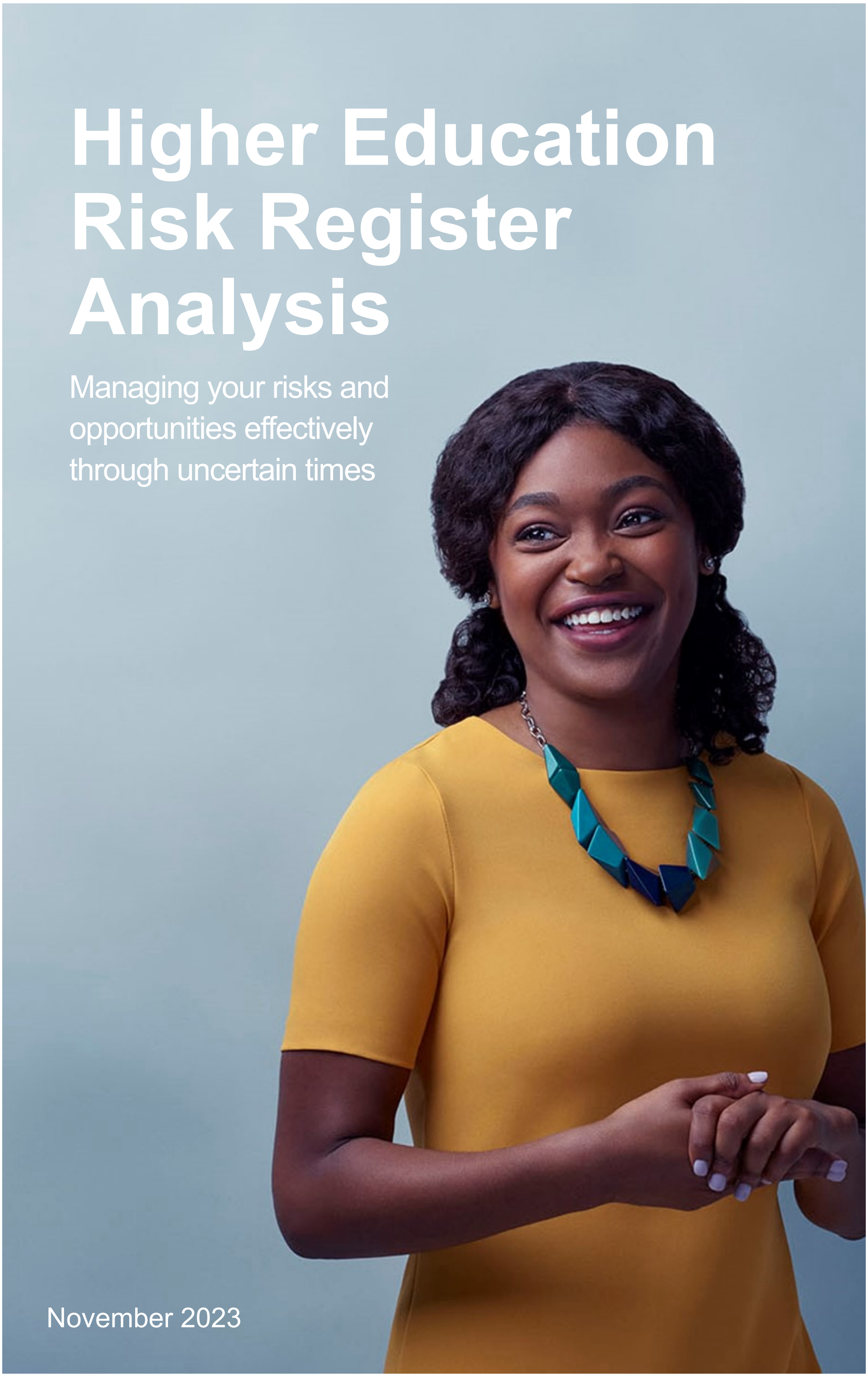
# Higher Education Risk Register Analysis

Managing your risks and opportunities effectively through uncertain times



November 2023

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

# Contents

# Executive summary

The higher education sector faces several uncertainties and interrelated risks and opportunities which need to be identified and managed robustly. This is necessary not only to protect the institution, but also to enable effective risk mitigation and opportunity maximisation in the face of significant change in student and regulatory needs.

These are tough times for students, staff and institutions, with rising costs having an impact on most institutions to varying degrees, creating financial pressures. This is coupled with technological advancements, evolving regulatory frameworks and shifting student expectations.

There is also a continued narrative focused on what constitutes 'quality' in respect of higher education, and the outcomes students achieve after graduating.

Providers also remain under immense pressure to safeguard stakeholders, alongside demonstrating positive equality, diversity and inclusion, and enhancing quality and experience, at a time of static tuition fees for the foreseeable future, higher operating costs and people pressures.

Effective risk management is crucial to drive focus on the institution's sustainability, resilience and ability to provide high-quality education and support services to students. By identifying and addressing potential risks and opportunities, the institution can potentially enhance its decision-making processes, allocate resources more effectively and minimise the negative impact of predictable or unforeseen events, or take opportunities in line with its risk appetite and accompanying growth strategies.

Although complete risk elimination is not possible, a strong risk management approach involves comprehending and efficiently managing potential risks. Providers should maintain current risk profiles and descriptions, aligning robust internal controls with each identified risk, while ensuring they are in accordance with the provider's risk tolerance. Seeking relevant assurances gives audit committees, or equivalent and senior management, the confidence that controls are effectively operating and informing the board or council's assurance framework, including in collaborative efforts or engagements with third-party providers.

Against this backdrop, we have undertaken our latest analysis of institutions' strategic risk registers. This publication is intended to help providers challenge their own risk profiles and assist them with ongoing risk identification and opportunity management.

# Overview of key risks

In undertaking our analysis, we have examined 377 risks collated from 21 client risk registers. We have categorised each risk by key theme and, where appropriate, applied sub-themes to understand those areas of greatest concern to higher education institutions in the UK.

