

MANAGING RISKS IN A CHANGING ENVIRONMENT

Analysis of fire and rescue service risk registers

December 2020

OVERVIEW OF RISKS

Our latest review of fire and rescue services (FRSs) strategic risk registers identifies some persistent challenges, together with some new and emerging risk areas, particularly in relation to IT and the external environment.

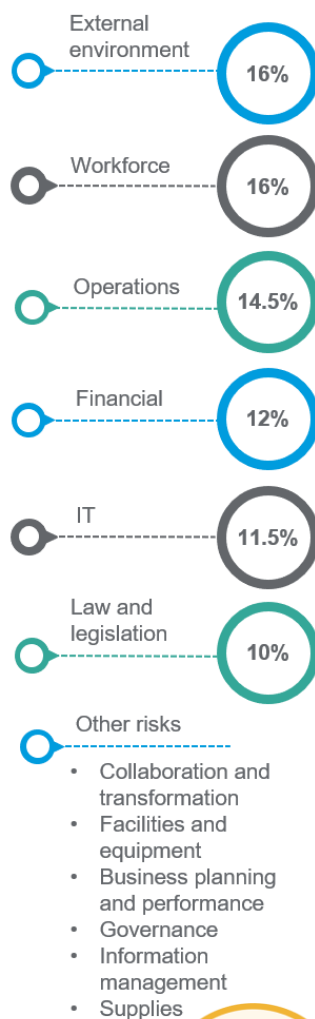
We have analysed the risk registers of 16 FRSs, examining 264 individual risks in total. We have categorised each risk by key theme to understand those areas of greatest concern. In doing so, services should be mindful of not just the risks highlighted but also those opportunities for development and service enhancement.

In terms of quantity, there were more risks related to environmental matters, such as the Covid-19 pandemic, workforce and operations. Yet, when we look at those high residual risks only – focusing on the top risk(s) facing services – more of those risks related to financial matters, followed by IT and the external environment.

Whilst each risk is categorised by theme, they nevertheless inter-relate and in culmination have the potential to have severe ramifications for FRSs. Financial factors, pensions, incident response capability, workforce numbers, increased regulation, reputation and operating within a pandemic situation are all elements creating significant uncertainty.

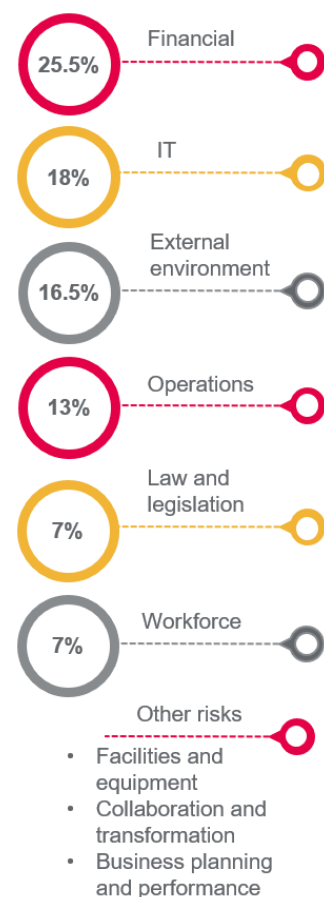
As such, effective planning, horizon scanning, and effective risk management are paramount. By understanding and seeing how risks inter-relate allows services to have a better understanding of their organisation, and in terms of controls, ensures that one mitigating action does not impinge upon another risk.

All risks within risk registers



Average number of risks per risk register: 16.5

High risks within risk registers



Average number of high risks per risk register: 3.6

External environment

In 2020, all organisations have had to deal with the far-reaching implications and impacts brought about by the Covid-19 pandemic. For the purposes of our analysis we have grouped pandemic related risks together. Yet we know the pandemic is not a risk in itself, but rather something that currently affects everything.

