MANAGING RISKS IN A CHANGING ENVIRONMENT

Analysis of police strategic risk registers

April 2021

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

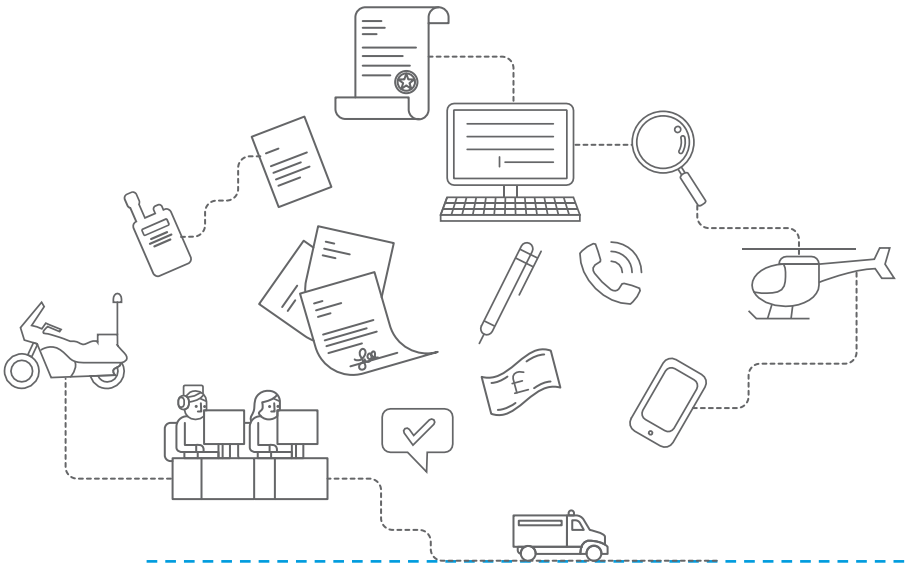
OVERVIEW OF RISKS

Our latest review of police strategic risk registers identifies some persistent challenges, together with some new and emerging risk areas, particularly in relation to demand management, workforce planning and responding to the Coronavirus pandemic.

We have analysed 31 strategic risk registers, examining 461 individual risks in total. Our analysis is made up of risk registers from police forces, offices of the police and crime commissioner (OPCC) and police, fire and crime commissioners (PFCC). We have categorised each risk by key theme to understand those areas of greatest concern. In doing so, police forces and PCCs (including PFCCs) should be mindful of not just the risks highlighted but also those opportunities for development and service enhancement.

In a statement to parliament on 16 March 2021 Home Secretary, Priti Patel, confirmed the government's intention to 'strengthen PCC accountability; improve their transparency to the public; clarify the relationship between PCCs and Chief Constables; bring more consistency to the PCC role; raise professional standards; and improve the checks and balances currently in place.' With the conclusion of part one of the review into the role of PCCs, Priti Patel stated that the Specified Information Order will be amended requiring PCCs 'to provide a narrative' on force performance against crime measures and Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) force performance reports. Providing information to the voting public is key in terms of enhancing accountability and will be firmly on the agenda for new and returning PCCs in the May elections, while government changes create an element of uncertainty.

Community engagement and reputation continue to be key for police forces, and regarding coronavirus, is an important part of ensuring the public adhere to the restrictions, in line with the government's roadmap. This has undoubtably presented new challenges, with different demands, and at a time where HMICFRS has stated that the 'police's response to protests needs to strike a better balance.' In its 'snapshot' report looking at policing between March and November 2020, HMICFRS noted that 'through innovation, flexibility and adaptability, forces generally successfully maximised the protection of staff while minimising the effect on public service.' The inspectorate also noted that police forces introduced new ways of working that have the potential to provide future benefits to policing, such as utilising video conferencing technology when working with local safeguarding services.



In terms of quantity (see figure 1 overleaf), there were more strategic risks related to operational policing matters than any other. This was closely followed by coronavirus risks and financial risks. Yet, when we look at those high residual risks only – focusing on the top risk(s) facing forces and PCCs – more of those risks related to financial matters, followed by operations and the workforce.

