Internal audit hot topics

Information technology

2019

Technology is continuing to advance at a rapid rate, bringing new growth opportunities for organisations around the world. While it enables new commercial models and supports emerging business areas, it brings additional pressure for established organisations to keep up to date. These advances create new challenges for risk management, and organisations must be more alert than ever around emerging risks. In this document we set out the top ten technology risks, which audit committees should seek to gain assurance over.

Contents

Analytics and big data

A robust data analytics programme is increasingly becoming essential for mature internal audit functions. Organisations that have not embraced data analytics may struggle to identify and mitigate risk, in comparison to their peers.

Until recently, internal audit would sample a small percentage of the population, performing audits in cycles, focusing on covering the audit universe and end-to-end audits of business units. This included very little data mining. The use of data analytics has rapidly gained momentum, and today's internal audit strategy has seen a shift from preserving value to creating value. Audits now focus on emerging risk indicators, with risk-based data collection and more efficient analysis of larger populations enabled by data analytics. Internal auditors should be thinking about how they can continuously audit in real time to identify anomalies and produce instant reports to inform strategy and decision-making.

Data analytics increases the chances of identifying the right risks. It provides a way to substantiate key risk areas and it gives internal auditors the ability to perform control and transaction-based testing based on risk. Data analytics also provides flexibility by providing a quantitative way to plan in dynamic environments that change often due to operational requirements, regulatory changes and industry dynamics. Companies that embrace data analytics may be able to significantly reduce reputational, regulatory and operational risk.

Impact on internal audit

Internal audit teams are at a fork in the road with respect to data analytics — those that embrace it are moving up the maturity curve, while those that do not, may be putting their companies in danger through the lack of identifying the right risks and allocating their scarce resources appropriately.

Digital transformation

The end of 2017 marked a turning point for many as the rise of 'digital'. Many organisations are subsequently reviewing their operations and focusing on digital transformation programmes. As with any major initiative, Audit Committees need assurance that these change programmes are well managed.

While many organisations have focused their efforts on new IT systems, websites and apps, it is important to note that this is only part of the challenge. Digital transformation is not just about technology, but about how the overall business operates. As such, successful transformation programmes rely on buy-in from the Board and Senior Leadership Team. This may be problematic as the world of digital is largely new and unproven, and buy-in may be dependent on the promise of demonstrable financial returns.

The question every organisation should be asking is, 'Do the digital initiatives support the wider business strategy?' Looking beyond the digital hype, organisations must consider if these changes will help achieve their business goals and create new opportunities. Organisations that have not assessed the value of digital change may waste significant resources on a futile transformation programme. This will be a key concern for any Audit Committee.

Digital transformation programmes must do more than simply offer return on investment. They must maximise the use of data from all channels, and drive real value across the business. To achieve this, organisations must review their internal processes, external communications channels and IT systems, considering these information streams as a whole, rather than a series of disconnected elements.

Impact on internal audit

Any large transformation programme requires a degree of cultural change, and digital transformation is no exception. Internal audit can offer the Audit Committee assurance over the management of digital transformation programmes and the associated cultural elements.

Cyber security

The UK government's National Cyber Security Centre (NCSC) recently released its annual report on cyber threats to businesses. It noted two key trends which have risen drastically over the last year ransomware, denial of service attacks, and the risk of data breaches, particularly in relation to insecure third party suppliers. Organisations across finance, internet services, public services, retail, telecommunications and transportation have all been victim to data breaches and persistent security threats. This has resulted in both financial losses and significant reputational damage.

It is well know that, in today's world, internal audit functions need to understand, and provide assurance over these, 'Cyber' risks. Looking ahead however, protecting IT environments from being compromised is not enough. Organisations must be able to monitor critical systems, detect malicious activity, respond quickly, and demonstrate the resiliency of IT systems to support core business services. As IT teams struggle to meet these challenges, they must achieve these in a cost effective way, and be able to justify their spending. Any associated investments must be put into solutions which will be the most impactful.

Impact on internal audit

Staffing and spending on IT security is a business investment. As such, internal audit can help management take a step back and highlight any unidentified risks in an organisation's security programme, or, for that matter, "business as usual" transformation programmes. These reviews can help outline the return on investment to the Board and demonstrate what measures are in place to mitigate the risks. They can also assess if business processes are set up in a way which allows organisations to realise the benefits of the products and services used. Reviews of this kind may be based on standards such as the '10 Steps to Cyber Security', from the NCSC, the 'Cyber Essentials' framework, or the more recent NIS Directive. While implementing security products and tools is part of the solution, a cyber security internal audit review can establish if business processes are designed to help maximise the full value of the products and services they use.