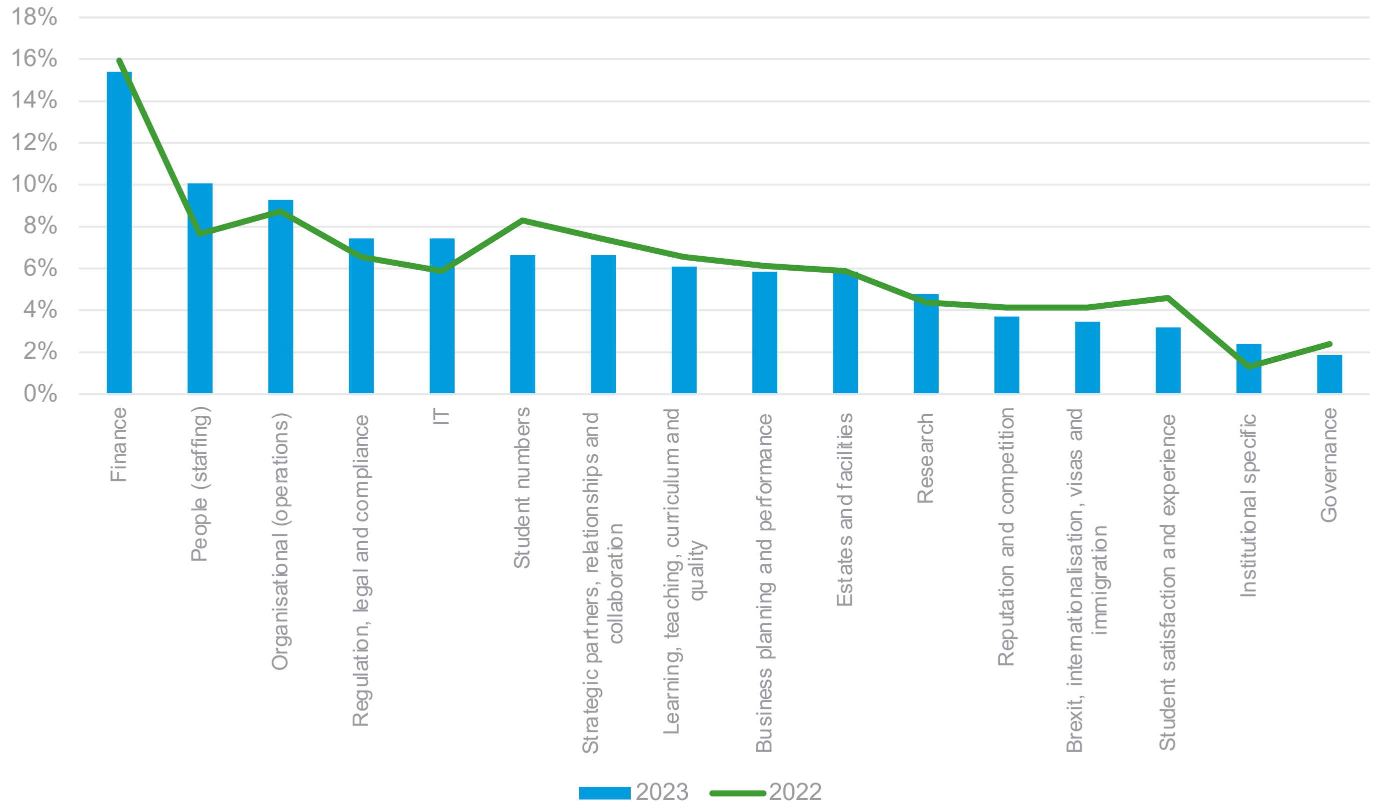
## Quantities of risks

In terms of quantities (number) of risks, from the risk registers in our sample, the top three risk areas were:

1. finance, representing 15% (58 risks);
2. people/staffing, at 10% (38 risks); and
3. organisational (operations), at 9% (35 risks).

Finance-related risks have consistently been the top risk area since our original 2012 analysis, which reflects the overarching concern in relation to financial stability and sustainability. This takes into consideration the fluidity in student recruitment and retention, while there are also heightened costs in relation to people, estates and general operating expenditure.

Figure 1: Analysis of risks between 2022 and 2023



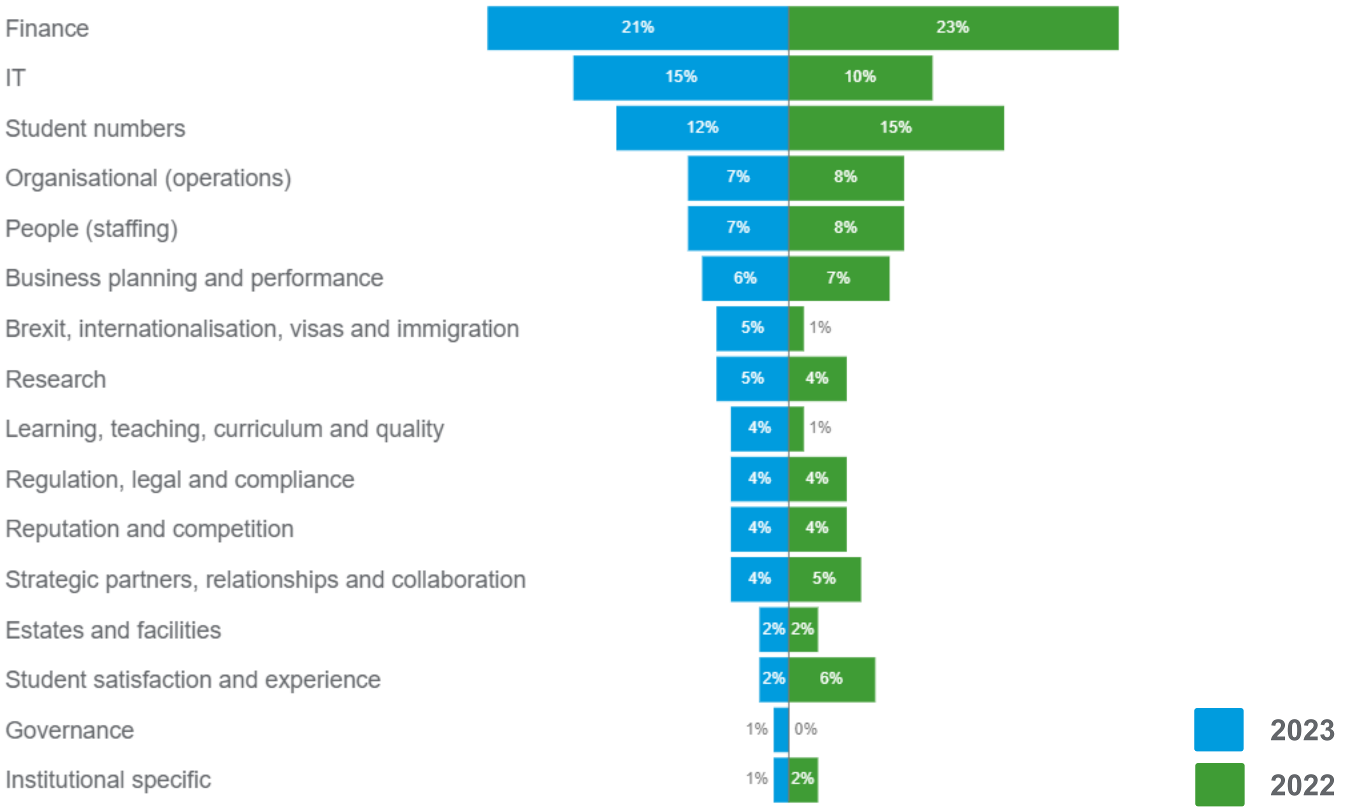
## High risks

We captured the residual risks (post controls and applied mitigations) considered by our higher education clients to be 'high' risk in terms of severity.

105 (28%) of the risks across the risk registers in our sample were deemed to be 'high'. The top three areas were finance, IT and student numbers; this remains in line with our analysis in 2022. While IT and student numbers are in the top three when analysing all 'high' risks, these risks were marginally less in terms of quantities (as seen in Figure 1 above). Despite being fewer in number, IT and student numbers remain among the top three 'high' risks. This is reflective of the external cyber considerations facing universities, which is a result of a cyber-attack at a university in the North West; and the demographic, policy and other factors impacting on home and international student numbers, alongside the regulatory changes for some international postgraduate students coming to the UK for studies.

The significance of the interdependencies and interconnections between the risk areas has never been as important in understanding the impact on the financial sustainability and related stress testing at an institution. Figure 2 below demonstrates the marginal movement in the top risks analysed between 2022 and 2023.

Figure 2: Percentage of 'high' risks between 2022 and 2023



# Financial

Higher education institutions face escalating costs in areas such as maintaining facilities and infrastructure; salaries; pensions; investing in technology and IT; and academic resources, materials and research. Managing operating costs and finding cost-saving measures are critical to maintaining financial stability.

The sector is well versed in this and over the years has demonstrated overall effective financial management, supported by external reports from the National Audit Office by way of example. The board's continued understanding of its strategic financial risks and the assurances it receives does remain a focal point, and this was heightened again during the pandemic as delivery models evolved, digitalisation was fast-tracked and what became the new norm was created. Financial oversight and scrutiny remain a priority for boards and are fundamental to good governance; and taking the learning of the past three years, with stakeholder requirements evolving, public culture changing and demands increasing, emphasis on such matters remains pertinent. The sector has seen the value that strong financial metrics have for a provider, whether for refinancing purposes, or to give confidence to lenders and stakeholders, or those engaged in joint ventures and partnership working. Therefore, it comes as no surprise that financial sustainability remains the top risk.

The latest report on **financial sustainability** by the Office for Students (OfS) noted that 'the aggregate financial position of universities, colleges and other higher education providers registered with the OfS remains sound'. Yet, significant variation remains in the performance of higher education providers, and there are growing risks from an overreliance on international students and from inflationary pressures. The OfS noted that the financial health of the sector is underpinned by overseas fee income, and overreliance on overseas fees remains a vulnerability.