Whilst each risk is categorised by theme, they nevertheless inter-relate and in culmination have the potential to have severe ramifications. Financial factors, incident response capability, workforce numbers and demand management, 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. Understanding and seeing how risks inter-relate allows forces and OPCCs to have a better understanding of their organisation, and in terms of controls, ensures that one mitigating action does not impinge upon another risk.

Figure 1: Force and OPCC strategic risk registers by quantity and 'high' residual risks only

Operations and the coronavirus pandemic

There is perhaps little surprise that risks focusing on operational policing are a significant feature in risk registers, particularly given the demands posed by the coronavirus pandemic.

Demand management continues to be an area of focus, where there are policing requirements that may be unmet due to limited resources (financial, people and skills). Given the complexity of the pandemic, together with its scale, the policing focus will have shifted since March 2020, and with it, created new challenges.

HMICFRS in its State of Policing report notes 'as quickly as the public had to adapt to life under the regulations, the police had to learn how to enforce them.'

Data from the Office for National Statistics (ONS) reveals that in the year ended September 2020 police recorded crime reduced by 6 per cent, driven largely by 'substantial falls during the April to June 2020 period, particularly in theft offences.'

Operations focused risks:

- local crime reduction priorities are not realised, for example preventing / reducing organised crime and anti-social behaviour;
- victim support services are under-resourced and / or do not deliver intended outcomes;
- investigation failures occur and forces fail to protect those who are vulnerable; and
- operational effectiveness is not achieved, so that, for example there are reductions in violent crime.

The ONS states there have been 'fluctuations' in crime levels, with falls in offences involving firearms, but increases in drug offences, which saw a 16 per cent increase, again driven by a significant increase during April to June 2020. Through national and local lockdowns forces have experienced greater demands in other areas too. Cyber-crime and domestic violence are notable examples. We have also seen forces support and work collaboratively with other arms of the emergency services in dealing with the pandemic response.

For the purposes of our analysis we have grouped pandemic related risks together; we know the pandemic is not a risk in itself, but rather something that currently affects everything. Within the risk registers in our sample, coronavirus related risks include:

- staff resource may reduce, with the need for officers to self-isolate, limiting the ability of forces to deliver critical services;
- officer exposure to the virus (and those in police custody) and the mental and health wellbeing of employees;
- there are rises in public disorder instances and there are backlogs within criminal justice;
- there is significant business disruption leading to ceased activities for a proportion of time and there may be equipment and supply shortages;
- IT facilities may not be adequate to meet the needs of remote employees and there are risks regarding information security breaches;

- there are additional costs (which are not met by the government through support grants) or lost income, which may create funding pressures or the need for further funding controls in the future;
- with the fluidity in which changes have occurred and varying restrictions imposed, there is uncertainty within the force, on how to respond appropriately in all instances; and
- resources are not used economically and efficiently, and high standards are not maintained.

Tips for managing risk through and after coronavirus

1. Do not throw governance out the window.

   Adapt your governance arrangements to make sure your Board is able to function properly. This will allow your Board to set direction, measure performance, have oversight, undertake scrutiny and make decisions.

2. Coronavirus is not a risk in its own right – it currently affects everything.

   Review your strategic risks cause descriptions. This will likely mean that you have to adapt your controls or create new actions in the context of the risk to ensure that it is being suitably managed.

3. Coronavirus response – things do happen.

   All organisations should have a contingency framework within which it can operate when situations like coronavirus or similar arise.

4. Don't manage the coronavirus response via spreadsheets.

   This is a fast-moving environment so make sure that the Board, management and staff have access to real time information, eg updated actions, communications, evidence etc, all in one place. This will provide all the main stakeholders visibility of the response and ensure a more coordinated and consistent approach. Investing in a system to communicate and track actions, progress and updates, and provide useful management information doesn't have to be expensive and will cut down on unnecessary and inefficient administration. This will provide a good return on investment.

