RSM'S ANALYSIS OF EMERGENCY SERVICES RISK REGISTERS 2023

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

CONTENTS

Challenge your risk profile and appetite and actively manage relevant risks and identify areas of opportunity.

EXECUTIVE SUMMARY

For the emergency services, the risk landscape is complex and evolving. Therefore, identifying and managing your risks effectively is vital.

Moving out of the uncertainty caused by the pandemic and the challenges this presented remains a feature of the operating environment. The cost-of-living crisis, rising energy, food and material prices, inflation and geopolitics are all part of the wider risk management landscape. We have also seen a greater focus on climate change, equality and diversity, mental health and wellbeing that form part of the wider environmental, social and governance (ESG) agenda. His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) has noted that within the police and fire services, some cultural change is necessary, linked to police officer behaviour and abuse of position, and promoting equality, diversity and inclusion in the fire service profession.

Persistent challenges around the inability to plan financially for the longer term remain (this is linked to the national funding formula). This is magnified as budgets are stretched and, despite government reviews, there is some uncertainty regarding how government may take forward key proposals. While the risk of fire fighter strikes has been abated in the short term, this has the potential to remain an issue.

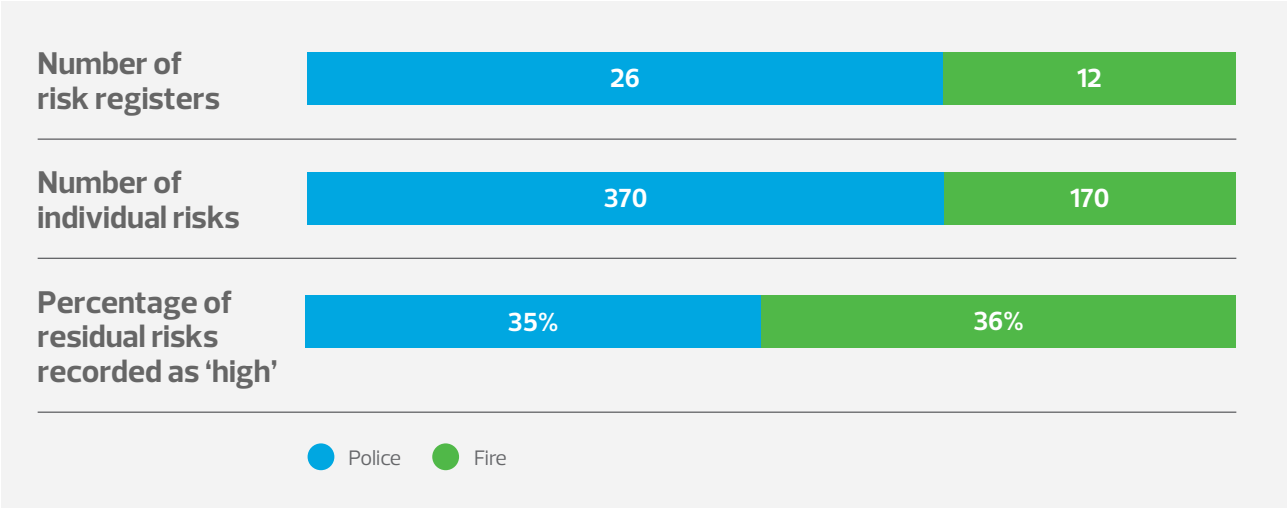
Cybercrime is another continuing threat and communications related issues remain, linked to delays in the emergency services mobile communications programme, which also has a significant cost. It is, therefore, critical that boards and management continue to focus on ensuring they have effective risk management procedures in place and that these are robustly and consistently implemented.

We have been publishing analyses of police and fire risk registers periodically for eight years now, allowing us to trace movement in risk profiles over time. This publication is our first cross-sector analysis, reviewing police force, office of police and crime commissioner (OPCC), office of police and fire crime commissioner (OPFCC) and fire service strategic risk registers. It allows emergency services organisations to consider how our risks compare and to assess whether we are missing any significant risks.

While the best risk management can never negate the potential for a risk to materialise, ensuring that risk is understood and managed effectively, efficiently and proportionately helps. Organisations should ensure that risk profiles and descriptions remain current, that robust internal controls are mapped to each risk and are in line with risk appetite, and that appropriate assurances are sought. This will allow audit committees and senior management to take comfort in the knowledge that controls to manage and mitigate risks are operating as intended and informing the board assurance framework where this is in place. This is particularly important where services are collaborated and/or involve third-party providers.

HIGH LEVEL OVERVIEW OF STRATEGIC RISKS

In seeking to understand the key risks faced by our emergency services clients, we examined the contents of 38 emergency services' strategic risk registers. 540 individual risks were analysed from across police and fire services.



Risks across emergency services

As part of our analysis, we have categorised each strategic risk by key theme to understand those areas of greatest concern to police and fire services.

In terms of **quantities** of risks, the top three areas representing 48% of the total population were:

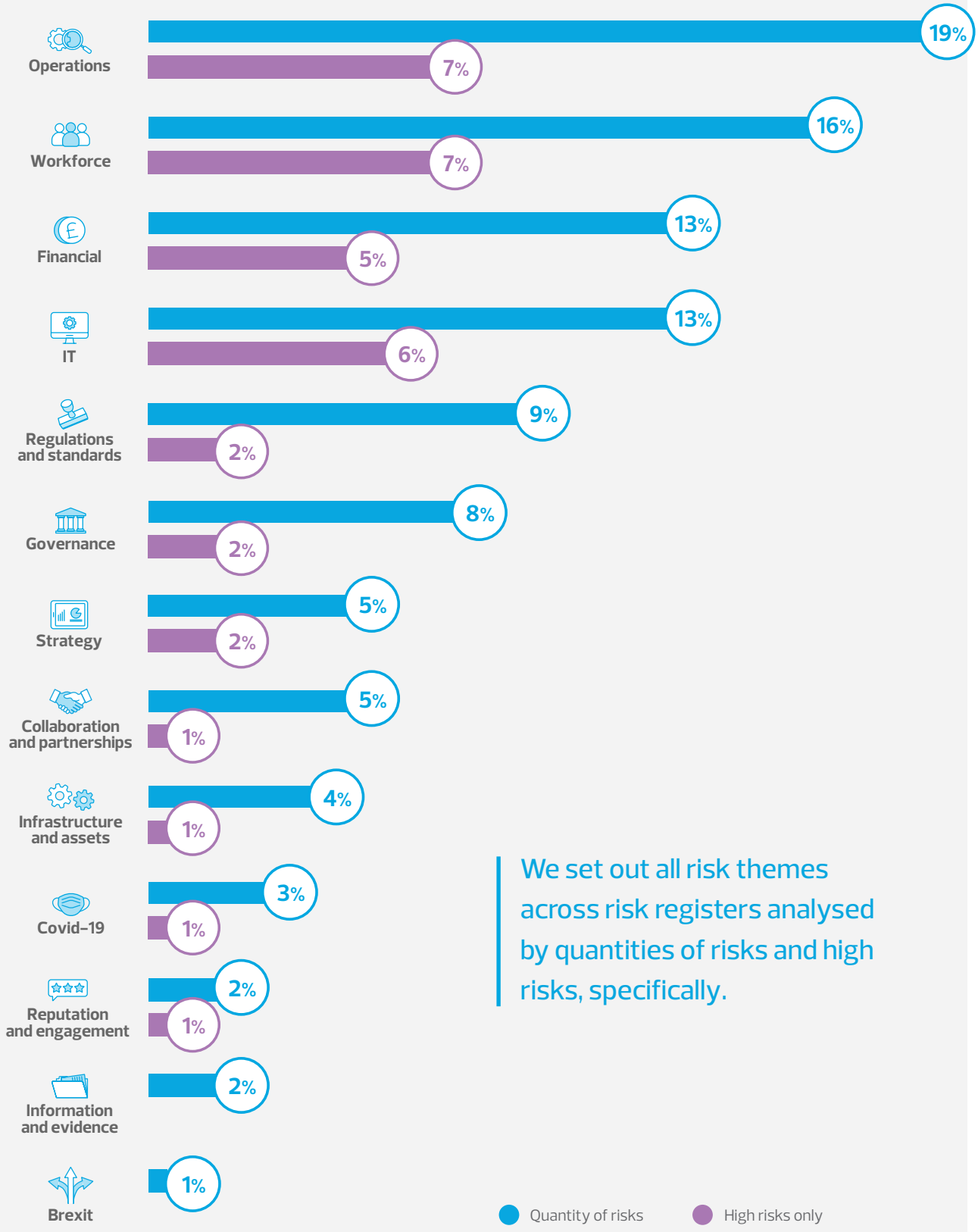
1	**operational** risks, accounting for 102 risks in total (or 19%)
2	**workforce** risks, accounting for 87 risks in total (or 16%)
3	**financial** risks, accounting for 70 risks in total (or 13%)