Income from course fees and educational contracts is forecast to increase by 27% between 2020/21 and 2024/25. We have already witnessed, across the sector, significant shifts for some institutions in income levels from home to international students. Fee income from EU domiciled students is expected to decline by 8.5% overall between 2020/21 and 2024/25. Analysis prepared by UCAS confirmed that there was continued growth in applications from international students, but reductions in the number of applications from people within the EU. International students are significantly important to providers and their income, but as the cost-of-living crisis intensifies, regular financial modelling and scenario planning remain key, alongside the support and welfare that international students may require when settling into the UK and campus life. Inevitably, student numbers remain a high-level strategic risk (12%), appearing on most risk registers. Providers had clearly outlined in their risk registers that most of these risks would have financial consequences.

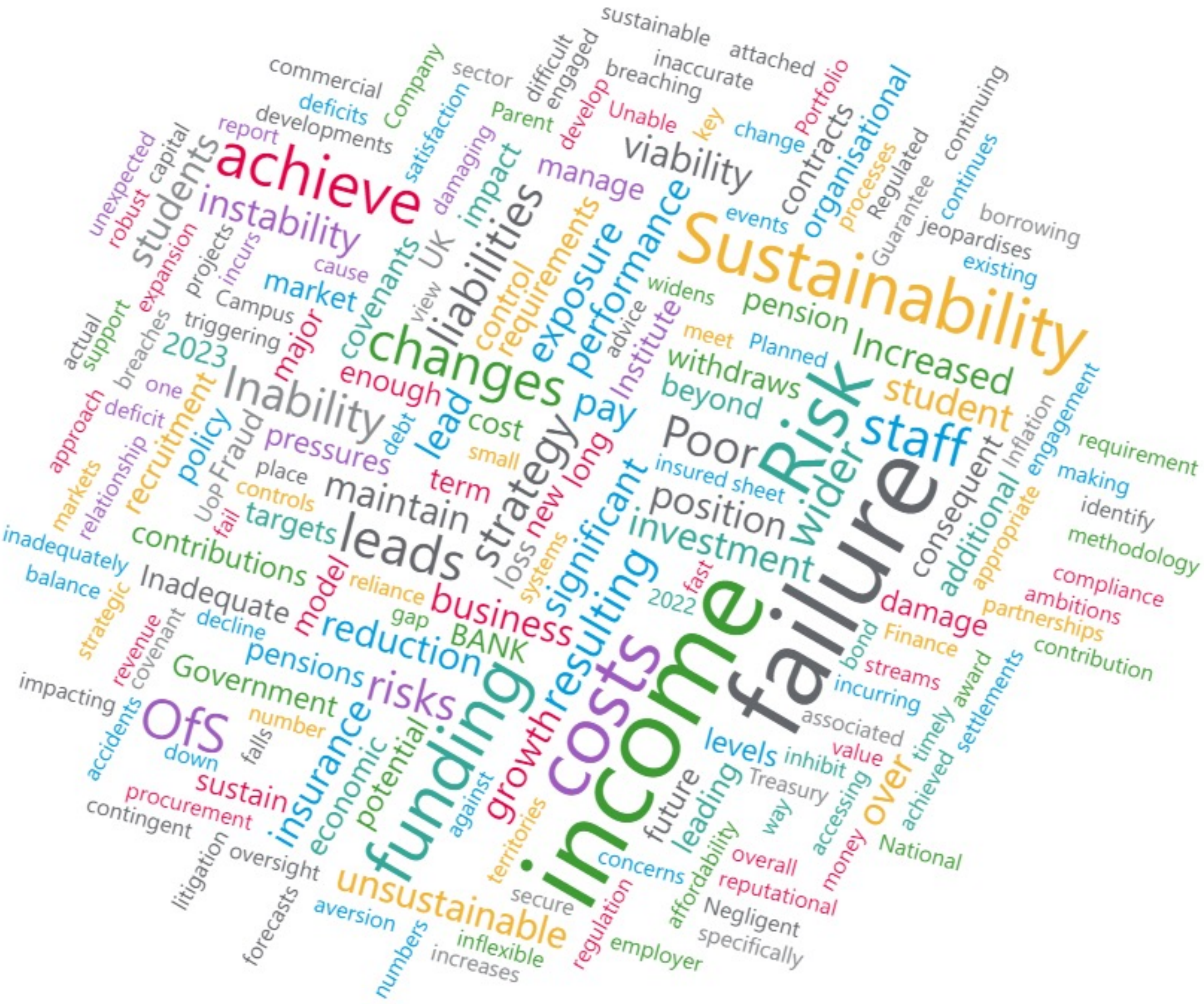
The rising cost-of-living could still impact student recruitment and retention, and while providers have continued to provide additional support, funds are limited. Potential applicants and their families could still take the view that attending higher education is less affordable, and a strong apprenticeship opportunity provides income security, with day release. The environment remains challenging. To protect longer-term sustainability, providers will need to continue to adapt to uncertainties and financial risks. Continued, robust student number projections and planning remain important to ensure that business plans are sound. For some institutions, even small percentage changes between planned and actual student numbers can have a significant financial impact.

The sector faces a challenging time in the aftermath of Covid-19 and in the current financial climate. Costs continue to rise, and with limited availability of talent and suppliers in some areas, this is expected to continue. Competition for UK students continues to be fierce with many institutions exploring how to diversify their income streams. Boards should continue to focus on financial projections, ensuring these include sensitivity to known financial risks.

## Types of finance risks

The word cloud provides a visual representation of the key elements contributing to the financial risks documented on the risk registers. The interdependencies of risks are evident, and understanding this will allow organisations to develop more comprehensive risk management strategies.

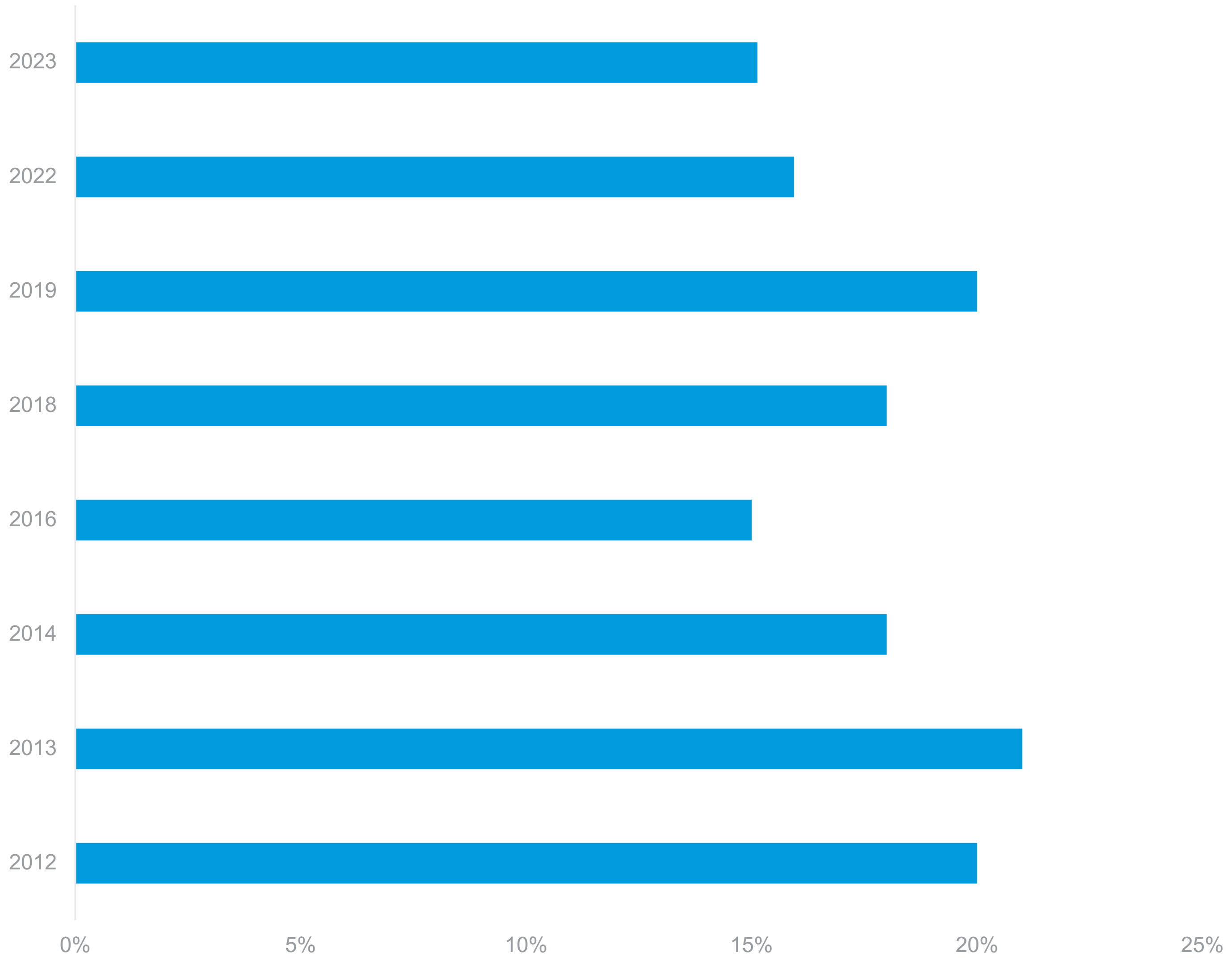
Figure 3: The word cloud illustrates those key elements which contribute to the financial risks recorded on risk registers