5. Prepare to manage the change risks - embracing the 'new normal'.

   Organisation leaders need to still be looking ahead, capturing the learning from this event, reviewing strategy and operating models, identifying emerging innovations and opportunities, listening to stakeholders. As important as it is to survive and bounce back, it is more important to bounce forward and be ready for the new normal.

   Having appropriate mechanisms in place to prepare, initiate and process the forthcoming change in the future short, medium and longer term will be as crucial (if not more so) as the initial response to ensure sustainability and growth.

To find out more, please visit: Tips for managing risk through and after coronavirus | Coronavirus: adapting to change | RSM UK

Financial

Despite increases in funding, financial risks continue to be a significant concern for forces and PCCs. More 'high' risks were finance related than any other. PCCs will receive an additional £636m in 2021/22 (as announced by the Home Office in December 2020) providing they utilise the full police precept flexibility. £415m of funding is to be used as part of the drive to recruit 20,000 additional officers by 2023. There remain however some wider concerns regarding the long-term financial impacts of the pandemic and what that may mean for future funding settlements. It also limits the ability of forces and PCCs to implement effective medium-term financial plans.

Whilst recent funding increases are welcome, there are concerns regarding potential increases in pension contributions, the impact of Brexit, that national projects including the Emergency Services Mobile Communication Programme (ESMCP) and the Police Education Qualifications Framework (PEQF) may impact upon force budgets as they exceed their affordability envelope. Other risks include:

- potential implementation of a new funding formula;
- funding sustainability for specific programmes / projects;
- financial resources may be insufficient to deliver an effective and efficient service and efficiency gains are not realised; and
- effective financial management is not in place, budgets are exceeded, and that the medium-term financial plan is not aligned to the police and crime plan.

Workforce

The police workforce has been increasing. The Home Office states that 'there were 216,155 workers (FTE) employed by the 43 territorial police forces in England and Wales on 30 September 2020, an increase of 11,341 (or 5.5%) compared with a year earlier, and of 5,402 (2.6%) since March 2020.' As at 31 December 6,814 police officers had been recruited; 6,620 via the Police Uplift programme and 194 through other funding streams.

Recruitment and training will be resource intensive and create additional demands but should leave forces better able to meet the policing requirements they face. There are also opportunities to consider force diversity. As at 31 March 2020, of those that stated their ethnicity, 7.3 per cent were BAME officers, while 'under-representation was highest amongst senior ranks.' This is a risk area we have seen in risk registers.

The requirement for forces to recruit 20,000 additional officers will have financial and workforce impacts.

There is a back office (support services) cost to more frontline officers, which will need to be funded. New recruits will clearly require training and on-the-job support, as well as access to vehicles, uniforms and ICT devices. All of the associated recruitment, investment in technology and equipment also needs to be managed carefully.

Whilst there is clearly a cost element, forces will be looking to establish a modernised workforce to meet anticipated future need.

Other risks include:

- there is a lack of supervisory officers, meaning that demand cannot be matched;
- inability to recruit and retain suitably trained staff;
- inability to move into and yield the benefits of a modern workforce;
- steps to promote a positive culture are not achieved;
- unethical behaviours by a minority of officers are sustained;
- vetting procedures encounter delays;
- the welfare of officers and staff are not safeguarded; and
- there is a failure in an employer's duty of care.

Employee engagement and mental health

We have all learnt to do things differently since the onset of the pandemic, 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. Forces and PCCs should consider the following:

- given the importance of wellbeing and mental health, is your organisation sighted on how these risks are managed within the workforce and if the actions taken are working and supporting your organisations sufficiently?
- what are the outcomes, required actions and progress made so far in relation to the College of Policing's 'Blue Light Wellbeing Framework' self-assessment tool?
- 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?

IT

We continue to see risks regarding the delayed ESMCP related to coverage, project timescales and costs. There are also other risks regarding system implementation and system vulnerabilities as well as performance. They relate to, for example, Case Management Systems.

