of competitive advantage for organisations as a result of the pandemic. It has evolved as the hardest challenge businesses face and has increased in priority by internal auditors.

Talent management

Talent management means investing in an organisations most important resource – its people. By implementing this process strategically, it can help to improve the overall performance and ensure it remains competitive. Talent management does not only address recruitment of new staff, it also targets the process to retain talents. It is often a shared responsibility between HR and responsible managers.

For successful talent management an organization needs to look at its long-term needs and develop a plan to address those needs, linked to the organisations long term goals.

In addition, a strategy and corresponding performance measures has to be developed and communicated.

Following the pandemic and new ways of working, organisations need to evaluate the new normal and, if needed, make appropriate adjustments going forward.

On-/off boarding

Employee onboarding and offboarding are critical processes that, when done effectively, can deliver value and a positive return on investment. One can discuss how long an onboarding process actually is to make sure a new employee has been fully integrated into the business? Same goes for offboarding but with the perspective that a successful offboarding allows the employee to leave in good terms, while maintaining company loyalty and employee engagement.

Use of consultants

Is it possible to run your business without consultants? Nowadays the answer seems to be no. It is more of a question how to manage consultants in the most effective way.

Consultants can provide expertise in various areas where organisations face shortage of skills. Has the organisation a strategy in place for the use of consultants? Is the proportion reasonable comparing to total FTEs? Is the organisation aware of potential conflict of interests? Are these situations being managed in a reasonable way?

The organisation should also be aware of which type of information the consultants have access to. Can they access too much information? Do they have decision-making mandate?

It is crucial that the organisations ensure that knowledge is transferred and kept within the organisation and not just with the consultants.

Organisational culture

Auditing the culture within an organisation were also addressed as a relevant topic in previous year. Internal auditors have historically mainly audited “hard controls”. Recently, there have been more attention on soft controls such as culture and behaviour.

Due to the pandemic, new ways of working have escalated, organisations are defining their new normal working practices and adapting to hybrid working styles. How have these changes affected the organisation and the culture within the organisation? Has a risk analysis been performed? What risks did it identify (if any) and how have they been managed?

Work environment

All employers are responsible for their working environment. Regulators produces provisions that clarifies applicable legislation. The most fundamental ones are those related to a systematic work environment management and its corresponding central activities.

The main objective for the systematic work environment is to integrate work environment aspects in the day-to-day operation. Do employers have a process in place to regularly identify, assess, act, and follow up work environment conditions?

Work environment management needs to be conducted both in the course of regular operations and in connection with changes, such as reorganization measures and construction, and when new working and production methods are being introduced. Have consequences for the work environment been assessed and considered before decisions are taken?

The organisational and social work environment provision has a strong connection to the pandemic and its consequences related to the work environment such as different social structures. Are there routines in place to cover the provisions scope such as allocation of work, workloads, working hours, violations etc.?

Digitalisation and agile development

Digitalisation was one of the megatrends that Transcendent Group identified last year. This trend is still relevant. The area consists of a large spectrum of risks where we highlight a few relevant ones for internal auditors to review. Cybersecurity and data security is the highest ranked risk in Risk in Focus 2023. It is also set to remain as the number one risk to organisations three years from now. Digital disruptions, new technology and AI are also among the highest ranked risks. According to the report, CAEs agreed that ransomware risk continues to be difficult to mitigate and poses a potential existential threat to businesses.

Strategies for digitalisation

A comprehensive cyber security strategy addresses technology, processes, and people. Internal audit can help organisations in many ways regarding their cybersecurity. We see a large potential in performing cybersecurity audits where we can evaluate and propose measures to improve the effectiveness of risk management, governance, and controls.

It could make sense to distinguish between "digitisation", which is the process of transforming information from a physical format to a digital version, from "digitalisation" which is the process of implementing more efficient ways of working with the help of new technology. Converting a process from a human-driven event can affect the organisations employees. However, does the organisation also evaluate potential consequences for customers?

Agile business development

Although agile methodologies have become more common, organisations need to adapt to new agile team roles such as product owners, developers etc. as well as clarifying what the roles mean in terms of responsibility and mandates. The risk management tends to be more informal in agile methodologies which is a risk.

Defined objectives is an effective method to monitor and manage expectations in a controlled way. Despite the variety of agile approaches, there are shortcomings in terms of how to define and use objectives to guide project execution. Even though objectives can be regularly changed as needed, it is essential to make sure that the organisation has considered the "why" when setting agile goals.

Agile way of working is commonly used within software-development as a methodology that helps teams work together, Scrum for example. While the agile practices are principle-based it is our opinion that there should be a systematic approach in place to ensure a strong internal control.

ESG (Environmental, Social and Governance)

Climate change is still on the agenda for most organisations. Even though it has been set back due to other emerging risks in the recent year, it is one of the most dynamic and fast moving risk areas for internal auditors. With that said, if you have not performed any audit within this area yet it is about time.

ESG - is the organisation on board?

ESG factors is an area that is facing more scrutiny from regulators. In 2021, new legislations in terms of EU non-financial reporting directive and the EU Taxonomy regulation were launched. Even though the regulations are primarily aimed at the financial sector, businesses operating in other sectors might have to comply with the regulations. As regulations are being introduced all the time, has the organisation a strategy to keep up with this speed? Are the consequences for non-compliance being analysed?

Although the importance of E, S and G factors differs for each sector, internal audit can analyse an organisations strategy on how these factors have been integrated into the daily business processes.

Failure to properly consider and manage ESG risks poses a large reputational risk, for example *greenwashing* - the act or practice of making a product, policy, activity, etc. appear to be more environmentally friendly or less environmentally damaging than it really is.

Auditors have a significant role to play in maintaining trust. An ESG audit could be conducted to answer specific questions, for example:

- What are the risks associated with these issues?
- How is the business organised in terms of ESG policies, systems, and controls?
- How are ESG goals and metrics being tracked and monitored?
- Process to ensure accuracy of external communication to stakeholders?

In addition, internal audit can also provide ESG-focused audits on specific topics such as climate, data security and environmental compliance and performance.

Fraud, corruption, and conflict of interests

These topics are constantly on the agenda. As a result of the current situation in the world, they also intend to increase. Internal auditors should regularly review organisations internal control procedures to limit the risk of fraud, corruption, and conflict of interests. How robust are they? Does the organisation have a systematic approach to manage these risks? Proactive and reactive mechanisms in place? Existence and extent of secondary occupations (specifically in the public sector)?

Internal audit's independence gives it the potential to be involved in whistleblowing arrangements, e.g., as a channel of communication or by carrying out investigations. Where internal audit is not playing a direct role, it can provide assurance of the effectiveness of the system and procedures.

We have helped many clients to audit the above areas! Do not hesitate to get in touch if you want help by experienced internal auditors!

Charlotte Eklund
Deputy Head of Audit and Governance
charlotte.eklund@transcendengroup.com
+46733 38 05 43

Magnus Thyllman
Head of IT-audit
magnus.thyllman@transcendentgroup.com
+46 708 41 77 03