Our latest risk register analysis shows the trajectory of financial risks. According to our analysis, and as shown in the graph below, since 2012, the number of finance-related risks has fluctuated. In 2013 the number of risks peaked at 21%; this was followed by a gradual variation of 18% and 15% between 2014 and 2018. In 2019 the number of risks rose again to 20%. The last two years have seen a decline in this number, with finance risks at 16% and 15% in 2022 and 2023 respectively. However, we are seeing an increase in other risk areas, such as people (8% in 2019 and 10% in 2023) and IT (6% in 2019 and 7% in 2023).

Organisations are increasingly recognising the importance of people-related matters and therefore are likely to be focusing more on people risks. Likewise, the changing landscape of cybersecurity and data protection is contributing to an increased focus on IT risks. The rise of remote working and the increasing reliance on digital platforms during the pandemic are also contributing factors likely to have intensified IT-related risks.

Figure 4: Number of finance risks between 2012 and 2023 analysed by percentage



In taking a deeper look at the finance-related risks across the risk registers, we found key risks recorded regarding the following:

**Cost increases and losses – as cost pressures increase, the need for operational efficiencies becomes greater, as institutions seek to achieve long-term sustainability.**

- Risk of incurring unexpected, one-off costs which cause providers to report a deficit.
- Pressure on costs accelerating faster than revenues.
- Income is declining and inflation increases costs beyond what is affordable.
- Pension risks, including unaffordable pension arrangements and potential changes to contributions, linked to pay awards.
- Poor approach to procurement could lead to poor value for money and reputational damage.

**Economic climate and financial health – with focus very much centred on the overall economic climate and institutional financial health.**

- Financial difficulties arising from the negative impact of the wider economic climate.
- Inability to maintain a financially sustainable position, impacting on future viability.
- Failure to achieve the outcomes set out in the financial strategy. Where organisations are unable to manage income and costs, financial strategy will not be achieved risking long term financial sustainability.

**Government funding/policy – the political landscape and government policy changes represent very real risks to the sector’s perceived financial sustainability.**

- Changes in government policy or a redirection of funding could negatively impact the sustainability and longer-term financial viability of the organisation.
- Funding methodology changes lead to reduction of income.

There were also risks recorded in relation to opportunities and income maximisation, banking covenants and loans, budgetary management, fraud, and insurance.

## Risks with financial repercussions

We are seeing numerous risk areas outside of finance risks having financial repercussions. 80 of the 377 risks collated were highlighted on risk registers as having a negative financial impact. Our analysis showed that, as expected, student numbers accounted for the most risks resulting in financial repercussions, followed by IT, business planning and performance, and regulation, legal and compliance.

Figure 5: Non-finance risk areas that are having a negative financial impact.

| | |
|---|---|
| 15% | Student numbers |
| 13% | IT |
| 10% | Business planning and performance |
| 10% | Regulation, legal and compliance |
| 9% | Organisational (operations) |
| 9% | Research |
| 6% | People (staffing) |
| 6% | Strategic partners, relationships and collaboration |
| 5% | Brexit, internationalisation, visas and immigration |
| 5% | Learning, teaching, curriculum and quality |
| 5% | Student satisfaction and experience |
| 3% | Estates and facilities |
| 3% | Reputation and competition |
| 1% | Governance |

# People

Similar to other industries, retaining high-quality staff is a significant concern in higher education. In addition, if there is a perceived lack of diversity and inclusion within institutions, this can influence the successful recruitment and retention of staff. Institutions should ensure their recruitment processes are robust and actively seek to create a culture of inclusivity.

With inflation outpacing pay awards in many industries, businesses are focusing on how they might support their employees through the cost-of-living crisis, when they are already managing a tighter and more challenging budget and face an uncertain outlook. In its **2024 Risk in Focus** report, the Institute of Internal Auditors noted that 58% of survey respondents cited human capital, diversity and talent management as a top-five risk. Related risks have arguably intensified in this area.

At 10%, people (staff) risks have remained broadly consistent since 2012, yet there are more risks focused on recruitment, retention and withdrawal, which is industrywide. By recognising and seeking to mitigate those key people-related risks, through for example implementing enhanced employee engagement programmes and other support services, institutions are better placed to attract and retain qualified and dedicated staff, and in turn promote a positive working environment.

The people-related risks across our registers included a failure to:

- attract, recruit, develop and retain high-quality staff, leading to an inability to operate effectively and to offer high-quality teaching and research;
- meet equality, diversity and inclusion (EDI) requirements and adequately respond to EDI initiatives;
- address the gender pay gap, resulting in inequality and imbalance within the workforce, leading to negative perceptions that impede recruitment and retention of staff;
- adhere to employment legislation and standards of good HR practice, leading to staff morale issues and/or litigation; and
- maintain good employee relations – particular areas of concern relate to increased mental health and staff wellbeing concerns.

With a multitude of pressures facing higher education, the results of the sector's people challenges are being seen more than ever. Our clients have moved people-related topics up their risk register year-on-year in an attempt to mitigate potential issues. The ability to keep people remains one of the biggest risks for our higher education clients. Though pay plays a significant part in this, the HR processes around retention are rarely robust enough, often with gaps in design or consistency in implementation across the staff population.

Other areas such as recruitment and performance management often show similar areas to focus on. Higher education institutions have needed to consider more innovative solutions to broaden their candidate attraction methods, as well as more effective career pathways for existing members of staff. RSM has found that reviewing and developing a broad range of benefits can be an effective solution in this area. Whether that be additional opportunities for agile working where appropriate or enhancing support for family leave over and above statutory requirements. This can be effective in reducing not only the risk but also the impact of those issues within recruitment and retention.

For more information, please contact **david.gibbens@rsmuk.com** or **donna.clark@rsmuk.com**.

**Things to consider:**

- creating an organisation where employees can access opportunity, see diversity throughout the organisational structure and feel genuinely able to bring their whole selves to work is part of protecting organisations in the long term.
  It should be a key focus for any ESG or people strategy;
- one size does not fit all. Every employee has their own needs in terms of flexibility, progression, development and their own sense of wellbeing. Traditional performance management processes need to be adapted to account for this; and
- engagement surveys help businesses to 'take the temperature' with their staff, especially if employees feel that they can respond anonymously. It provides them with the chance to voice concerns and contribute to conversations about the employee experience.