Covid-19 pandemic

Pandemic related risks include:

- failing to deliver core services and emergency response due to a reduction in staff resource as a result of absence;
- services are unable to access safety and protective equipment as supply chains are impacted;
- prevention activities are halted leading to backlogs and missed actions / referrals;
- in assisting other arms of the emergency services FRS response resources are reduced;
- recovery has not been mapped out effectively, meaning that as Covid-19 alert levels reduce, programmes and activities beyond those core obligations are not understood;
- financial loss and reputational damage through adopting new technologies that have not been thoroughly tested; and
- employees exploit the test and trace programme, while the services response regarding employee health, safety and wellbeing is ineffective.

When managing risks through the pandemic it is important to ensure continuity of effective governance arrangements for effective oversight, challenge and decision making. In responding to the pandemic FRSs have encountered new risks, which together with their impact, need to be managed. Services should consider the following actions:

- adapt your governance arrangements to ensure that the Service and Authority are able to function effectively (to set direction, measure performance, have oversight, undertake scrutiny and make decisions) whilst working and meeting remotely. Map and receive regular and relevant assurances on your strategic risks;
- don't manage your response through spreadsheets. The Service, management and staff need to have access to real time information. Investing in a system with workflow and action tracking could help;
- manage change risks, embracing the 'new normal' and take steps to reshape the organisation as required;
- reforecast to identify specific financial resilience and sustainability challenges; and
- communicate with partners and suppliers, and work more collaboratively, recognising that in some cases things do not always go as planned.

To find out more, please visit:

<https://www.rsmuk.com/coronavirus-adapting-to-change/governance-and-risk/seven-ways-to-prepare-your-business-for-a-coronavirus-second-wave>

Brexit

There are concerns that Brexit will impact on the sustainable supply of equipment, impacting upon the ability of services to deliver their duties effectively and efficiently. Data sharing arrangements at the end of the transition period are also a significant cause for concern. Whilst the Information Commissioner's Office confirms the General Data Protection Regulation will be taken into UK law, there will be other requirements for EU data transfers / EU located data / operations.

Prevention and outreach

An ageing population creates greater demand for services, amidst other challenges, such as unemployment and social isolation. Services are likely to be revisiting their prevention and outreach initiatives at this time.

Climate change

There are concerns that changes within our environment, for example hotter summers, may create an increase in fire service demand at both the local and national level.

Financial

Most high risks across the risk registers in our sample focus on financial matters. Income had reduced through the period 2016/17 to 2019/20, while FRSs have received a proportion of the £1.6bn of government funding to support the response to the pandemic. That said, there continue to be risks regarding the amount of funding services have at their disposal to deliver vital services, and there are risks that budget savings and efficiencies are not achieved. Concerns regarding future funding settlements are mounting, as services could face a reduction in grant allocation as a consequence of the pandemic, as well as a cap on public sector wages.

We have seen services make savings and efficiencies in recent years. That said, the importance of appropriate and sufficiently robust budgetary management processes cannot be overstated. There needs to be clear engagement with budget holders and, as services work to agreed budgets, there should be a process of validation checks to ensure the accuracy of figures and any cash flow variances (between actual and budgeted) should be fully explained. This helps services to work towards delivering the agreed budgets and to take preventative action where this is needed.

Areas of potential efficiency gains

- Buying goods smarter – from uniforms to vehicles. Using collaborative buying power.
- Collaboration – such as shared services including back office functions.
- De-collaboration – where intended efficiency outcomes or public safety objectives are not realised.
- Operational transformation – including the development of automated systems and processes and increased technological solutions.

Workforce

Workforce related risks centre upon a lack of suitably trained, skilled and knowledgeable staff and officers, a failure to recruit and retain officers including on-call firefighters, in addition to experience being lost through retirement with an increasingly ageing workforce in some areas. There are risks that the service does not reflect community diversity, robust succession plans are not in place, and there is a failure to bring about workforce changes to meet future needs and deliver against the people strategy.