Forces and PCCs, like other organisations, are increasingly susceptible to cyber-crime. While our reliance on technology is increasing, the pandemic has brought with it an increased risk of fraud, in particular through targeting staff and access credentials being compromised. 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-criminals to target areas of change and potential weakness, the coronavirus 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.
- **Credentials and 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

The Real Economy – Cyber Security

The cyber-crime threat has been amplified by the impact of the pandemic. Of course, forces and OPCCs face cyber security threats directly, but with attacks growing in sophistication police investigation teams also face greater demands.

RSM's 'The Real Economy, Cyber Security' report on threats to the middle market highlights that 20 per cent of survey respondents have experienced a cyber attack during the past 12 months. Of this sample, 71 per cent stated the attack was as a direct result of the coronavirus pandemic.

75 per cent of our survey respondents said they could see their businesses becoming a target of an attack by manipulating business' employees into providing access to, or altering, systems, data, or business processes by pretending to be trusted third parties or high-ranking business executives.

As an increasing number of business 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.

For more information and insights visit: Cyber Security | The Real Economy | RSM UK

Strategy

There are several risks relating to strategic failure, where the objectives within the police and crime plan (PCP) are not achieved or that the Strategic Policing Requirement set by the Home Office is not met. Other risks include:

- transformation programmes are not achieved and other programmes for organisational enhancement are not realised;
- the objective to be 'agile' in working practices fails to take shape;
- crime prevention or demand management is not effective, meaning forces take a reactionary approach to policing; and
- failing to adequately prepare for PCC elections that are postponed until May 2021.

We know that a number of PCC's are not standing for re-election. As a result, there could be different priorities within PCPs, which may have an impact.

Environmental, Social and Governance (ESG)

The emerging Environmental Social Governance agenda is creating a new risk dimension for emergency services, in that these risks are:

1. largely driven by external / global risk drivers and emergency service providers need to be prepared to understand the potential implications they have on the way they provide services; and
2. of interest to stakeholders, of which there are many, and therefore emergency service providers need to ensure that they respond to these risks appropriately ie ethics, equality, modern slavery, inclusivity, climate change etc.

For more information, access: ESG | RSM UK

Collaboration and partnerships

We know that collaboration has the potential to yield significant benefits. With the monumental demands of the pandemic, we have seen police forces and fire services support the 999 ambulance response, illustrating just how beneficial working together can be.

Yet, we continue to see risks relating to identifying collaborative opportunities, an inability to realise anticipated efficiencies, as well as effectiveness within collaborative ventures. There are risks that intended benefits are not achieved and that measures for assessing success are unreliable. In seeking to maximise efficiency gains, de-collaboration should be considered where intended efficiency outcomes or public safety objectives are not realised.

Following previous inspection work, HMICFRS has noted that more work needs to be done to address the issues around the uncertainty of who has overall responsibility for the collaboration, and the difficulty to reach a consensus across several forces. Should collaborations fail or there is ineffective partnership working, perhaps as a consequence of weak governance and accountability, there could be reputational consequences and a failure to meet strategic aims.

The Policing and Crime Act 2017 places a statutory duty on police, fire and ambulance services to keep collaboration opportunities under review and enter into collaboration when it is in the best interests of efficient and effective service delivery.

As with all collaborations there are challenges, such as the misalignment of objectives and poorly articulated risks. What we are seeing, is a greater need for chief constables (CCs), PCCs and audit committees requiring assurance over their collaborations.

Assurance provides an element of confidence. It allows the PCC and CC to be sure that governance, risk and internal control processes are operating as intended and that an effective and efficient policing service is in operation. Given the complexities of joint ventures and collaborative working, it is essential that PCCs and CCs understand their assurance needs and how those assurances will be obtained.

Collaborative working is likely to continue to grow, involve wider agencies and become more complex. The Police, Crime, Sentencing and Courts Bill aims to introduce a duty on specified authorities (police, local authorities, specified health authorities, youth offending teams, probation services, and fire and rescue services) to work together to prevent and reduce serious violence.

Against this backdrop, CCs, PCCs and audit committees may question, ‘are we clear and comfortable with our assurance model?’ We have seen that collaborative assurance arrangements can be inconsistent, and not as effective or efficient as they could be.