For more information, access our report: **The Real Economy – UK – Modern Workforce**

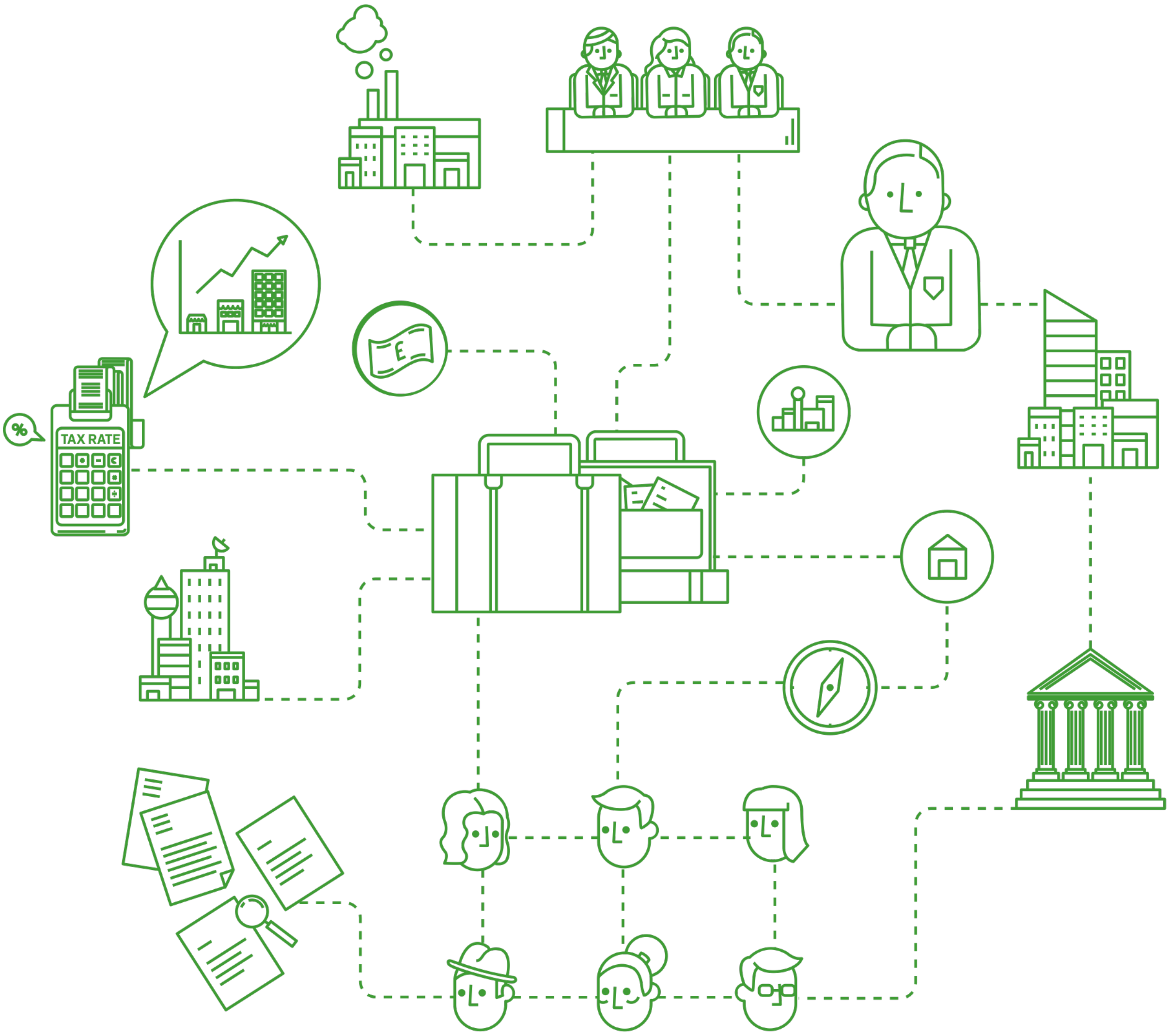
### People Perspectives – redefining the workforce

In The Real Economy’s latest topical survey on workforce challenges, we asked our panel of middle market business leaders about three key topics: recruitment and retention, hybrid working and globalisation, and technology and skills. With expert insights and data from the heart of the middle market, we uncover the prevailing trends and strategies that map today’s dynamic labour market.

Key findings include:

- 41% of businesses have experienced rising salary costs, 40% performance management issues and 37% skills shortages;
- 69% of businesses have redefined their workforce strategy as a result of staffing challenges;
- in the last 12 months, the top actions businesses have taken due to staffing challenges have been improving employee benefits (40%), automating processes (37%), increasing salary levels (35%) and implementing a hybrid working model (35%); and
- the top five offerings by businesses to attract or retain employees are hybrid working (41%), healthcare benefits (35%), flexible hours or schedules (33%), wellness options (28%) and employee recognition programmes (28%).

Read the full report on the RSM website: **People Perspectives | The Real Economy | RSM UK**



# Organisational

Higher education institutions face numerous organisational (or operational) risks that can impact their overall effectiveness and reputation. Operational risks made up 9% of the risks that pose a significant threat to the organisation. This is consistent with last year's analysis.

Many of the organisational risks related to safeguarding and health and safety (47%). Other external factors, such as coronavirus, institutional disruption and business continuity, are also significant within the risk registers in our sample. Safeguarding and health and safety risks can have significant implications for the overall learning environment, institutional reputation and legal/regulatory compliance.

Mental health concerns among students have become increasingly prevalent in higher education. The Office for National Statistics' **latest survey** on the impact of the cost-of-living crisis on university students found that 46% of students reported that their mental health and wellbeing had worsened since the start of the autumn term in 2022. Factors such as academic pressure, social isolation and the transition to university life can contribute to mental health challenges. Institutions should promote mental health awareness, offer counselling services, provide training for faculty and staff to recognise signs of distress, and create a supportive campus environment. Establishing peer support networks, promoting self-care practices and reducing stigma around mental health can help mitigate these risks. The OfS' focus in this area, alongside harassment and sexual misconduct are key areas of discussion and internal review and is covered in the next section.

Organisational risks include a failure to:

- respond to a changing external environment and policies, for example changing government policies;
- respond effectively and appropriately to business interruption and to adverse events such as a new pandemic or major world event which could in turn disrupt student recruitment;
- provide support for mental health issues for staff and students; and
- ensure effective safeguarding systems are in place in order to provide a safe learning environment for students.

The areas of risk related to business interruption and adverse events are mirrored in the **National Risk Register 2023** published by the government, very much demonstrating the different levels at which global issues now impact at country, institution and person level. As governments respond to these issues, they of course make policy decisions which impact on the industry, meaning adaptability is a key trait for institutions.

The increasing prevalence of reported cases of mental health and wellbeing matters goes hand in hand with the need for further development of safeguarding arrangements. Safeguarding arrangements are embedded in the pre-18 education system and historically have been less of a focus in the post-18 education system; there needs to be a more nuanced application in the industry, given the range of students from young adults through to mature students, and this remains a work in progress for some institutions.

# Regulation, legal and compliance

## Risks related to regulation and government policy continue to be a significant concern for higher education providers.

Providers need to comply with the OfS conditions of registration, the UK Data Protection Act (which embeds the General Data Protection Regulation, or, as it is more commonly known, GDPR, into UK law) and health and safety requirements, as well as other legislation, of course. Failure to comply with laws and regulations can have severe ramifications, including financial penalties, regulator sanctions and reputational damage.

Risks related to regulation, legal and compliance in the risk registers in our analysis include a failure to:

- comply with OfS conditions of registration or maintain registration;
- observe statutory requirements;
- provide appropriate legal, corporate and research governance;
- have appropriate information management and data quality and data protection controls in place; and
- adapt to changes in government policy and regulation, and subsequent changes in the market.

# Harassment and sexual misconduct

## The OfS has proposed a **new approach** to the regulation of harassment and sexual misconduct affecting students in registered higher education providers.

Universities and colleges would need to maintain a register of personal relationships between staff and students under the new plans. The relationships register would apply to certain personal relationships in circumstances where a staff member has particular responsibilities towards a student, for example where an academic is responsible for assessing a student's work. The consultation proposes that any academic not disclosing such a personal relationship should be liable for dismissal.

