# HE Insight

# Risk Briefing – Beyond Higher Education

## September 2018

## Background

The Chartered Institute of Internal Auditors has surveyed company executives with responsibility for risk across Europe (France, Germany, Italy, the Netherlands, Spain, Sweden, the UK and Ireland) to assess where they expect risk efforts to focus in the forthcoming year and further into the future. This survey included a wide range of sectors beyond education and provides a tool for internal audit and audit committees to horizon scan. It follows a similar exercise undertaken last year.

Cyber security continues to be the single biggest risk. New risks to emerge and / or with increasing emphasis over the last year, include those relating to inequality in the workplace and all types of discrimination. Similarly, there is more focus on social media – but recognising that there are significant opportunities as well as risks to manage. Inevitably, Brexit and global / international relations flow through a number of the areas – whether in relation to suppliers, trade restrictions or political uncertainty.

| Risk theme | Comment |
|---|---|
| **Cyber security**<br><br>Detail included:<br><br>• 37% of UK business experienced a data breach in 2017<br><br>• 63% of cybersecurity breaches can be traced back to third party vendors | This was identified as the single biggest risk. Context included:<br>• Increasing sophistication of adversaries (including nation states)<br>• Piecemeal approach to IT infrastructure development over a number of years – migration from unsupported platforms without appropriate testing (penetration testing and ethical hacking)<br>• Cloud based security – Microsoft has reported quadrupling in the number of attacks on its customers cloud based accounts<br>• GDPR data controllers and data processors jointly and severally liable for damage caused by processing of data<br>• Organisations are only as strong as the weakest link in their supply chain through malware ability to infiltrate unsuspecting targets (Petya strike).<br>*Internal audit considerations*:<br>• Ensuring core controls are periodically tested (e.g. firewalls, patch management, access control)<br>• Governance – assessing whether IT is seen as peripheral, rather than core, to development of the business<br>• Greater scrutiny of procurement processes for IT and strategy for the long term<br>• Third party environment – gaining assurance on controls in the same way as internal environment (e.g. password policy). Cloud providers need to ensure that they are GDPR compliant and exercising audit rights to test controls. Assessing due diligence processes for new suppliers. |

| Risk theme | Comment |
|---|---|
| **GDPR**<br><br>Detail included:<br><br>• 80% of analyst time is spent discovering and preparing data rather than analysing it | Area of focus for all those interviewed for the survey in 2019 – not least due to heavy penalties for non-compliance. Context included:<br><br>• Facebook and Cambridge Analytica – use of personal data for political and commercial purposes and increasing demands internationally for accountability<br>• Data – trust and reputation at stake ($70 billion wiped off value of Facebook following the Cambridge Analytica episode)<br>• Exponentially increasing volume of data to be protected – internet traffic expected to treble by 2021.<br><br>*Internal audit considerations:*<br><br>• Is there a Data Management Strategy in place?<br>• Are there processes and protocols for sharing data with third parties and ensuring that this is secure? |
| **Sustainability** – the environment and social ethics (including culture)<br><br>Detail included:<br><br>• 23% of businesses globally are actively tackling climate change | Increased expectation by the public and regulators to behave in an environmentally and socially responsible manner: Context included:<br><br>• EU non-financial reporting directives require reporting and policies on environmental protection, social responsibility and treatment of employees, human rights, anti-corruption and bribery and diversity of company boards.<br>• Challenging to report accurate information (e.g. on sustainability)<br>• Climate change threat – more environmentally friendly buildings, renewable sources of energy, and reduction in vehicle emissions<br>• Human rights – requirement to comply with Modern Slavery Act<br>• Ethical integrity in operations and supply chain.<br><br>*Internal audit considerations*:<br><br>• Are sustainability reports being published as required by EU legislation<br>• Assessment of the maturity of reporting sustainability and extent to which environmental and social ethics statements reflect reality<br>• Performance against peers and availability of sector specific KPIs. |
| **Workplace discrimination and staff inequality**<br><br>Details included:<br><br>• 18% of men and 40% of women in the UK workplace have experienced unwanted sexual behaviour | New emphasis given the high profile issues in the US and #metoo campaign spread by social media. Context included:<br><br>• Gender pay reporting requirement from April 2018<br>• HR investigation of complaints and robust whistleblowing policies and procedures required.<br><br>*Internal audit considerations*:<br><br>• Senior management commitment to changes in societal expectations for women and other marginalised groups<br>• Is there an appropriate "tone at the top"?<br>• Is there a clear anti-harassment policy in place? |