As part of our analysis, we have analysed strategic risks in terms of **severity**, tracing those residual risks (post controls and applied mitigations) considered by police and fire services to be '**high**'.

Overall, 187 (or 35%) of risks across the risk registers in our sample were deemed to be 'high'. The top three areas representing 20% of all 'high' risks recorded were:

1	**operational** risks, accounting for 38 high risks (or 7%);
2	**workforce** risks, accounting for 37 high risks (or 7%); and
3	**IT** risks, accounting for 32 high risks (or 6%).

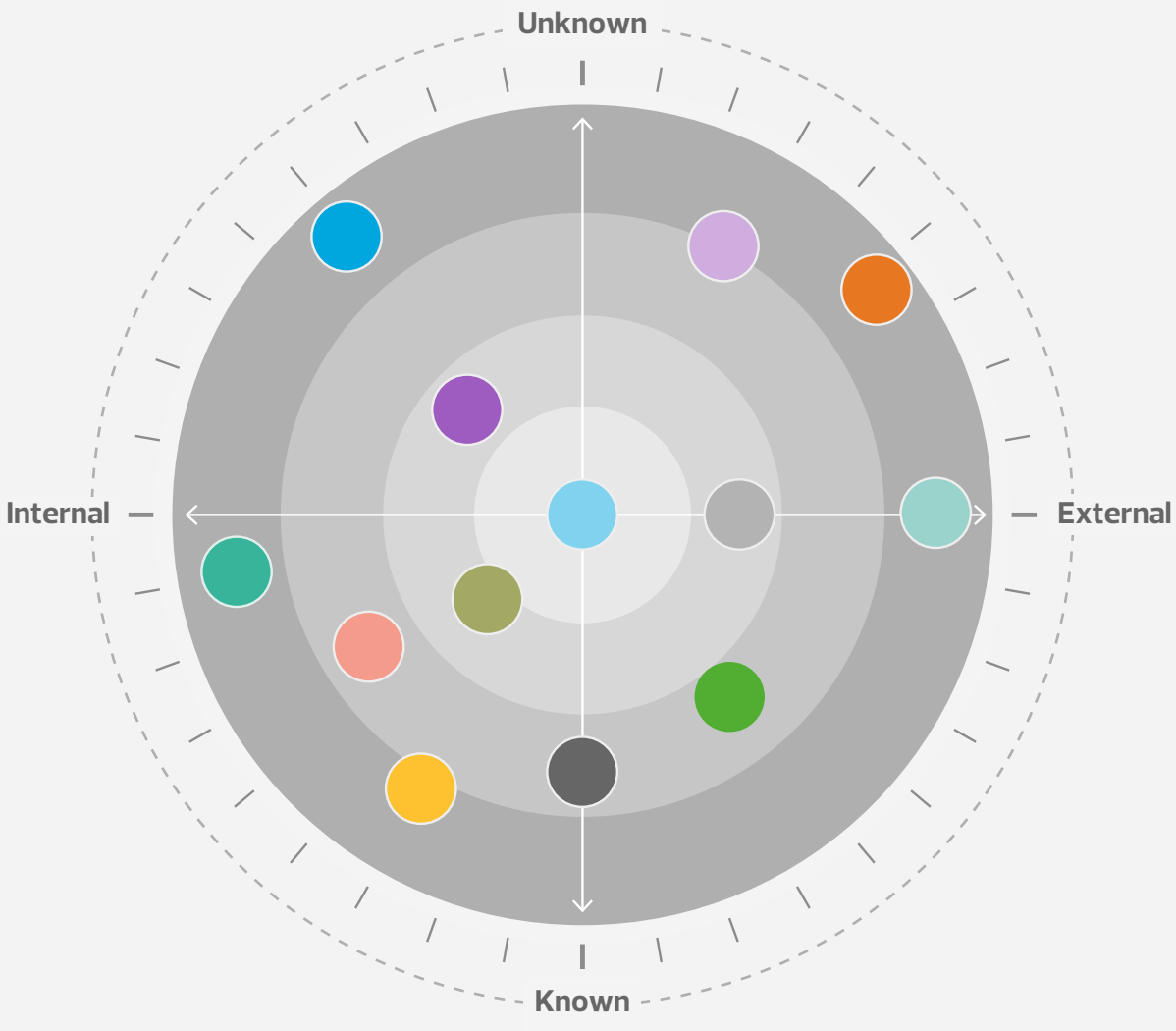
Across emergency services, risks relating to core operations and the workforce are paramount and are clearly on the radar as being intrinsically important areas of focus. While financial risks fell out of the top three high-risk areas, they did feature at number four, representing 5% of all high risks in total.



We set out all risk themes across risk registers analysed by quantities of risks and high risks, specifically.

Risk radar

Using our radar, we plot where each of the 'high' risks recorded within the strategic risk registers sit. The closer the area is to the centre of the radar, the greater the risk score. We also identify each risk area in terms of whether risks are known, and whether they are internal or external.



Key observations

- Operations related risks sit directly at the centre, featuring more high risks than any other area. They relate to risks that are both known and unknown, and while in many respects are focused on service delivery to the public, they link to internal processes and systems operating effectively.
- Workforce-related risks were internal, with there being an awareness of the issues faced by the organisation.
- Regulations and standards related risks are also clear, having been set by external bodies, yet reputational risks were less understood, with links to public perception and satisfaction.
- Many of the finance risks relate to funding. While annual funding allocations are known, longer term financial planning can be more challenging as a consequence of the funding model.
- A cybercrime attack could happen at any time, and we have seen continued risks in this area. There also remains uncertainty in relation to the emergency services mobile communications system.
- While there was little mention of culture, weaved within some police risk registers were risks relating to officer behaviour and abuse of position and how this ultimately threatens force legitimacy and the erosion of public trust and reputation.

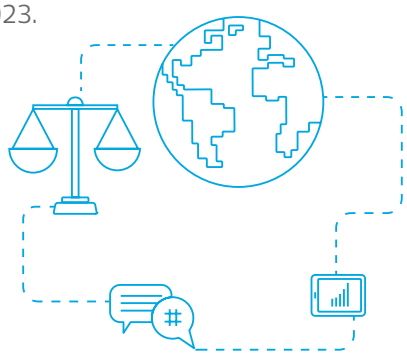
Trending risks analysed by sub-sector

In our latest analysis, across emergency services there are more risks related to operations and workforce than any other. This demonstrates that, in many respects, the broad risk themes across the sector are similar in nature, despite the distinct roles of forces and commissioners, and fire and rescue services.

As we have been analysing police and fire strategic risk registers for several years, we can illustrate risk movement and trends.