The OfS has proposed a new condition of registration for harassment and sexual misconduct. If a condition is introduced following the consultation, universities and colleges would have to take a number of steps, including:

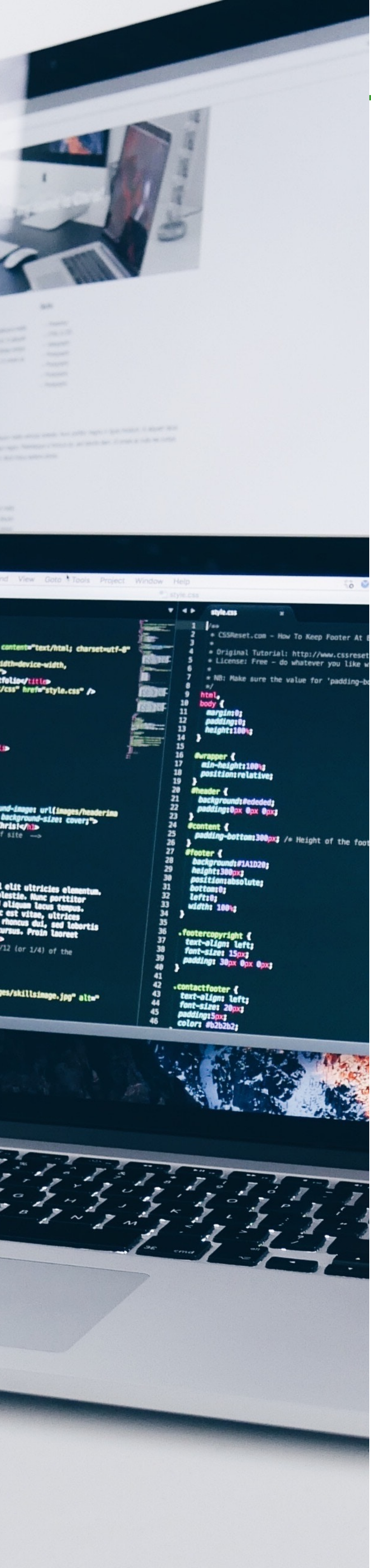
- introducing mandatory training for students and staff – this should include 'bystander training' for potential witnesses to raise awareness of and prevent sexual misconduct;
- publishing a single document setting out how an institution will make a significant and credible difference in tackling harassment and sexual misconduct – the document would include information about how to report cases of harassment and sexual misconduct, and explain how students will be supported through the process; and
- banning the use of non-disclosure agreements in cases of harassment and sexual misconduct, and any enforcement of existing non-disclosure agreements.

This area of regulation will continue to evolve, and institutions should ensure that all associated risks are considered as part of their wider risk management and risk register updates. Look out for our report detailing the outcomes of our internal audit reviews of harassment and sexual misconduct at providers.

Based on our experience, it is only over the last 12 months or so that we have found higher education institutions starting to engage with this area of risk more openly due to its highly sensitive nature, coupled with the many associated complexities, from reporting through to investigation. For any higher education institution that is not seeking to assess the effectiveness of existing sexual harassment risk management arrangements and continually improve these, the implications could be significant, from a best-use-of-resources and reputational perspective. Getting it wrong or not being willing to accept the severity of this risk will be deeply damaging, while openly engaging, talking about and promoting what is being done can strengthen an institution's brand and profile.

RSM, in conjunction with a community interest company, The Subtle Group, has over the last 12 months been working with a number of higher education institutions and businesses in the night-time industry, via a number of pilots, to create a sexual harassment risk assessment tool. This has culminated in the launch of Safer Dance, a stakeholder-focused membership scheme enabling those that participate to access online solutions, information and advice in connection with establishing and strengthening their sexual harassment risk management.

More information can be found at **www.saferdance.org** or please contact **matthew.humphrey@rsmuk.com**.



# IT

Of all ‘high’ risks in total, IT risks featured second only to finance. An organisation’s senior leadership have a key role in ensuring a robust cybersecurity strategy is in place.

It is therefore vital that any board has representation from someone with comprehensive knowledge of the cybersecurity landscape and is able to challenge and support any cybersecurity-related decisions being made by the business.

Jisc’s **cybersecurity posture survey** looked at how the UK education and research sectors are dealing with the evolving threat of cyber-attacks. The survey found that cybersecurity remains a priority for senior leaders, with 97% of higher education providers including it on their risk register, while 87% of providers regularly report on cyber risks and resilience to their executive board. The number of organisations with dedicated cybersecurity staff continues to rise, with 90% reporting specialist roles. It was also highlighted that ransomware/malware was the top threat to higher education, with phishing/social engineering second.

## Generative Artificial Intelligence (AI)

With ransomware booming and cyber-attacks hitting headlines daily, crippling businesses, the automation that AI brings will be a vital tool for those trying to fight this type of cybercrime, as well as other frauds. Unfortunately, it is also invaluable for the criminals enacting these crimes.

The Real Economy’s latest research found that:

- 76% of businesses that have successfully implemented automation say that they have improved productivity, with a further 64% having provided training for those working with automation, while 44% have accepted more orders, 35% have redeployed staff within the business and 29% have reduced headcount;
- 44% of businesses believe that AI will have a very positive impact on their business in the next three years, with a further 49% responding that AI will have a somewhat positive impact; and
- 51% of businesses believe that automation and AI will lead to a reduction in their workforce in the next three years, while 19% believe the same initiatives will lead to an increase in workforce numbers.

Read the full article on the **RSM website**.

## Emerging risk

# AI is scaling up one of the biggest threats to businesses, which is ransomware.

A human-driven ransomware attack, which is targeted and tailored to a specific organisation, cannot be done at scale. The introduction of AI means that such attacks can in large part be automated. In terms of security, AI allows automation in relation to monitoring systems, changing codes and registering new domains, which can all be done without time-consuming human intervention.

Key actions for businesses are:

- hire skilled AI cybersecurity professionals;
- implement AI intelligence operations;
- invest significantly in IT audits;
- provide and enforce diligent fraud and cybersecurity training;
- enhance cyber-hygiene and condense sprawling legacy systems;
- complete penetration testing; and
- invest in defensive AI.

Read the full article on the RSM website:
**Generative AI – fraud friend or foe | RSM UK**

Of course, AI has particular implications for higher education. For instance, to maximise the benefits of AI, students and staff need to be 'leaders in an increasingly AI-enabled world', which will require significant investment. The Russell Group has produced **New principles on use of AI in education** to provide a framework for the future.

There are also the risks of AI to be managed, which, for the higher education industry, include ensuring that assessment methods are robust enough to detect where work submitted is not the student's own.

**The IT risks in the risk registers in our sample included:**

- the failure of security measures designed to mitigate the risk of a cyber-attack, leading to financial or reputational damage;
- IT network security breaches, leading to damage or misappropriation of data;
- inadequate management of cybersecurity risks, such as malware, phishing, hacking and equipment loss or theft, which can result in regulatory fines, the loss of critical systems and damage to the institution's reputation;
- the failure to agree, appropriately prioritise or implement the digital plan to support IT infrastructure development;
- the failure to invest sufficiently in digital infrastructure; and
- the failure to manage and store data securely, which can lead to breaches in legislation and regulation and incur substantial fines and reputational damage.

### Managing the increasing cyber-crime threat

We continue to see providers identifying cybercrime as a key strategic risk, and the threat is growing. Cybercriminals are becoming more sophisticated in their techniques and approach, as awareness of the cybercrime threat grows. RaaS (ransomware as a service) and ransomware attacks are on the rise, and phishing or whaling attacks are becoming increasingly difficult to identify. Cybercriminals remain intent on exploiting employees, who are often the weakest link in an organisation's cybercrime defences.

**Has your IT incident response plan been tested recently?**

A comprehensive incident response plan is essential, as it will guide a provider's response to an attack. At a minimum, a formal incident management policy and related processes should be in place, including:

- roles;
- responsibilities;
- accountabilities;
- references to related regulation;
- reporting requirements; and
- explicit examples of what constitutes an incident or security breach.