| Risk theme | Comment |
|---|---|
| **Protection of brand and reputation**<br><br>Details included:<br><br>• 75% of board directors consider this a top concern …, but only 6% say they are well versed in social media issues | Context included:<br><br>• Organisational response in the public domain can mitigate or exacerbate reputational harm and therefore communication is key<br>• Positively, social media is low cost, responsive and has the potential to reach millions<br>• Marketing budgets efficacy and evidence of the effectiveness of marketing expenditure – how is the return on advertising expenditure captured and monitored?<br>• Compliance considerations covering how the organisation markets its products, services and itself and avoidance of misleading statements and representations<br>• Policies for what can and cannot be said with appropriate inclusion of social media<br><br>*Internal audit considerations:*<br><br>• Assurance that controls are in place to mitigate the risk of breaching marketing regulations<br>• Sign off procedures for communications<br>• Effective crisis management plan needs to be in place<br>• Where appropriate, prompt appropriate measure and authentic response with willingness to own the issues and put in place prevention for future. |
| **Digitalisation, Automation and Artificial Intelligence (AI)**<br><br>Details included:<br><br>• More than 40% of business leaders anticipate that AI will start displacing some jobs in their industry by 2021 | It is potentially transformative to adopt automation for costs and efficiency, but risks need to be considered. Context included:<br><br>• An assessment of the organisational competitive position re digitalisation<br>• Enterprise resource planning (ERP) and customer relationship management (CRM) systems are initial indicators of digitalisation<br>• Increased automation by the use of algorithms but they are still programmed by humans and, therefore, there is a margin for error.<br><br>*Internal audit considerations*:<br><br>• Are automated processes being risk assessed for data quality, the accuracy of algorithms and outputs and is internal audit equipped to confirm that technologies are working as intended? If not, who is providing this independent assurance?<br>• How is resistance to digitalisation being dealt with and is this adversely affecting the culture of the organisation? |
| **Anti-Bribery and Anti-Corruption compliance**<br><br>Detail included: | Long standing risk but increased penalties and legislative reforms have increased the risk profile. Context included:<br><br>• Enforcement agencies are coordinating their efforts and sharing evidence with enforcement in multiple jurisdictions<br>• Anti-bribery and corruption programmes needed in organisations to demonstrate ethical values and commitment to combatting bribery |

| Risk theme | Comment |
|---|---|
| 57% of bribes are paid to secure public procurement contracts | • Clear and explicit statement that bribery of any form, direct or indirect, is prohibited ('zero tolerance')<br>• Best interests of the organisation to report any issues themselves in a timely manner and cooperate with any investigation<br>• ISO 37001 is the first international anti bribery management system standard – which could be used as a benchmark.<br><br>*Internal audit considerations*:<br><br>• Is there a 'zero tolerance' statement in place and reflected in the organisation's culture<br>• Has a risk assessment been undertaken in respect of anti-bribery?<br>• Are payments to agents and adviser made with sufficient segregation of duties and due diligence processes? |
| **Pace of change and adaptation to it** | Change means that risk, governance and control environments become outdated very quickly.<br><br>*Internal audit considerations*:<br><br>• Can the ability of the organisation to innovate (and change at pace) be assessed?<br>• Does an innovation strategy align with the overarching corporate strategy?<br>• How does technology affect the control environment?<br>• Are redundant of ineffective controls which do not mitigate risk dropped or replaced? |
| **Trade restrictions and political uncertainty** | Trade sanctions and US/China "tit for tat" competitiveness of trade and protectionist policies and European disruption due to Brexit and ensuing uncertainty. Context included:<br><br>• Trade and economic sanctions impacting exporters<br>• Assessment of risk to determine whether the supply chain needs to be restructured<br>• Unpredictability of the US Trump administration.<br><br>*Internal audit considerations*:<br><br>• The impact of sanctions and trade barriers are not always obvious and may be indirect<br>• The ability to audit these risks is questionable but risk assessments of supply chains and potential for disruption should be in place<br>• Assurance on the organisation's ability to respond to policy changes and put in place mitigating actions and contingency plans. |

# How can we help?

Internal audit should be risk based – and the programme should be aligned to the risks in the risk registers. Increasingly, this means that coverage will be wide ranging and looking forward as well as backwards.

Not surprisingly, IT and data themes remain prevalent. The survey highlighted a mismatch between the most important risks and internal audit coverage with a suggestion that not enough time is spent on cyber / IT risks and excessive time on general mandatory compliance audits (partly driven by external funders and expectations).

Whilst acknowledging that internal audit teams need to have the requisite skills and expertise, it's timely for organisations to be (1) comfortable that they are capturing the real risks on their risk registers and (2) mapping the sources of assurance against them.

For further information on how we can help or any other aspect of Uniac's internal audit and assurance service please do get in touch.

Richard Young
Director
t: 0161 247 2959
e: ryoung@uniac.co.uk
www.uniac.co.uk