POLICE

- The number of operations related risks continues to account for more risks than any other, with the percentage growing from 13% in 2021 to 19% in 2023.
- The number of workforce risks has increased from 12% in 2021 to 14% in 2023.
- At 13%, IT-related risks have increased by two percentage points since 2021.
- In terms of high risks specifically, finance risks have reduced by two percentage points since our analysis in 2021 and are no longer the top area of high risk for the police service. The top high-risk areas for the police service are now operations and IT.
- IT risks have increased from 11% of all police high risks in 2021 to 18% of all police high risks in 2023.
- The number of Covid-19 related risks has fallen significantly, from 12% of all risks in 2021 to 3.5% of risks in 2023.

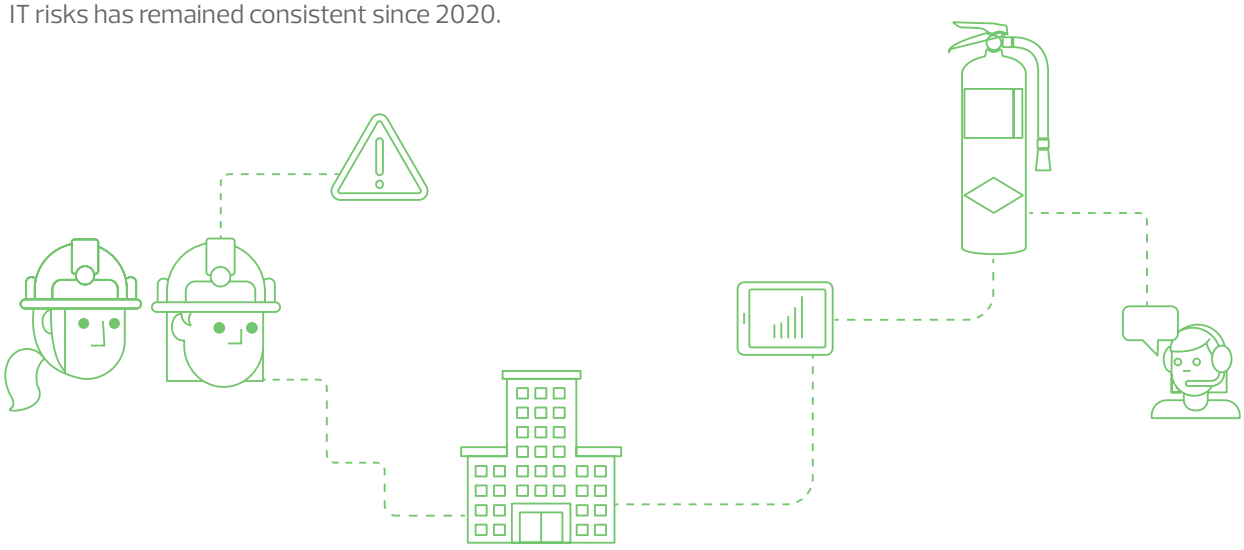


DIRECTION OF TRAVEL – TOP FIVE RISKS IN 2023, 2021 AND 2018 (NUMBER OF RISKS)

		2023	2021	2018
1	→	Operations	Operations	Financial
2	↑	Workforce	Covid-19	IT
3	↑	IT	Financial	Operations
4	↓	Financial	Workforce	Collaboration and partnerships
5	↑	Governance	IT	Regulation and standards

FIRE

- At 21%, there has been a five-percentage point increase in the number of workforce-related risks across the fire service since our last analysis in 2020.
- In a similar pattern, workforce risks have also significantly increased in terms of severity. In our last analysis, just 7% of workforce risks were high; in our latest analysis this has increased to 31%.
- The number of finance-related risks has increased by 2% (from 12% to 14%), while the number of IT risks has remained consistent since 2020.
- Risks relating to Covid-19, which were all-encompassing at the height of the pandemic, have reduced significantly across the fire service, from 16% in 2020 to 3% in 2023.
- We have continued to see collaboration and transformation risks outside of the top five risk areas, despite increased focus on this with the Policing and Crime Act 2017.



DIRECTION OF TRAVEL – TOP FIVE RISKS IN 2023, 2021 AND 2018 (NUMBER OF RISKS)

		2023	2021	2018
1	↑	Workforce	External environment and Covid-19	Workforce
2	↑	Operations	Workforce	Financial
3	↑	Financial	Operations	Operations
4	↑	Regulation and standards	Financial	Legislation (Regulation and standards)
5	→	IT	IT	Collaboration and transformation

NEW AND EVOLVING RISKS

Below, we set out some of the key areas across emergency services where we consider risks to be emerging or evolving.

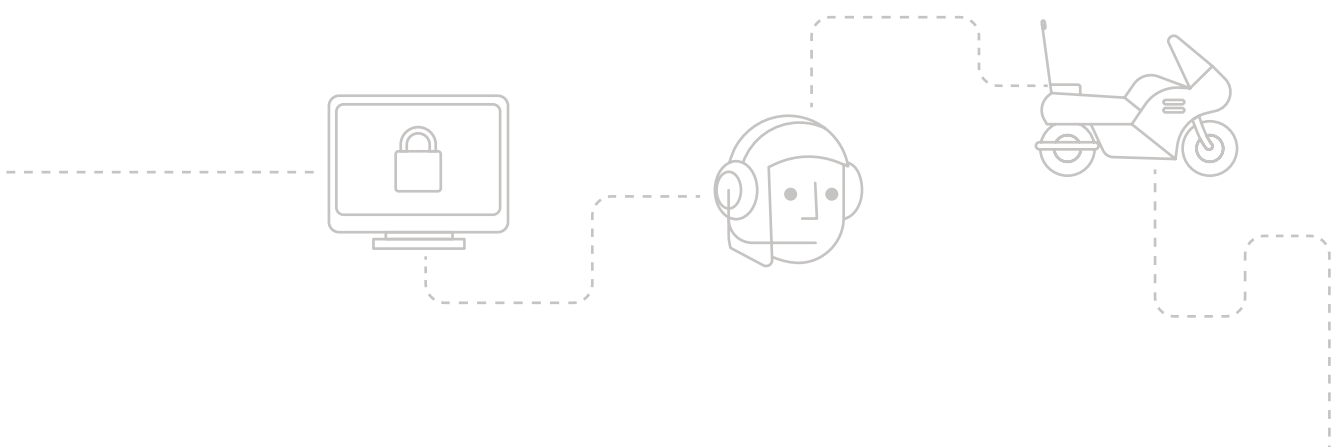
Economic Environment

Economic uncertainty (linked to significant cost pressures), inflation and having to pay more for goods and services are all evolving risks. Greater focus on medium-term financial plans will be needed and capital projects may need to be reconsidered as the costs of borrowing have increased.

Public Procurement

New UK Public Procurement Legislation will be effective, starting from late 2023/early 2024 and will fundamentally change the way all public procurement is conducted. The new legislation will replace the Public Contracts Regulations 2015; the Utilities Contracts Regulations 2016; the Concession Contracts Regulations 2016; and the Defence and Security Public Contracts Regulations 2011. The new bill repeals these regulations and introduces a single framework.

The scale of change to the public procurement regime will be significant and far-reaching. The changes will apply to all public sector bodies, including local authorities and central government departments. The impact will also be significant for all companies and others who sell goods and services to the public sector. Everyone involved will need time to prepare themselves to function effectively under the new regime. If you are a public sector buyer or a seller to government, all procurement-related governance, processes and control will need to be updated. Management and staff will need training and new guidance will need to be written.



Environmental, Social and Governance (ESG)

ESG will continue to evolve. Equality and diversity strategies, equal pay, ethical investments, and sustainability are just some areas where services will need to do more in terms of their investment of time, resource and response, to what is an increasingly important area of focus.

Cybercrime

IT and cybercrime risks will continue to evolve in their complexity, highlighting the need for network and secure configuration controls that are tested routinely, while continuing to raise staff awareness and undertake training.