Security culture

Keeping data secure is about more than just IT controls. Developing an effective and sustainable information security culture is vital. But a 'one size fits all' approach is not appropriate and what works for one organisation may not be ideal for another.

To a large extent, this is dependent on what the organisation does, the risks it faces, its strategic priorities, goals and its employees' behaviour. Creating the right security culture will help employees to be security-conscious and to actively think about protecting both their own and the company's information. Employees should take a 'preventative approach' to threats and continually consider how to protect the data, information and assets they work with. A number of factors may impact an organisation's security culture, including vision, purpose and corporate values. Both the evident and perceived behaviours of employees and management will contribute to the organisation's culture – as will the governance and business model and the political and legislative environment. While some of these factors are external and beyond the organisation's control, many factors can be proactively shaped and controlled.

Impact on internal audit

Business practices may need to change in order to maintain security. The Centre for the Protection of National Infrastructure advises organisations to review their "security culture in light of changes to the threat landscape, working practices and technology". When identifying the root cause of security issues, assessing an organisation's security culture is crucial to ensure the security control framework is effective. Internal audit teams can perform periodic reviews of their organisation's security culture and propose actions that will help drive the right behaviours to address security risks. These can either be performed as discreet 'security culture reviews', or by incorporating an assessment of culture into other internal audit reviews.

GDPR and data privacy

The EU General Data Protection Regulation (GDPR) took effect on 25 May 2018. It applies to all organisations in the EU that process personal information. The penalties for non-compliance can be severe, but organisations also face reputationaldamage if they cannot show that they take data protectionseriously.

Organisations continue to be required to deal with individuals' rights requests – for example subject access or the 'right to erasure'. They have to be transparent when collecting personal information and may only process it for the specified purposes. They must also have appropriate security arrangements in place, report significant data breaches to the Regulator, carry our Data Protection Impact Assessments, and delete personal information when it is no longer necessary to retain it. All these only begin to scratch the surface of GDPR.

Many organisations struggled to achieve compliance in the run up to 25 May 18. Now in the post-implementation stage, GDPR is about compliance and sustainability, and organisations must maintain their processes and ensure controls continue to be effective. This presents a series of new challenges that not all organisations are well equipped to handle.

Impact on internal audit

Internal audit, supported by data management, privacy, and IT specialists, can be a part of a continuous monitoring plan. They can check if management is taking a risk-based approach to compliance, and if controls are operating effectively. These risk-based reviews will help organisations keep data protection at the top of the agenda within the organisation, as it continues to be an area of public concern.

Cloud adoption

Cloud computing is reshaping the IT landscape and driving major strategic change for many businesses. Many enterprises are trying to determine how these changes fit into their business strategy. For some, it is clear that cloud computing can enable new process models, which can transform their business and give them a competitive advantage. For others, there are challenges around roles and responsibilities, data ownership, security and compliance.

Studies have found several key drivers which influence cloud adoption, including both business and technology elements. Business drivers include user satisfaction and further innovation, while technology drivers focus on scalability, agility and cost reduction. Costs can shift from capital expenditure to an operating expense, maximising the IT budget. Research shows that organisations adopting cloud solutions expect lower ongoing costs and increased agility in their IT resources, supporting further business growth.

Internal audit functions help organisations become more aware of their responsibilities and can provide assurance over how cloud providers are protecting their data. This is achieved by requesting attestation reports from vendors that certain controls are in place to mitigate the risk of systems and data being compromised. As a minimum, vendor attestation reports should include assurance over security, availability, processing integrity, confidentiality and privacy.

Impact on internal audit

Internal audit can offer assurance that IT investments are aligned to business strategy, including assessing the business case for them. They can also help to identify and document risks which could damage the objectives of the organisation, including security vulnerabilities, laws, regulations and access to customer or other sensitive information. Internal audit can also identify risks which could affect reliability, accuracy and safety of sensitive information, including risks around the use of third parties who are hosting infrastructure and/or other services.

Robotics and artificial intelligence

New technologies continue to transform how businesses operate, which can provide competitive advantages. Robotic Process Automation (RPA) helps companies to mechanise basic tasks, which improves resource efficiency and allows skilled staff to focus on more complex business areas. Alongside these benefits, there are associated risks which internal audit should seek to mitigate.