Data from the Home Office illustrates that (in England) between 2015 and 2020, the number of firefighters (in terms of headcount) has reduced by 7.2 per cent, while total staff reduced by 5.3 per cent. From its inspection activities Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) has concluded that the majority of services do not have enough on-call firefighters, which shows that recruitment and retention remains a concern.

While recruitment continues to be an issue for FRSs, with 60 per cent of services deemed either inadequate or to require improvement, HMICFRS is clear that more is needed regarding people. From its inspection work, HMICFRS has stated that some services need to do more to address 'toxic' environments involving bullying and harassment and improve the diversity of the workforce. In addition, and perhaps more than ever, employee mental health and wellbeing is an area receiving greater attention.

Employee engagement and mental health

We have all learnt to do things differently this year, adapting in ways we would not have imagined and at a faster pace. Employee engagement is important, it always has been, but with different approaches emerging in a changing set of circumstances which give rise to new risks, it is more important than ever. Services should consider the following:

- given the increased importance on wellbeing and mental health, is your service sighted on how these risks are managed within the workforce and if the actions taken are working and supporting your organisation sufficiently?
- are key performance indicators in place to determine any impact on service delivery / performance because of mental health absence or do you capture statistics on early retirement due to mental health?
- agile, remote and flexible working practices may have emerged for support teams. How is training being delivered remotely? Are remote personnel aware of their data security responsibilities, to ensure there is no data loss?

Operations

After a steady rise, between 2018/19 and 2019/20 there has been a 3 per cent reduction in incidents attended in England. In a similar trend, the number of incidents attended across Scotland and Wales has also reduced over the same period. Yet, we know that through lockdown, with more people staying at home, the risk of fire is greater. Risk registers include risks focused on inadequate operational systems and system failures, and service management and response capability. There are concerns that a preventable death may occur, there is a failure to effectively mobilise services hindering emergency response, and the service is unable to respond adequately to an incident, or there is a fundamental loss of service provision placing the welfare of communities at risk.









IT

HMICFRS has noted that across the sector the use of technology varies considerably. Some services are investing in technology to improve their effectiveness and efficiency, yet almost half of services inspected are using IT systems that are broken, dated or unreliable, and some rely on using inefficient paper-based systems. In some services, the lack of investment in IT is leading to reduced levels of productivity. There are also the additional costs and issues around the delayed implementation of the Emergency Services Network (ESN) to replace the Airwave networks, which is impacting all Emergency Services. An effective Digital / IT Strategy and vision remains crucial to support digital transformation, along with investment in robotics over the coming years.

While our reliance on technology is increasing, the pandemic has brought with it an increased risk of fraud. It has made many organisations more vulnerable to cyber-attacks as a result of relaxed control environments, revised processes and procedures, and changing employee workforce profiles. Given the increase in remote working, the roll-out of IT equipment to facilitate this at high speed and the opportunistic nature of the cyber-criminal to target areas of change and potential weakness, the Covid-19 pandemic has provided the environment which has consequently enhanced the associated risks in this area.

Gaps in your defences can be targeted both at a human and system level, and with increased remote working, the risk of data loss increases.

Typical methods of cyber-crime

-  **Social engineering** - criminals manipulate people to gain access to confidential and sensitive information.
-  **Phishing** - criminals send emails pretending to be someone else, often an organisation, to obtain key information or a fund transfer.
-  **Identity theft** - the deliberate and intentional use of someone else's identity and credentials for gain.
-  **Spam emails** - unsolicited emails which are sent in bulk.
-  **Malware** - a type of software that is designed to disrupt systems.
-  **Ransomware** - a type of malware that blocks access to data and systems until payment is made by the organisation or person under-attack.
-  **Whaling** - targets those in senior positions for financial gain or access to sensitive information.
-  **Island hopping** - supply chain and third parties are used to target another organisation, usually one that's bigger or more complex.