Tax

The trend continues for legislation and HMRC to focus on tax risk governance, with a greater onus on larger organisations to help enforce compliance across their supply chains. For example, powers under the Criminal Finance Act 2017 for the offence of failing to prevent tax evasion are being used more frequently by HMRC. This is especially so where HMRC suspects tax leakage in a supply chain and where an organisation does not have suitable processes in place to have helped identify potential evasion by a third party or workers. Commonly, risks are an over-reliance for tax on any one individual, a lack of written procedures and a lack of suitable customer/supplier checks.

Human Capital, Diversity and Talent Management

In its 2023 Risk in Focus report, the Institute of Internal Auditors (IIA) noted that 50% of survey respondents cited human capital, diversity and talent management as a top five risk. Related risks have arguably intensified in this area. The government has reached its target of recruiting 20,000 additional police officers, yet the profile of the workforce is changing. This is an issue spanning the emergency services, as experienced officers and firefighters are reaching retirement, resulting in the loss of key knowledge and skills.

Recruiting people with the skills and technical abilities required is challenging and can be linked to several factors, including pay and reward. The latter is a particular issue for the fire service, with the threat of strike action as a result of reduced pay and failing to fill open posts. There is also a much greater focus on wellbeing.

Culture

Organisational culture is in the spotlight and receiving greater focus. In its latest annual assessment of fire services, HMICFRS stated that 'many services need to improve how they promote their values and culture', while in its annual assessment of policing, HMICFRS noted recent reports 'have contained highly alarming evidence of toxic behaviour and attitudes among some police officers.' To bring about change, internal processes, policies and strategies should align with values that can drive cultural change where this is needed.

ESG and how RSM can help

We all have a responsibility to make the world and our environment a better place. The responsibility for taking tangible action extends to public and third-sector organisations, and we are seeing regulators take a much deeper interest in ESG matters than ever before. While organisations will likely talk about ESG, and perhaps develop associated strategies, plans, commitments and targets, we are clearly all on a journey.

To help organisations understand where they are on their ESG journey, RSM has developed an ESG maturity assessment. To complement the framework assessment, RSM can also undertake an ESG appetite review.

Read RSM's The Real Economy ESG.

Emerging risks

At RSM, we monitor emerging risks across various sectors, highlighting board member views on emerging events or threats that could impact businesses either negatively or positively.

For a copy of our latest Emerging Risk Radar, please get in touch with your RSM contact.

RISKS IN FOCUS

Operations

Key operations related risks by sub-sector.

POLICE

- Forces fail in their remit to protect the public, business organisations and vulnerable people, and fail to reduce violence against women and girls.
- Risks that demand will overwhelm capacity and capability to efficiently and effectively deal with crime.
- Failing to increase police visibility and public confidence across the local community.

FIRE

- Demographic changes, such as an ageing population or younger people moving out of small urban areas, change the demand for fire services.
- As people respond to the cost-of-living rises, there may be a linked increase in primary and secondary fires.
- On-call availability does not align with incident call demand peaks.

Emergency services should be focused on prevention, protecting the community and incident response. This links to effective community engagement and ensuring there are sufficient officers and firefighters to meet the demands placed on them. Operationally, the sector is facing some notable challenges.

Online crime is now the most prevalent type of crime, with online fraud having increased. For forces, there are also concerns that hidden and complex crimes, such as child exploitation and human trafficking, create significant challenges, while for some crimes there is a risk that forces are seen to be not doing enough in their response. For example, youth-related gun and knife crime continues to be a key area where focus is required, along with other crime-related areas, including violence against women and girls. We have seen risks that note that the legitimacy of the force may be questioned should it fail to ensure the right balance between effective and ethical policing.

The police service has made some notable improvements in several areas, such as child protection and crime recording, however, HMICFRS notes in its annual assessment of policing in England and Wales 2021 that there are 'unacceptably wide inconsistencies in performance between police forces' and that 'detection rates in some crime types are very low and have deteriorated.'

Due to changing incident types and fewer calls than in previous years, for some fire services, there is a risk that operational competence is not sustained, especially in stations with low call demand. In England, the latest data reveals that the average response time to primary fires was 8 minutes and 50 seconds, which was an increase of 15 seconds on the response times for the year ending March 2021. Despite these numbers, we know the sector is well-prepared to deal with routine emergency responses and major incidents. At a national level, the number of incidents attended by fire services has increased by 16% in the year ending September 2022 and fire incidents have increased by 28% from 145,313 to 185,437.

While fire services must focus on aligning their on-call capability to meet changing local requirements, HMICFRS noted in its 2021 annual assessment that 'too many services aren't taking enough action on prevention' while in its 2022 annual assessment, the inspectorate noted that fire prevention was 'an area in which almost half of services need to significantly improve if they are to keep their communities safe'.

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Are you satisfied with the data being reported through your organisation and action **plans in place to improve performance?**

Is training aligned to the different **demands being placed on the service?**

Do you carry out deep-dive reviews into **key operational risks at your audit committee or joint audit committee meetings?**

Does your chief officer team and audit committee receive regular **reports/assurance that HMICFRS recommendations are being addressed?**

Workforce

Key workforce related risks by sub-sector.

POLICE

- Forces experience high attrition rates, losing key experience when crimes rise in complexity.
- Linked to the availability of staff, serious crimes may not be investigated by trained detectives, impacting negatively on support to victims.
- Police officer uplift programme, while increasing police numbers, creates additional pressure for forces, including back-office functions.

FIRE

- Service fails to achieve a positive, safe and inclusive culture.
- As a result of a lack of investment, the service fails to develop and manage its people effectively.
- Linked to pay negotiations, there was a risk of industrial action, which in the short term has been abated.

Many of the workforce-related risks focus on the potential lack of people resource, which impact on the ability to deliver core operational objectives. The risks also focus on a failure to recruit and retain suitably skilled people and ensure effective succession planning.

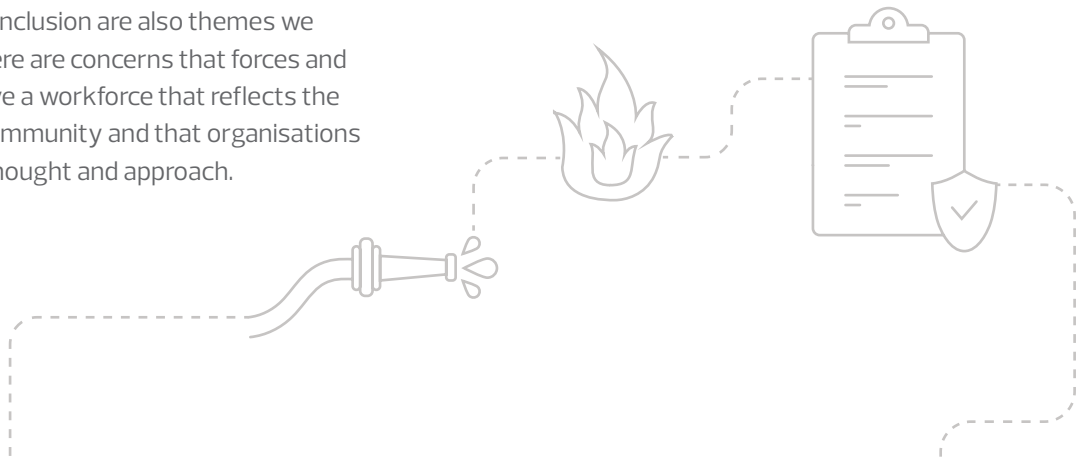
Linked to recruitment, we would have anticipated seeing more risks in relation to vetting. In some areas, the police have been working hard to rebuild public trust and confidence after internal processes failed to protect members of the public from corrupt serving police officers. Where not done so already, forces should review the 43 recommendations made by HMICFRS in its inspection of vetting, misconduct, and misogyny in the police service.