RPA is often combined with machine learning or artificial intelligence (AI), which by their nature adapt to their surroundings and therefore increase the risk of unintended consequences. AI does not come with a built-in morality, so organisations need to find a way to ensure their values and ethics are reflected in the way AI is implemented.

Not only must organisations ensure robots are acting ethically in order to protect clients, there is also a regulatory consideration. Under the EU General Data Protection Regulation (GDPR), wholly-automated decision-making processes require explicit consumer consent, unless otherwise authorised by law.

Effective risk management by internal audit can help protect organisations from an ethical standpoint, and maximise the value of robotic software. The growth in RPA is an exciting time for internal auditors. It is an opportunity to support controlled technological development and facilitate innovative applications of that technology. To achieve this, auditors can influence policy creation and collaborate with the rest of the business.

Impact on internal audit

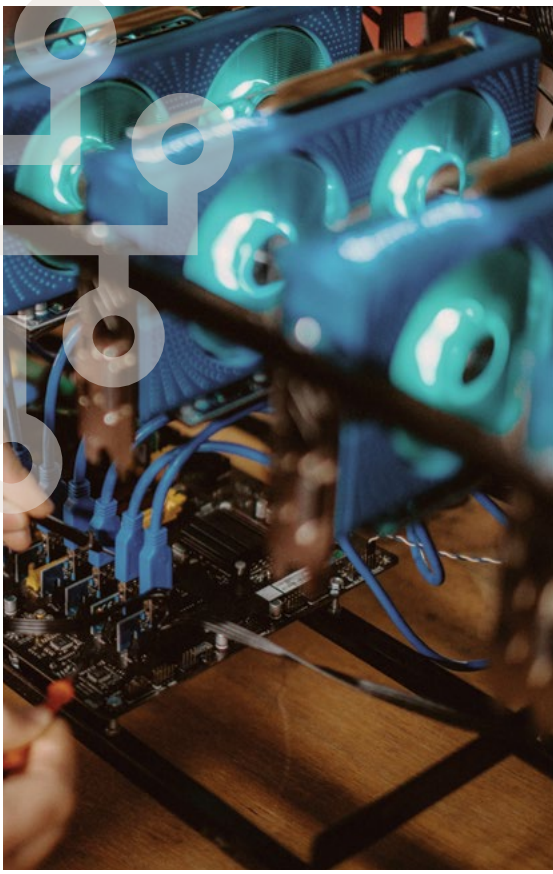
Rather than seeing RPA as a threat, internal audit should use this technology to improve efficiency and to offer greater insights into emerging risk across the business. For example, auditing expense items can be performed using machine learning and natural language processing to automate tasks and evaluating expense line items. By embracing these technologies, identifying the ethical implications and looking ahead to machine learning and AI, internal audit will boost its relevance and be seen as trusted partners in ever-changing organisations.

IT transformation

As technology evolves, businesses continue to transform their IT environments, fundamentally changing the way they are operating and how processes are automated. This requires significant investment in organisations' IT landscapes.

Most organisations are embarking on, or already running, front office or back office IT transformation projects. These are aiming to transform the way IT operates, enhancing their IT capabilities, and the ways in which IT and the business interact. One of the main challenges organisations are facing with their IT transformations is 'speed'. IT transformations must be delivered over a short time period, often simultaneously with other organisational changes, making the project more complex and increasing the risk of failure. Further, these need to be delivered while not negatively impacting the existing services levels being delivered to the organisation.

Due to the fast pace of transformations, their complexity, cost and associated risk – internal audit is becoming increasingly important. Independent assurance is needed over governance and controls, to ensure the project is on target and the intended benefits will be realised.



Impact on internal audit

Internal audit teams are typically taking one of two assurance approaches over IT transformation - either a single point in time review or a series of reviews for on-going assurance throughout the programme's life. A point in time review may coincide with a particular milestone or provide a readiness status report, typically these are performed pre-implementation or at a specific time in the project where major decisions need to be made, acting as a type of project health check. Given the scale and complexities of IT transformation programmes, more mature internal audit functions are adopting the on-going assurance model, aiming to ensure continuous improvement and effective risk management during the programme's life cycle.