Maximising the benefits of collaboration

- Are all partners clear on the intended benefits and outcomes of the collaboration, understand all associated costs and what it would mean should the collaboration fail?
- How are you monitoring, and are you sighted on, all outcomes and consequent benefits from collaborative working?
- Are lines of command for decision making clear and working effectively?
- Are the right people, with the required skills and expertise, matched to need, and are they sharing lessons learnt?

Given the complexities that can arise through joint working it is important to gain the required level of assurance that risks and resources are being well managed. Each individual organisation should have its own mechanisms in place to gain assurance. When multiple organisations are working together, there is a tendency to rely on other collaborative partners providing or monitoring the assurance, and without a defined assurance map there is a potential for things to slip through the net.

Other risks

Regulation and standards

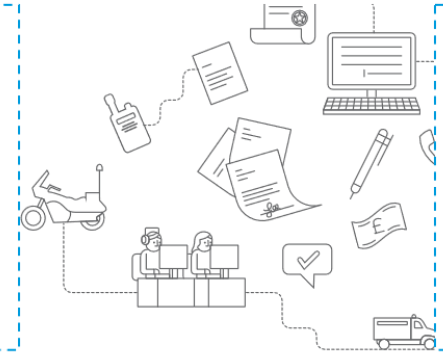
- Failure to comply with regulations including the General Data Protection Regulation, Freedom of Information requests, Subject Access Requests and Records Deletion.
- Failure to comply with Management of Police Information (MoPI) regulations.
- Improvement areas are not rectified, and positive inspection outcomes are not achieved.

Infrastructure and assets

- Supply chains fail to deliver vital equipment.
- Estate deterioration, and lack of maintenance relating to, for example, inadequate door entry systems, which hinder effective and efficient policing.
- Estates strategy is not achieved, with project complexities and insufficient resources, while there is a failure to obtain value for money in estate disposal.

Governance

- PCC fails to hold the CC to account and ensure they are appointed, supported and challenged.
- PCC and CC fail to demonstrate, and apply the principles of, good governance.
- Structural changes, for example as a result of devolution of power, impact negatively on service provision.



Reputation and engagement

- Lack of awareness and confidence in PCC, linked to a failure to engage with the public.
- Public confidence in local policing is reduced as a result of ineffective communications on priority matters including for example Coronavirus and Black Lives Matter.
- Delays in the criminal justice system impacts reputation.

Information and evidence

- Crime data integrity and data quality issues hinder the ability of forces to understand crime patterns.

Brexit

- There is a level of uncertainty regarding the potential impacts of Brexit and concern that cross boarder co-operation arrangements may be inadequate.

Risk identification

Our review of 31 strategic risk registers illustrated that:

The risk registers in our sample included as few as four risks; up to a maximum of 35 risks. 12 risk registers contained more risks than the average (14.8). This is further analysed in figure 2.