In risk registers across the sector, we are also seeing more risks in relation to mental health and employee wellbeing, where both the police and fire services understand the need to prioritise their people's health.

Equality, diversity and inclusion are also themes we are seeing more of. There are concerns that forces and fire services do not have a workforce that reflects the diversity of the local community and that organisations may lack diversity of thought and approach.

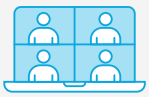
As part of the Police Uplift Programme, the government has achieved its target of recruiting 20,000 additional police officers by March 2023, and at 53,083, female officers make up 35.5% of officers in post, the highest percentage since records began. While still disproportionally low, many forces have successfully recruited more officers who identify as Black, Asian or other minority ethnic groups.

The Reforming our Fire and Rescue Service white paper consultation (which closed in July 2022) also articulated plans to 'clarify the role of fire and rescue services and of the firefighter, unlock talent and improve diversity within services, take action to ensure that we are supporting the creation of a positive culture, and further develop schemes to consistently identify and nurture talent.'



Workforce challenges

The pandemic has produced some key learning points for organisations. As we move forward, there are some significant areas for emergency services providers to consider.



Ways of working

This includes hybrid, remote or flexible working, as they are not all the same. Consider hybrid working approaches and a mixture of different skill sets so that operational delivery across the emergency services sector is effective.

Culture, leadership and engagement

Fostering a good sense of belonging and ensuring good leadership where there are new ways of working.

Global war for talent

How to attract and retain the employees you need. Linked to this, are the wider equality and diversity agenda and transparency in pay.

Equality, diversity and inclusion

Ensure that diversity and inclusion continue to underpin ways of working.

Individualisation and humanisation of management

One size doesn't fit all. Every employee has their own desires for flexibility, progression and development, as well as their own sense of wellbeing.

Burnout

Keep focusing on the wellbeing of staff so that everyone can achieve the future they're working towards.

Read The Real Economy: The Modern Workforce.

Access further information on our HR services, how we can provide advice, and operational support and our Employment legal services.

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Do you provide timely and sufficient support to staff regarding **mental health and wellbeing?**

Do you understand the levels of job satisfaction and morale of your workforce, and have related **initiatives been implemented?**

Is there scope to enhance your recruitment strategies and initiatives, to better **demonstrate your value and to attract talent?**

Is your culture aligned with organisational values, strategy and processes and, where needed, **how are cultural changes communicated to enable change?**

Financial

Key finance related risks by sub-sector.

POLICE

- Risk of reduction in government funding or that government funding is insufficient to enable effective policing.
- Potential impacts of changes to the policing funding formula, while one-year spending settlements impact longer term financial planning.
- Pensions and pension liabilities arising from the McCloud judgement.

FIRE

- That government grant funding for specific programmes is not extended or renewed, impacting service delivery and the ability to meet new legislative requirements.
- For contracts in place, there is no assurance that value for money is being achieved.
- The service falls victim to financial crime or fraud leading to financial losses.

Financial risks feature significantly and routinely within strategic risk registers. This is no exception in our latest analysis, with finance risks making up 13% of all risks. There are concerns that financial planning and forecasting are not robust and operating and spending costs are not controlled.

There are also risks that services have insufficient financial resources to enable them to fulfil their remit adequately and maintain financial sustainability. While budgets for 2022/23 may have increased and additional funding may have been granted for national initiatives and programmes, there are concerns that the costs outweigh the funding awarded. The key is strong financial planning, yet there are fears that amidst the rising costs of living and inflationary pressures, budgets will be impacted with the possibility of increased savings requirements stipulated by government. There is also the risk that Brexit, the war in Ukraine, the fuel crisis and Coronavirus recovery will not only lead to supply delays but increased costs, too.

Government spending is likely to be tightened with a greater focus on achieving efficiency savings. In an unpredictable financial environment, achieving value for money and projected cost savings is increasingly important.

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Is your budgeting process sufficiently robust? Have your underlying financial planning and budgeting assumptions been considered, with appropriate challenge from both management and board?

To understand your financial resilience, do you reforecast cashflow frequently? Does this incorporate scenario planning and sensitivity analysis?

Do you undertake detailed sensitivity analysis as part of your yearly budget setting and for medium-term financial plans?

Do you combine financial and non-financial data in a dashboard to more easily identify trends and anomalies, using **meaningful KPIs aligned to financial objectives?**

Fraud risks and how we can help

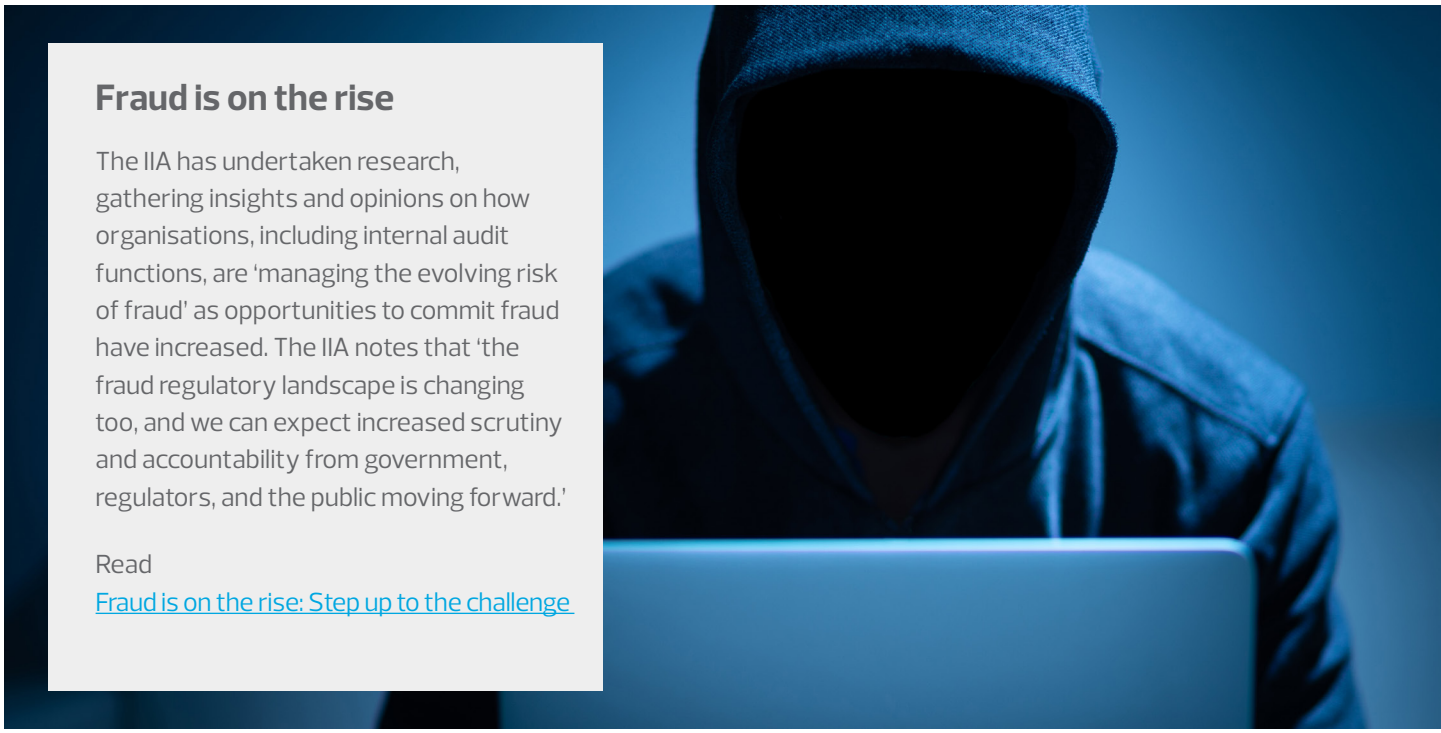
During the pandemic, we saw an increase in electronic/remote authorisations. These have continued as remote working for some back-office functions has become a permanent feature. However, they now provide greater opportunity for fraudsters to exploit this change successfully. While the financial losses can be significant, there are also associated reputational impacts. Below, we highlight some of those key considerations to ensure fraud risks are adequately managed.