Third party assurance

Organisations iincreasingly rely on third parties to support their core activities and in tough market conditions,outsourcing can help businesses gain a competitive edge.Typical third party services include cloud-based infrastructure,software development, in addition to other technical or business support activities. The increased reliance on third parties may improve performance and create efficiencies across the business, but what some organisations fail to fully appreciate is that organisations who outsource business processes still own the associated operational risks, and retain regulatory responsibility for that outsourced process. Assurance reports, such as ISAE3402s, provide a review of the controls in place at a third party service provider which can then be provided to the third party' customer upon request. This regulatory responsibility spans legislation covering antimoney laundering, and anti-bribery and corruption, amongst others. It also has implications for specific regulations, such as the Sarbanes-Oxley Act (SOX), the Financial Instruments and Exchange Act and more recently GDPR. With high penalties for non-compliance, and increasing customer expectations, user organisations need evidence that their third parties take these responsibilities seriously and have the necessary controls in place.

Impact on internal audit

More organisations are turning to internal audit for assurance over third party risk management. Organisations must be able to prove they have an effective framework to mitigate risk from their third party relationships which go above and beyond just obtaining a ISAE3402 report (or similar) once a year and placing these in a draw. If they cannot, stakeholders may lose confidence and the business could face fines or censure. Internal audit is a vital step between an organisation and its third parties, to check responsibilities are clearly defined and necessary controls are in place, with an internal control framework in place to mitigate risks from outsourcing core processes.

IT resilience

Recent research1 shows that IT outages cause the greatest disruption to an organisation's operations. As such, crisis management, business continuity and IT resilience remain high priorities for audit committees over the next 12 months. These areas have undergone significant change in the last few years, and organisations may struggle to meet the new requirements and achieve best practice.

First and foremost, the nature of business disruptions has evolved. Previously, many firms focussed their planning efforts on 'loss of people, buildings or IT', but the risk arena has expanded to include a broader range of scenarios, such as data loss due to a cyber-attack or data breach. It may also refer to loss of key suppliers or social media incidents. In the event of a disaster, business continuity and response plans must be put into action, so they should be fully documented and rehearsed to ensure an organisation's people know what to do. These plans often involve many different areas of the business, who must work together with limited information and short timeframes.

Secondly, in a digital age consumers' expectations have grown and organisations need to be almost always available, recover instantly and lose as little data as possible. Not only do these demands affect IT disaster recovery arrangements, they also impact the IT resilience arrangements which are in place to prevent the disasters from happening in the first place. These arrangements can be technically complex and difficult to manage internally, so many organisations rely on cloud or Disaster Recovery as a Service (DRaaS) to help them fill the gap.

Impact on internal audit

Audit Committees are increasing turning to internal audit to gain assurance that their organisation's IT disaster recovery plans and resilience arrangements are holistic and can protect them against today's threat landscape. Furthermore, an organisation's digital services need careful oversight, and Audit Committees are looking to internal audit for assurance regarding the IT resilience arrangements of any third parties on whom the organisation relies upon.

Technology risk services

Grant Thornton is one of the largest providers of professional services delivering assurance and advisory services to industries as diverse as financial services, telecoms, retail and the public sector, as well as small to medium sized enterprises (SMEs). Within technology riskservices, our client service teams consist of highly specialisedand experienced professionals with extensive experience of keyrisk management areas including:

- IT risk management
- Data and digital security
- Data governance
- Data analytics
- Business and IT resilience
- IT and business process outsourcing
- Project management and system development
- Enterprise resource planning (ERP) technology and business processes
- IT operations
- Cyber security

Our specialist areas

We combine our deep technical skills and market understanding, with a desire to collaborate with you, to manage your IT and project risks. We can support your requirements via co-source and outsource agreements or project specific engagements to suit your needs. This includes provision of resources in the following, but not limited to, specialist areas:

- IT internal audit
- Cyber security and privacy services
- Data analytics
- Business continuity and resilience
- Digital assurance advisory services
- Third party assurance
- Outsourcing risk management
- ERP advisory and assurance services
- Project assurance and advisory services
- IT due diligence

By developing an in-depth understanding of your business, we can effectively

Who should I contact for assistance?

To understand more about our technology risk services or a wider range of our consulting services, please contact:

Christopher Oehri
Director – Advisory IT & Digitalisation
Grant Thornton AG
T +423 237 42 10
F +41 43 960 71 00
E christopher.oehri@li.gt.com

Grant Thornton