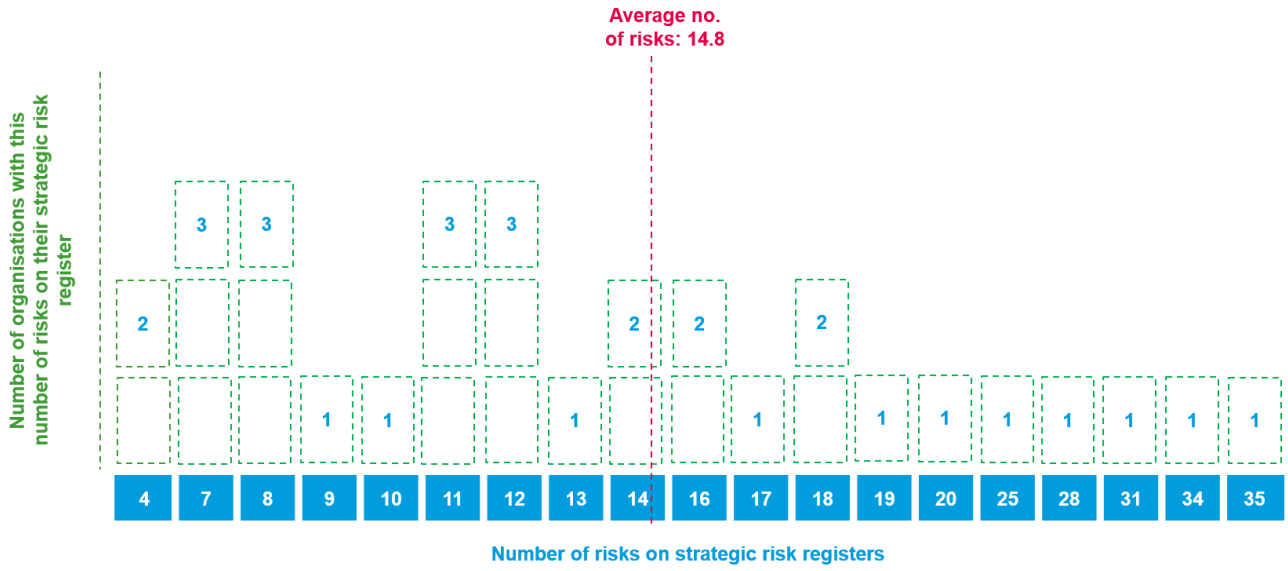


Figure 2: Number of risks on each risk register in our sample compared by average

Within those risk registers containing greater numbers of risks, some of the risks were not as high-level and strategic in nature, as those strategic risk registers containing fewer risks. There was some room for risk rationalisation as there were examples of some duplication. The greater the number of risks present on the strategic risk register, the harder it is to maintain effective management and oversight of them.

Linked to this is the need to ensure only strategic risks feature on the strategic risk register. Those more operational risks should be managed through operational risk registers, thereby ensuring the strategic risk registers are focused at the strategic level.

We also noted that risks had not in all instances been clearly articulated, which then poses the issue of 'how do we really know what we are seeking to manage?'

Risk evaluation

Risks contained within the strategic risk registers in our sample identified impact and likelihood, which of course is vital to understanding how risks should be managed. All of the force and PCC risk registers utilised some form of risk severity evaluation. 61 per cent had utilised 5 x 5 matrices (see examples in figure 3) and 36 per cent utilised a 4 x 4 model (see figure 4).

		Likelihood				
		1 Unlikely	2 Possible	3 Likely	4 More likely than not	5 Probable
Impact	5 Catastrophic	Medium-high risks 5	Medium-high risks 10	High risks 15	High risks 20	Critical risks 25
	4 Significant	Low-medium risks 4	Medium risks 8	Medium-high risks 12	High risks 16	High risks 20
	3 Moderate	Low risks 3	Medium risks 6	Medium risks 9	Medium-high risks 12	High risks 15
	2 Minor	Low risks 2	Low-medium risks 4	Medium risks 6	Medium risks 8	Medium-high risks 10
	1 Insignificant	Low risks 1	Low risks 2	Low risks 3	Low-medium risks 4	Low-medium risks 5

		Likelihood				
		1 Unlikely	2 Possible	3 Likely	4 More likely than not	5 Probable
Impact	5 Catastrophic	Medium-high risks 15	Medium-high risks 19	High risks 22	Critical risks 24	Critical risks 25
	4 Significant	Medium risks 10	Medium-high risks 14	Medium-high risks 18	High risks 21	High risks 23
	3 Moderate	Low risks 6	Medium risks 9	Medium risks 13	Medium-high risks 17	High risks 20
	2 Minor	Low risks 3	Low risks 5	Medium risks 8	Medium risks 12	Medium-high risks 16
	1 Insignificant	Low risks 1	Low risks 2	Low risks 4	Low risks 7	Moderate 11

Impact	Catastrophic 20	20	40	60	80	100
	Major 15	15	30	45	60	75
	Moderate 10	10	20	30	40	50
	Minor 5	5	10	15	20	25
	Negligible 2	2	4	6	8	10
		Rare 1	Unlikely 2	Possible 3	Likely 4	Almost certain 5
		Likelihood				