Ensure staff understand what fraud and bribery are, their associated responsibilities, and how fraud offences might present themselves within the operating environment. The introduction of a fraud awareness strategy that is inclusive of training, as well as workshop events, can assist in achieving this.

Ensure the fraud policy is supported by a fraud response plan, which can be deployed by those charged with undertaking investigations when needed. The fraud policy can be reviewed by a counter fraud specialist to ensure it is appropriate and fit for purpose.

You should complete a Fraud Risk Assessment (FRA) to understand which processes, systems and even particular personnel are most at risk of fraud or bribery.

Ensure the policy is appropriately communicated to staff, delivery partners, suppliers and other key stakeholders.



Fraud is on the rise

The IIA has undertaken research, gathering insights and opinions on how organisations, including internal audit functions, are 'managing the evolving risk of fraud' as opportunities to commit fraud have increased. The IIA notes that 'the fraud regulatory landscape is changing too, and we can expect increased scrutiny and accountability from government, regulators, and the public moving forward.'

Read
Fraud is on the rise: Step up to the challenge

IT

Key IT-related risks by sub-sector.

POLICE

- The force does not effectively use technology to its potential and fails to realise the possible benefits of digital solutions, which impacts upon delivery.
- Ongoing delays to the Emergency Services Mobile Communications Programme (ESMCP) result in significant additional costs to forces and negatively impacts operational policing.
- A cyber-attack occurs, resulting in a loss of system access, possible loss of data and impacts service delivery.

FIRE

- There may be insufficient resource to upgrade and improve the ICT infrastructure and use of unsupported technology leaves the service vulnerable.
- Delays continue on the ESMCP and services are not given sufficient time to complete required actions linked to cutover target dates.
- An outsourced third-party service provider is entrusted with data, which is subsequently lost, compromised or becomes inaccessible.

13% of all risks across the risk registers in our sample were IT-related. A significant proportion of those IT risks related to cybercrime. Risks focused on:

- systems being hacked, leading to significant data and financial losses and resulting in reputational damage;
- ransomware or denial of service attacks occur creating disruption and loss of data, while phishing emails continue to entice staff; and
- there are poor access controls in place, allowing unauthorised individuals to have access to systems.

As an increasing number of processes and systems are digitalised, more opportunities are created for cyber criminals. The same types of attacks that have been used for the last decade – phishing, business takeover threats and ransomware – are still commonly used, but they are growing in effectiveness, speed and sophistication.

More recently, reported cyber incidents relate to the human element of cyber risk, where the act of clicking on a seemingly harmless link 'opened the door' for malicious software to infect systems, resulting in data loss.

Therefore, the need for regular cyber risk awareness training, together with robust incident response plans, is crucial in helping to both reduce the propensity of such issues occurring and recovering quickly if a cyber incident arises.

Moreover, the relatively recent BS 31111 Cyber Resilience standard sets out a range of cyber governance requirements that is very applicable for the sector. It provides further guidance regarding the development and maintenance of robust cyber control environments.

Other IT risks in the risk registers reviewed include:

- there is a major IT outage or failure of key systems, creating operational challenges, impacting services to the public and potentially resulting in a data breach; and
- there is a lack of investment in IT and that the IT infrastructure does not meet the needs of the service.

Security testing services to help you understand your security posture and combat cyber threats

Security testing is a critical component of your organisation's cyber security strategy. To assess the effectiveness of your cyber security and your ability to combat cyber threats, you need:

- **proper penetration testing;**
- **threat modelling; and**
- **security training and awareness.**

For more information, please visit the RSM website – Security testing services to help you understand your security posture and combat cyber threats | RSM UK

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

How are you identifying your cyber security risks and are your network **controls and configurations keeping cyber criminals at bay?**

Has your IT department developed and implemented a **framework to ensure the security of your systems?**

Is the force aware of and understanding of the implications of the use of **new technology and potential criminality around this?** For example, facial recognition, automated vehicles and the use of 3D printers for firearms.

Have you undertaken penetration testing to provide independent **assurance that your cyber /IT defences are effective?**

IT access controls good practice examples

- Rename or disable access to the default built-in administrator account as this account will often be the primary target for security breach attacks.
- Implement a lockout threshold of five attempts.
- Review 'password history' controls, preventing individuals from using the same passwords, frequently.
- Establish Multi Factor Authentication (MFA), as without MFA there is an increased risk of accounts being compromised.
- Strong password policy configurations should be in place.
- Undertake periodic reviews of privileged user access accounts.
- Disable the 'store passwords using reversible encryption' option, as this allows the operating system to store passwords in plain text format that can weaken overall security.
- Undertake periodic reconciliations of active staff against user accounts and review inactivity reports, ensuring inactive accounts are disabled.

Regulations and standards

Key regulations and standards related risks by sub-sector.

POLICE

- That official enquiries identify issues for forces, which require corrective action and result in a loss of public confidence, or that officer behaviour/conduct does not align with expectations.
- Police National Database (PND) audits are not being undertaken and the service fails to address issues raised in HMICFRS inspection reports.
- Legislative changes expand the role and remit of PCCs, creating significant pressures on staff and work streams.

FIRE

- Response and rescue performance targets are not achieved and there is a failure to adopt National Operational Guidance policies and procedures.
- There may be a lack of awareness or adherence to health and safety legislation linked, for example, to asbestos and legionella. This may lead to the injury or death of an employee or to prosecution or compensation claims.
- Failure to ensure there are adequate resources in place to meet the requirements of new fire safety and building legislation, in light of the Grenfell Tower tragedy.

Failure to comply with laws and regulations can have severe ramifications, including financial penalties, regulator sanctions and reputational damage. There are, of course, many statutory requirements in place for emergency services, and there are risks recorded regarding a failure to adhere to legislation relating to safeguarding and the Equalities Act, specifically. There are also concerns that the organisation fails to comply and meet the requirements of the General Data Protection Regulation (GDPR)/ Data Protection Act and for the police, there is a risk of fines from non-compliance with subject access requests or court order disclosures.

The Strategic Review of Policing in England and Wales, chaired by Sir Michael Barber and carried out by the Police Foundation, included 56 recommendations 'urging radical reform to police culture, skills and training and organisational structure.' Within the risk registers in our analysis, there is acknowledgement of the challenges linked to systemic issues of racism and sexism but there was little mention of culture. Where a cultural shift is needed, leaders must drive change and lead by example. Internal processes, policies and procedures relating, for example, to vetting and disciplinary, as well as reporting, communication and training, are all essential.

The government has undertaken a two-part review of the role of PCCs[1], with the aim of making PCCs more accountable to their local communities and strengthening the relationship with the force chief constable. With the goal of raising professional standards and increasing transparency, the specified information order would be amended. Yet, within the risk registers, we have seen concerns regarding how these measures will be implemented by the Home Office, and whether the OPCC may require more resource to meet new or changing requirements.

Health and safety is a significant risk area for the emergency services. The stark findings of the Fire Brigades Union commissioned research undertaken by the University of Central Lancashire (UCLan) revealed that 'firefighters' mortality rate from all cancers is 1.6 times higher than the general population.'

[1] *The government review applied to all PCCs including PFCCs. Within this paper, where we refer to PCCs this also incorporates PFCCs.*

This finding highlights the very real risks associated with firefighting and will focus the service on taking measures that reduce, as much as possible, exposure to fire contaminants.