## Top six things to consider to minimise threats and strengthen cybersecurity resilience

### Governance

Keep your security policy and procedures up-to-date and well publicised internally.

### Frameworks

Implement or benchmark your cyber controls against industry standard frameworks.

### Threat modelling

Understand your assets, their risks and the potential impact of a security event.

### Penetration testing

Get to know your organisation’s network and where your vulnerabilities are.

### Phishing and whaling exercises

Ongoing and regular testing is vital in creating a security culture.

### Incident response

Practice your recovery plans and incident response procedures.

# Other risk areas in summary

The below risk areas continue to be themes that appear on provider risk registers. We summarise those key risk areas, which sit outside of the top five in terms of quantity.

**Strategic partners, relationships and collaboration**

- A poor relationship with the Students' Union and poor services to the student community, which could lead to a breakdown in communication and poor student satisfaction.
- Failure to realise opportunities for engagement and partnerships, or damage to existing partnerships, giving rise to potential financial and reputational damage.
- Failure to manage collaborative partnerships effectively to produce quality outcomes and performance metrics.

**Student numbers**

- Failure to recruit sufficient domestic and international students.
- Failure to retain students, which impacts income from fees and wider financial sustainability.

**Learning, teaching, curriculum and quality**

- Failure to maintain learning and teaching quality and standards (especially in light of the July 2023 announcement that the government has asked the OfS "to limit the number of students universities can recruit onto courses that are failing to deliver good outcomes for students").
- Concerns that courses do not meet the needs of students or reflect demand.

**Estates and facilities**

- Concerns that failing to maintain the estate to a good standard may impact on student recruitment and damage reputation.
- Inadequate management arrangements for delivery of capital projects and developments.

### Business planning and performance

- Failure to achieve and maintain accreditation from professional bodies.
- Quality assurance requirements not being met.
- Failure to maximise opportunities and adapt in a rapidly changing environment.

### Research

- Failure to expand research capacity, which then impacts future research opportunities, funding, reputation and rankings.
- Insufficient capacity to achieve desired research outcomes.
- Failure to develop a research environment that can attract staff.

### Reputation and competition

- Failure to develop a strong organisational reputation.
- Reputational damage as a result of a poor external assessment, which in turn leads to poor student recruitment.

### Brexit, internationalisation, visas and immigration

- International student programmes not being adequately managed.
- Geopolitical changes such as the ongoing impacts of Brexit, UK devolution and global conflicts, which impact students and staff.
- International student numbers being negatively affected due to UK Visas and Immigration regulations.

### Student satisfaction and experience

- Failure to maintain student satisfaction levels, leading to loss of students.
- Failure to provide and maintain a high-quality student experience.

# Conclusion

This analysis highlights the continued challenges and uncertainties that institutions face in a rapidly changing environment. While we explore the various risk areas, institutions should ensure there are strategies and controls in place to successfully mitigate the associated risks.

Effective financial practices, such as embracing strong governance and leadership, investing in robust IT infrastructure, navigating emerging digital technology, maintaining regulatory compliance, and adapting to external factors, are key to managing those risk areas.

We have seen no new risk areas, and the areas we have highlighted continue to be the key risk areas we have observed throughout the years in which we have conducted this analysis. A significant factor to note is the interconnectivity of risks. A comprehensive approach that considers the interactions between different risks can better equip providers to proactively mitigate potential threats and enhance resilience in the face of uncertainties.

The rise of AI also presents an emerging risk for providers. As AI technologies continue to advance, their impact on higher education institutions, students, faculty and the overall academic landscape becomes increasingly significant. To effectively manage the emerging risks associated with AI in higher education, providers need to adopt proactive risk management strategies, including developing clear policies and guidelines for AI implementation. By addressing the challenges posed by AI, higher education institutions can harness its potential to enhance teaching, learning, and administrative practices while mitigating potential adverse effects.

Changes in the regulatory landscape are ever evolving, with for example the OfS' new **approach** to the regulation of harassment and sexual misconduct. Providers should ensure that their approach to harassment and sexual misconduct enables students to freely participate in all activities during their time in education without facing fear or risk of sexual harassment, violence or abuse, and without facing fear or risk of negative consequences if it does happen and they make a report.

The Department for Education also announced that it plans to limit the number of students that can enrol onto courses that are deemed 'poor quality'. The stated intention is that this seeks to protect students' interests, ensure fair value for money and maintain the integrity of the higher education system.

The government plans to introduce stricter regulations and provide clearer information to prospective students about the 'quality' and outcomes of different courses. Under the plans, the OfS will be asked "to limit the number of students universities can recruit onto courses that are failing to deliver good outcomes for students". If these plans are implemented, universities offering courses deemed as poor quality, possibly based on the existing metrics, may face limitations on student recruitment, leading to potential financial implications for these institutions.

Restricting student enrolments in these courses would affect their revenue streams and could affect their overall financial stability. Institutions will need to comply with these restrictions and ensure their courses meet the required quality standards to avoid potential penalties and reputational risks. While it aims to protect students' interests, the enforcement of stricter regulations and limitations on student recruitment may pose challenges for universities, making it an emerging risk in the higher education sector.

This is a complex issue, as it is noted that being a university graduate, regardless of the degree taken, continues (on average) to result in a salary premium and being more likely to be employed (**graduate labour market statistics, Calendar year 2022 – Explore education statistics**). It has been clear for some years that based on the existing conversion rates into higher education, projected demographic growth could not be accommodated by the existing capacity and infrastructure. Also, given the wider economic challenges, the sustainability of the upfront investment in higher education by the taxpayer would be an area for reflection for the **Journey to a Million** in 2030.

With the constant evolution and revolution of digital technologies including AI, combined with climate change and geopolitical changes, it may be time to truly harness risk management strategies to show how institutions can deliver the skills and insights needed to keep UK HE plc at the forefront of global developments.

## Emerging risk considerations

How will emerging risks affect your organisation? What do you see as the emerging risks?

How will emerging risks play through into your existing strategic risks, and how far will they change the way you currently manage your strategic risks?

How will you respond, and how will you continue to keep under review the risks emerging?

For a copy of our latest emerging risk radar, visit the **RSM website**.

# Risk management

To effectively manage risks, higher education institutions should have robust risk management processes in place, including regular risk assessments, mitigation strategies and contingency plans. They should also establish clear lines of communication and responsibility for risk management across the institution, while ensuring senior executive oversight and accountability.

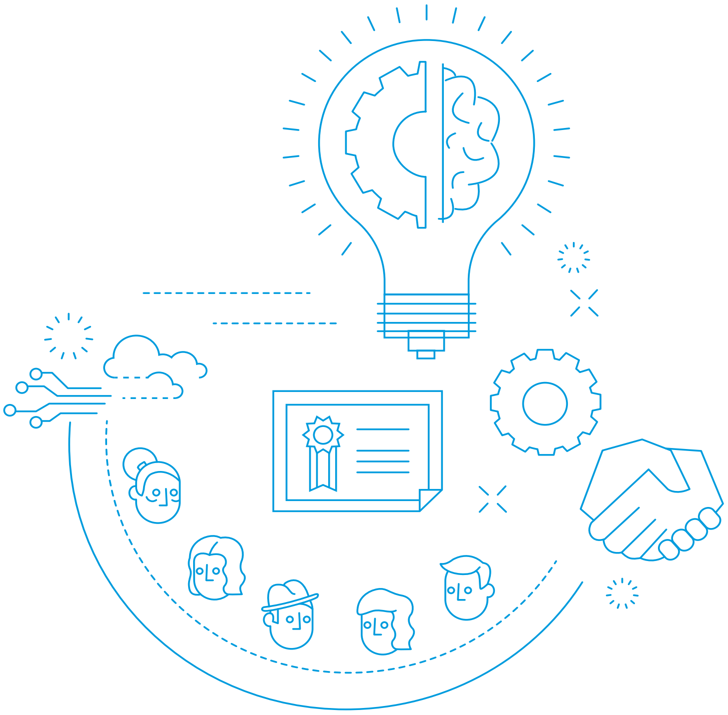
## Risk management deep dive

A ‘deep dive’ is an end-to-end review of a specific risk, priority, focus area or concern. Risk assessment deep dives are essential for gaining a better understanding of inhibitors and opportunities, thereby improving your risk management strategy and practices. They also provide an opportunity for organisations to understand the risk in more detail.