Six ways to protect your organisation against cyber-crime

Cyber criminals don't just target large businesses. Data is king when it comes to cyber-crime, and cyber criminals are on the hunt for vulnerabilities wherever they exist. Weak IT controls can grant access to systems and provide cyber criminals with a route to underlying business and personnel data.

1. Raise cyber security awareness.
2. Back up your information.
3. Protect your social media accounts.
4. Examine your supply chains.
5. Update your operating systems.
6. Educate staff on credential theft.

To find out more, please visit:

<https://www.rsmuk.com/ideas-and-insights/why-cybercrime-is-increasing-and-how-to-stay-secure>

Laws and legislation

Legislative requirements and regulatory scrutiny are increasing. There are concerns that services fail to adhere to their legal / statutory responsibilities relating to, for example, health and safety, building fire safety regulations, and data protection.

Other risk areas

Collaboration and transformation

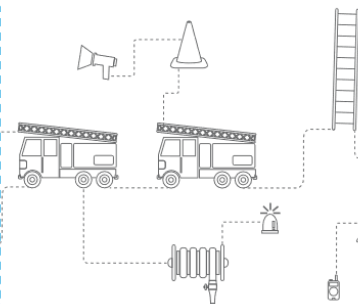
- To increase efficiency and effectiveness in terms of service delivery and in securing financial gain, risks are focused on grasping collaborative or transformative opportunities.
- Concerns that the intended benefits of a collaboration are not achieved, there is ineffective project management and that service delivery is impacted.

Facilities and equipment

- Inadequate facilities and equipment such as an aging estate and vehicles, and a lack of regular safety checks of equipment, pose risks in terms of health and safety but also potential service disruption.
- Asset management record processes are not in place, meaning services do not have a clear view of their equipment, vehicles, buildings and other property.

Business planning and performance

- Set performance targets (including response standards) are not achieved owing to resource levels, leading to intervention and adverse reputational impact.
- Business continuity plans are not fully effective to ensure that in the event of crisis, services are as fully maintained as possible.



Supplies

- There is a failure in the supply chain, meaning services are unable to obtain key equipment to ensure service delivery.
- Failure to comply with procurement rules.

Governance

- Internal control arrangements are not in place, resulting in services becoming at risk of intervention and failure to achieve statutory responsibilities.
- Failure to embed organisational culture and failure in leadership capacity.

Information management

- Due to the increasingly complex nature and volume of data, data is not managed and shared properly across the service.
- Data is not of quality, posing risks where it is being relied upon to take business decisions, and a lack of effective information management may lead to data breaches.

Concluding comments

The challenge for FRSs is to ensure that risk profiles remain current, that robust internal controls are mapped to each risk and are in line with risk appetite, and that appropriate assurances are sought so that the service can take comfort in the knowledge that controls are operating as intended. Through the pandemic, this is more important than ever, as it is likely that updated or new internal controls will have been implemented at scale and at pace.

FOR FURTHER INFORMATION CONTACT

Daniel Harris

National Head of Emergency Services and Local Government

M +44 (0)7792 948 767

E daniel.harris@rsmuk.com

Steven Snaith

Technology Risk Assurance

M +44 (0)7966 039 009

E steven.snaith@rsmuk.com

Matthew Humphrey

Insight4GRC, Risk management

M +44 (0)7711 960 728

E matthew.humphrey@rsmuk.com

Insight4GRC™ is a cost-effective governance, risk and compliance software (GRC) suite that provides management teams with the tools needed to monitor and control performance, assess organisational risks, track assigned actions, enable employee awareness and facilitate company policy acceptance.

Each of our Insight4GRC™ products has initial training and implementation services available and ongoing hosting, support and maintenance is provided through our dedicated support programme. Advisory and assistance services are available if required.

For more information please visit www.insight4grc.com.

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 Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Employer Services Limited, 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 members of 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 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. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Before accepting an engagement, contact with the existing accountant will be made to request information on any matters of which, in the existing accountant's opinion, the firm needs to be aware before deciding whether to accept the engagement.