The Fire Safety (England) Regulations 2022 and the Fire Safety Act 2021 form a key part of a series of changes to fire and building safety that the government is making, following the Grenfell Tower fire in 2017. This means that building owners or managers in multi-occupied residential buildings must include an assessment of risk related to fire and take precautions to reduce the risk of fire spreading regarding these parts of the relevant premises. As a result, fire and rescue authorities have the relevant enforcement powers to hold owners or managers to account.

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Have you identified all relevant legislation and are relevant individuals in the organisation **clear about their responsibilities?**

Are all regulatory breaches treated as serious, logged and where required, reported?

In making use of new technologies and artificial intelligence, are you confident that how you **collect and use data, complies with the GDPR?**

Are you confident that you have the **right mandatory and advisory training programmes in place** that cover all health and safety related training, and are compliance levels communicated to chief officers regularly?

Governance

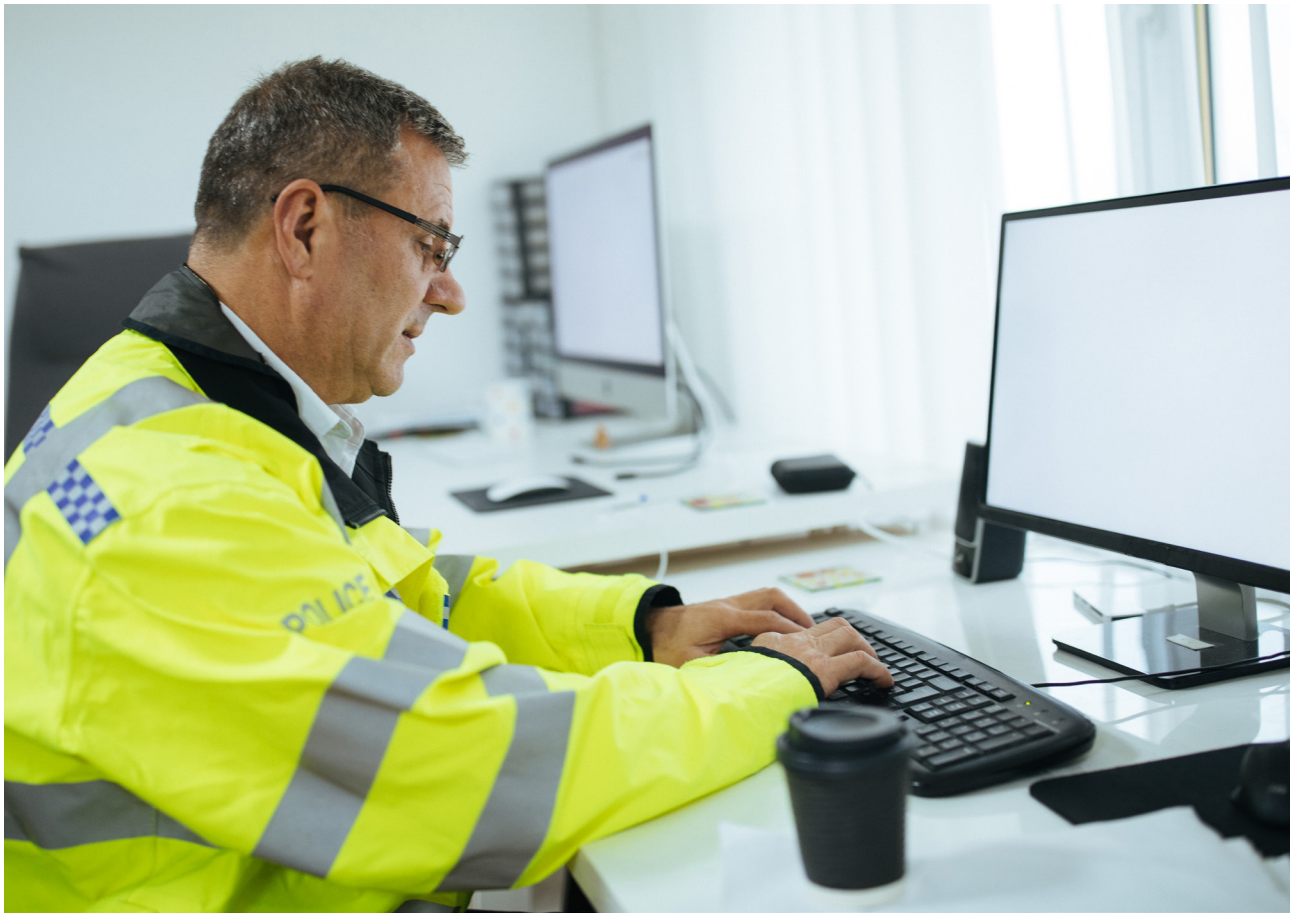
Key governance related risks by sub-sector.

POLICE

- The PCC fails to hold the chief constable accountable for the delivery of an effective and efficient policing service.
- The PCC fails to comply with good governance principles, aligning with best practice and complying with the Code of Conduct.
- There is instability and a lack of resilience within the OPCC and complaints made in respect of the PCC or chief constable are not handled correctly.

FIRE

- There is an inability to create a resilient and forward-thinking organisation.
- Failing to create a culture of openness and transparency.
- That appropriate internal controls are in place across the organisation and that assurance has been sought on their effectiveness.



Ineffective governance structures and processes can prevent an organisation from achieving its strategic objectives, leading to poor decision making and resulting in poor reporting.

Most governance related risks in our analysis were contained within OPCC risk registers. While many of these risks are similar to those seen in previous analysis, there are wider changes anticipated to be on the horizon, linked to the government's one and two-part reviews.

While there was little mention of governance across fire risk registers, the government's Reforming our Fire and Rescue Service white paper includes measures to strengthen governance within the sector. Aligned with the government's commitment to mayoral devolution, in the proposals published in May 2022 it was stated that fire functions would be transferred 'to a single, elected – ideally directly elected – individual who would hold their operationally independent Chief Fire Officer to account. This person could be: a mayor who could delegate day-to-day oversight to a deputy mayor; or a council leader who could delegate to a cabinet member or a police, fire and crime commissioner.' This arrangement is believed to enhance 'public accountability.'

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Are your values and culture, strategic direction and objectives understood by all members of the board and its sub-committees? **How do you ensure this is the case?**

Do terms of reference adequately and accurately define the roles and responsibilities of the committees? Are committee effectiveness **self-assessments undertaken?**

Does the board consider its composition, with a **view to enhancing diversity and experience?**

Does your organisation have a blind spot in relation to documenting a risk of culture within the Force/Service and **how this is being managed and monitored?**

Other risk themes in summary

Strategy

- That strategic plans are undeliverable due to capacity issues and business change is not embedded, resulting in a failure to deliver efficiencies or improved services.
- Transformation to drive through efficiencies is not delivered and the best use of resources is not achieved.
- The business continuity plan/strategy is not effectively developed to ensure that service delivery can be maintained in the event of severe disruption.
- Failing to respond to environmental challenges and the need for an aligned climate action plan.

Collaboration and partnerships

- The anticipated benefits of collaboration, such as improved productivity, are not realised and a planned increase in collaborations to improve efficiency is not achieved.
- For police, there is a risk the PCC fails to work effectively in partnership with community leaders, which can impact the successful delivery of the Police and Crime Plan.
- Due to administrative difficulties, a shared service may have to be brought back in-house, which could increase costs.
- Data may be unreliable, meaning the true benefits of collaboration cannot be measured or quantified.

Ensuring effective collaborations

The organisation involved in each collaboration project should work towards the agreed objectives and measures, which are set out in clearly defined metrics. They should deliver against the financial plan and not use statistics that have not been agreed by other members or which meet their own requirements but potentially not the requirements of other collaborative partners.