Key considerations include:

- being clear on the purpose and approach of the deep dive;
- making suitable preparations and focusing the deep dive on a strategic risk or matter;
- understanding and exploring the effectiveness of current risk management controls and planned actions and the basis of assurance;
- providing appropriate challenge; and
- documenting outcomes, actions to be taken, communication and follow-up.

To receive a copy of our risk management deep dive guidance, get in touch with your usual RSM contact.



## What can providers do to improve?

Risk registers need to be subject to regular review and have allocated owners for all risks and appropriate oversight. This ensures responsibility and, ultimately, that accountability measures are in place.

It's important that boards understand their risks and use the risk framework both to drive decision-making and to understand the assurances received. They must also know what this means for the risk profile. Adequate training should be provided to all relevant members of the board and staff so that risk is understood and managed effectively.

To ensure boards are exercising appropriate oversight, providers need to review and strengthen their risk management, internal control framework and assurance mechanisms. A risk appetite statement and risk management policy aligned to the framework should also be in place.

In addition to the risk management oversight and framework, key elements for every organisation are data integrity, data quality and management information. This means clear policies and procedures, and enhanced board reporting. Boards should drive awareness of the critical role that technology and data play in enhancing risk management.

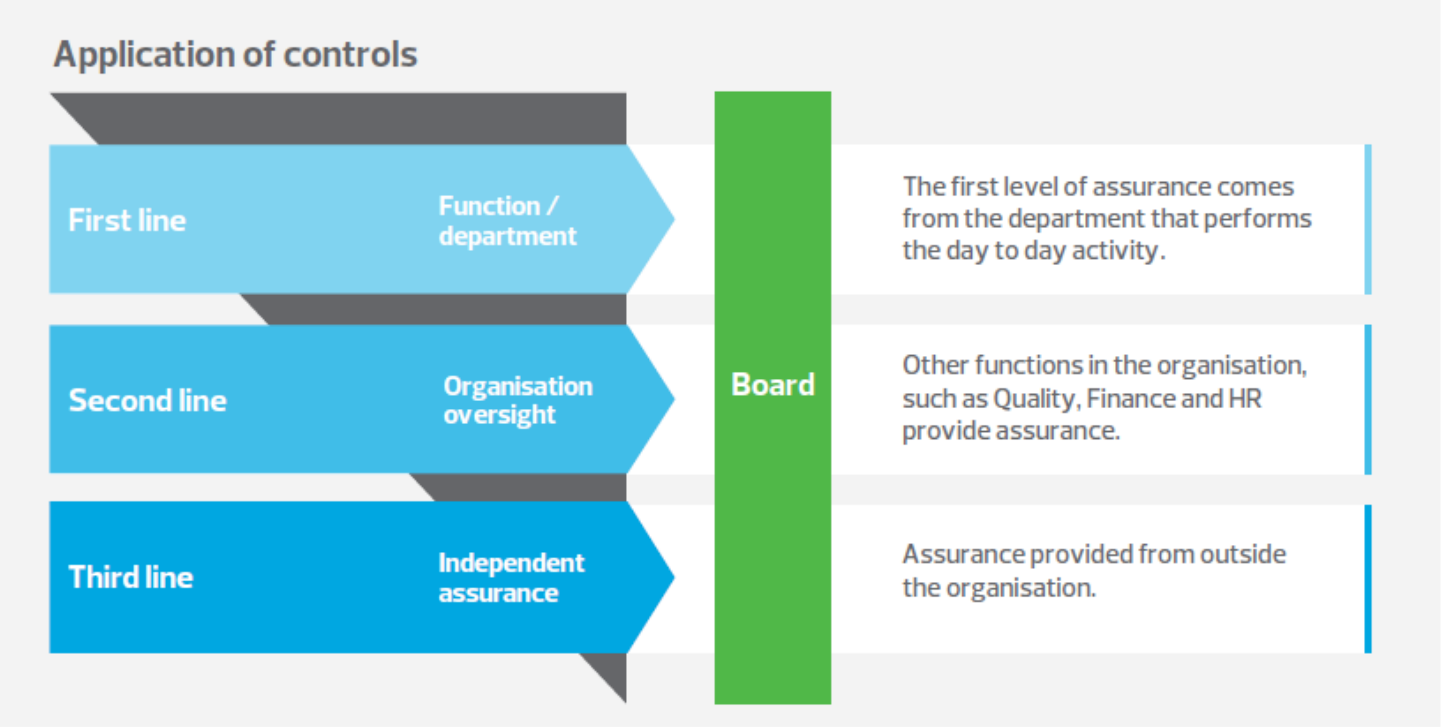
# Assurance mapping

Mapping your assurances is vital to effective risk management. An assurance mapping exercise helps to highlight anomalies in respect of the quantum of assurances so that, in effect, assurances are better aligned to ensure a good balance across all strategic risks.

Assurance mapping identifies and records the key sources of assurance that inform management and the audit committee on the effectiveness of how key risks are managed or mitigated. It also identifies the key controls/processes that are relied on in order to manage risk and achieve the service's objectives.

As with risk management, managing your assurances through the assurance map is an ongoing process. The assurance map, like your risk register, should be a document that is updated throughout the year, with the results being fed back into your risk management framework and understanding. To ensure that the process is useful, the frequency with which updates are required should be considered as part of setting your assurance policy but may also evolve over time with familiarity.

Assurance – first, second and third line – is vital in managing the key control environment, and mapping assurance will highlight any assurance gaps or indicate where current assurance provision may need strengthening.


Application of controls
First line
Function / department
Second line
Organisation oversight
Third line
Independent assurance
Board
The first level of assurance comes from the department that performs the day to day activity.
Other functions in the organisation, such as Quality, Finance and HR provide assurance.
Assurance provided from outside the organisation.

# Risk appetite

Risk appetite can be complicated to understand, a challenge to establish and difficult to apply, and, as a result, many boards give up.

However, the risk appetite conversation which explores the types of risks that an organisation is facing, is a healthy (and essential) boardroom discussion.

- What areas of risk do we want to engage with and potentially exploit?
- What areas of risk do we want to avoid?
- How much risk are we prepared to take in pursuit of our objectives?

If we understand this, we are in a better position to manage the risk. We can make better decisions, focus our monitoring and reporting and make better use of our assurance resources.

## INSIGHT4GRC

Insight4GRC (**www.insight4grc.com**) is RSM's proprietary digital governance, risk and compliance solution.

We have over 300 organisations from all sectors that license and use one, some or all of the Insight4GRC modules, which are 4risk, 4action, 4policies and 4questionnaires. Insight4GRC provides management with real-time information in connection with the identification, assessment and management of risks, the communication and acceptance of policies, and the distribution and tracking of actions.

To find out how Insight4GRC can help you better manage your organisational risks, contact **matthew.humphrey@rsmuk.com.**

SCAN ME

# Key contacts

### Lisa Randall
Head of Higher Education
lisa.randall@rsmuk.com

### Louise Tweedie
Risk Assurance
louise.tweedie@rsmuk.com

### Donna Clark
Senior HR Consultant
donna.clark@rsmuk.com

### David Gibbens
Associate Director, HR
david.gibbens@rsmuk.com

### Lucy Robson
Partner, External Audit
lucy.robson@rsmuk.com

### Matthew Humphrey
Partner, Insight4GRC
mathew.humphrey@rsmuk.com

### Steven Snaith
Partner, Technology Risk Assurance
steven.snaith@rsmuk.com

### Research
Risk Assurance Technical
technical.ra@rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Corporate Finance LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are licensed by the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM UK Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.