Figure 3: Example 5 x 5 risk evaluation models

Impact	Likelihood			
	1 Low	2 Medium	3 High	4 Very high
4 Very high	Green 4	Amber 8	High 12	High 16
3 High	Green 3	Amber 6	High 9	High 12
2 Medium	Green 2	Green 4	Amber 6	Amber 8
1 Low	Low 1	Low 2	Low 3	Low 4

Likelihood	Impact			
	1 Low	2 Medium	3 High	4 Very high
4 Very high	Amber 4	Amber 8	Red 12	Red 16
3 High	Green 3	Amber 6	Amber 9	Red 12
2 Medium	Green 2	Amber 4	Amber 6	Amber 8
1 Low	Green 1	Green 2	Green 3	Amber 4

Figure 4: Example 4 x 4 risk evaluation models

There is some variation in the models and risks scoring approaches utilised by forces and PCCs.

When considering those critical / red risks only, whether adopting a 5 x 5 or 4 x 4 matrices approach, high risks accounted for 25 per cent of all risks within the strategic risk registers in our sample.

Whilst there are examples of all risks being scored as high these were few. Most had much more of a mix of high, medium-high, medium, medium-low and low risks. This indicates due consideration to the evaluation process, which is important to ensure that risks get the right focus.

Some of the matrices were very clear in illustrating risk tolerance level, demonstrating what is below and above risk appetite.

Good practice and areas of improvement

- Whilst risk identification is of course important, there needs to be clear ownership. Risks should have a dedicated senior lead (such as the Chief Finance Officer) and ideally a responsible forum (such as the Chief Officer Group). This ensures responsibility and ultimately, that accountability measures are in place.

- Some forces and PCCs trace risk movement, incorporating anticipated direction of travel and future levels of risk exposure. As part of this process heat maps can be useful to map risks pre-controls (inherent), to post-controls (residual) and in utilising a long-term heat map, mapping current risk (residual) to their target position.

  When mapping risks to future direction it is useful to set out those key actions that will enable achievement of the anticipated risk scoring reduction (or further manage any risks that are anticipated to become more severe).

  Key to scoring any risk is understanding the descriptors that guide decision making. For some forces and PCCs this is clear and articulated well.

- Assurance is a key factor in the management of risk, especially given the majority of realised risk is a result of failure in the key control environment. In this case assurance is the level of confidence that can be obtained in connection with the on-going effectiveness of the key control environment in the management of risk. Too often there is an assumption that the controls identified in a risk register are effective and that the residual risk exposure is acceptable or within risk appetite. However, without firm evidence that this is the case then a force or PCC may be unknowingly exposed to a higher level of risk.

  Mapping assurances to key controls provides a way and means of making visible what evidence can be relied upon to provide the confidence required that the key controls are effective. This can include the assurance source, the timing of assurance and assurance provider ie management or a third party. These are often broken down and described as the 1st, 2nd and 3rd lines of assurance. The assurance mapping exercise will enable management to determine where there may be assurance gaps, or the current assurance provision may need strengthening.

  We have found through our risk management work in all sectors that the assurance map can substantially assist the Audit Committee (or equivalent) in gaining oversight of the key control environment, inform scrutiny of risks and controls, help with determining the deployment of risk mitigation resources and increase the ownership of risk management amongst those responsible.

- In managing risks, it is beneficial to set out and identify areas where change is anticipated, together with the associated level of risk this poses. An example of this would be whether financial performance is expected to be on plan. As well as identifying current risks, which are linked to objectives, the risk management process should identify future risks as well as opportunities. This is an area where there is room for further enhancement.

Concluding comments

The challenge for forces and PCCs is to ensure that risk profiles and risk 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 so that the Force / PCC can take comfort in the knowledge that controls are indeed operating as intended. Risk registers need to be subject to regular review, have allocated owners and appropriate oversight. 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.

AUTHORS

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

Suzanne Rowlett

Senior Manager, Risk Assurance

E suzanne.rowlett@rsmuk.com

Emma Griffiths

Risk Assurance Technical

E emma.griffiths@rsmuk.com

Marketing enquiries:

Claire Smallman

Business Development Manager

E claire.smallman@rsmuk.com

rsmuk.com