This can be difficult to agree when each party may have differing driving forces and requirements for the collaboration, but it is crucial to the achievement of the collaboration itself.

Periodically, there needs to be a formal review of the cost versus benefit of the collaboration, to ensure that it is in line with both service delivery and efficiency plans, and to put remedial actions into place, if not. This should be reported via the governance framework to allow for effective discussion and clear, transparent decisions to be made.

How are you managing collaborative partnerships to ensure they deliver quality outcomes?

Infrastructure and assets

- Fire and police services have an aging estate that does not meet current or anticipated future needs.
- Assets are lost, damaged or stolen and there is wider ineffective asset management.
- That value for money in estate and asset disposal is not achieved.
- With the government's ambition to phase out the sale of new petrol and diesel cars and vans by 2030, there is uncertainty what this means for fleet vehicles.

Covid-19

- The risk of staff being exposed to the virus and the associated impacts of the pandemic on wellbeing.
- There may be a resurgence of the virus putting pressure on people as a resource.
- As a result of the pandemic, there are backlogs in the criminal justice system, which may lead to victims losing faith in the system. It also puts at risk cost recovery from police-led prosecutions.

Reputation and engagement

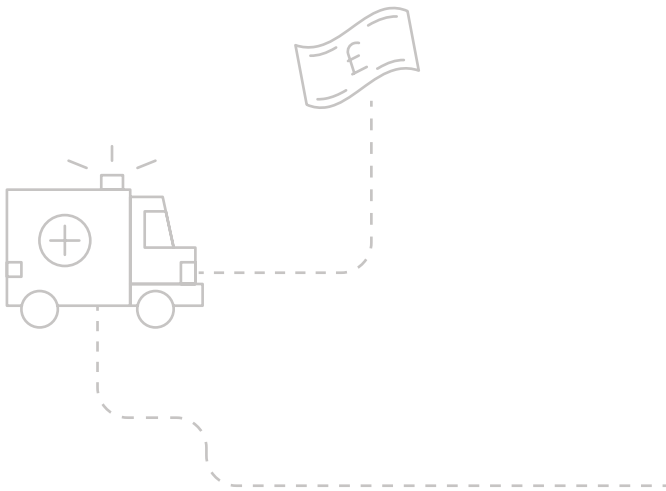
- Force reputation could be damaged if relationships with media and communication channels (social media) are not properly managed and may lead to incorrect information being publicised.
- Force reputation is damaged as a result of an external review or the behaviour of officers, which ultimately places the force's legitimacy in question. As links with the community become fractured, this can also impact the ability of the force to cut crime successfully.

Information and evidence

- There are data quality issues, such as inaccurate data recording or duplicate data entries, meaning data cannot always be relied on.
- Data is not managed across regions effectively or presented effectively, through clear visualisations.

Brexit

Brexit risks remain within a minority of the risk registers in our analysis. There are concerns that Brexit creates disruption, impeding the effective sharing of information and there are supply issues and that associated costs increase.



Research for the Independent Office for Police Complaints, undertaken by YONDER shows that positivity towards the police has declined to 49% at March 2021. Key to rebuilding trust will be ensuring greater focus on vetting and counter-corruption measures and publicising the results of the work in this area.

Managing risks

Risks should be clearly articulated, so that the risk you are trying to manage is clearly understood. There are established risk management practices across the sector with 84% of organisations using a 5x5 risk scoring matrix and 16% of services using a 4x4 matrix.

The average number of risks per risk register was 14.2 risks. Our last measure in 2020 revealed the average number of risks to be 14.8, which means there has been little movement. We continue to see some wide variation, with two services in our sample having over 30 risks on their strategic risk register. Services should be mindful that only strategic risks should be included within the strategic risk registers to ensure that effective oversight and management is focused on areas where it is most required.

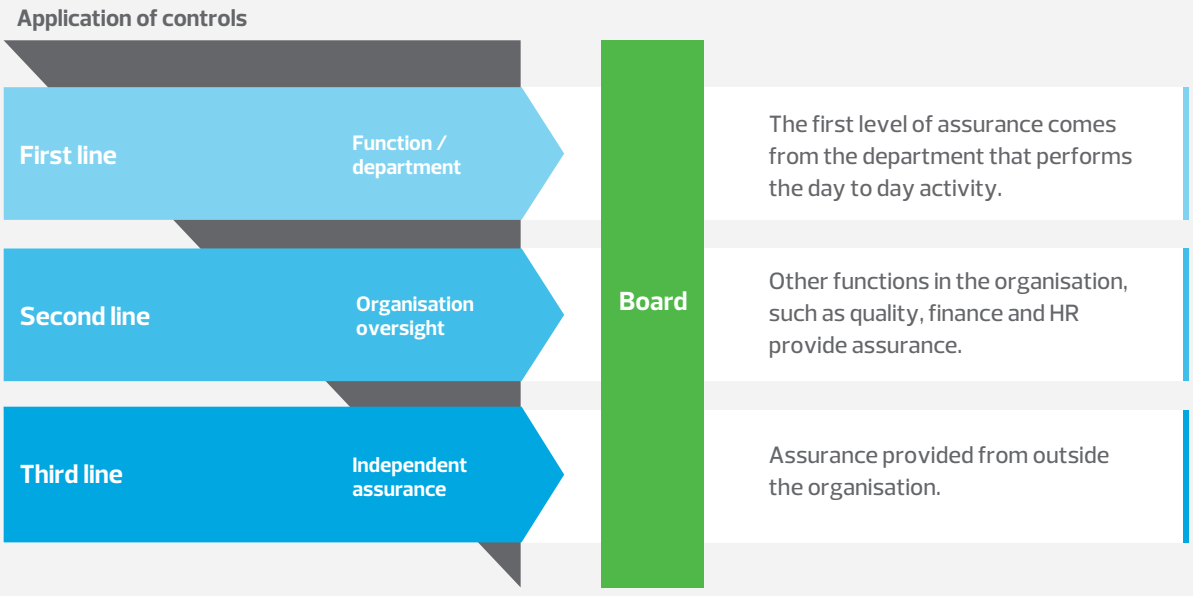
Target risk scoring is used by some services, and some identify their sources of assurance. Assurance provides an element of confidence, and allows services to be sure that governance, risk and internal control processes are operating as intended. There is merit in mapping assurance at the first, second and third line, identifying both internal and external sources.

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.

With services and directly elected commissioners, the process for managing risk needs to be clear, ensuring visibility of the entirety of the risks being faced. There should be a consistent approach where senior leaders understand, for example, the organisation's risk appetite and how to apply it.

Horizon scanning is also important to understand emerging risks in the short, medium and longer term.

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



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 is a healthy (essential) boardroom discussion – exploring as a collective the types of risks we are facing.

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, then we are in a much better position to manage risk in making decisions, focusing our monitoring and reporting as well as our use of our assurance resources.

Insight4GRC

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

We have over 250 organisations from all sectors licenced and use one, some or all, of the Insight4GRC modules. Insight4GRC provides management with real time information in connection with the identification, assessment and management of risks, the communication and acceptance of policiesand 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

FURTHER INFORMATION

Daniel Harris
Head of Emergency Services and Local Government
E: daniel.harris@rsmuk.com

Walter Akers
Contracts and Procurement
E: walter.akers@rsmuk.com

Matthew Humphrey
Insight4GRC, Risk Management
E: matthew.humphrey@rsmuk.com

Scott Harwood
Public Sector VAT
E: scott.harwood@rsmuk.com

Andrea Deegan
Fraud Risk Services
E: andrea.deegan@rsmuk.com

Emma Griffiths
Risk Assurance Technical
E: emma.griffiths@rsmuk.com

Steven Snaith
Technology Risk Assurance
E: steven.snaith@rsmuk.com

rsmuk.com