Audit, Scrutiny and Risk

Centre for Governance and Scrutiny

March 2024

77 Mansell Street, London E1 8AN

info@cfgs.org.uk / @cfgscrutiny

About the Centre for Governance and Scrutiny

CfGS exists to promote better governance and scrutiny, both in policy and in practice. We support local government, the public, corporate and voluntary sectors in ensuring transparency, accountability and greater involvement in their governance processes.

Governance and scrutiny are essential for the successful working of any organisation. Now, more than ever, trusted decisions are needed. We believe that decisions are better made when they are open to challenge and involve others – whether that's democratically elected representatives, those affected by decisions, or other key stakeholders.

At the heart of better governance and scrutiny are the right behaviours and culture. Our work champions these relational aspects and designs the structures to support them, leading to more effective decision-making and improved outcomes for organisations and people.

https://www.cfgs.org.uk/

Contents

Introduction

This publication is intended to support members of council audit committees, and members of council scrutiny committees, to:

- Understand the key elements of risk management, and the questions that can be asked of other members and officers at the council to bring challenge and support to risk management practice;
- Understand the specific roles of the audit committee, and of scrutiny committees, in challenge and support relating to risk management;
- Develop a blueprint for the collaboration between audit and scrutiny functions, to ensure a seamless and consistent approach to member oversight in this area.

1. What is risk?

Why risk is important in the design and delivery of services

Effective risk management is central to a local authority's ability to function properly.

Councils' work is inherently uncertain. We don't know for sure what adverse events, or issues, might materialise – and what their impact will be, if they do, on the delivery of our objectives. Carrying out research to better understand, and anticipate, these issues help to put in place plans to mitigate them – either to prevent them from happening altogether or lessening their impact if they do happen. Understanding risk also helps to inform better decision-making. It helps to make better choices between different options – where the relative risks of competing options in delivering outcomes are a crucial part of councils' evidence base.

Many councils are being driven – because of financial circumstances, the need to be more responsive to local people's needs, a shift in political priorities or by other objectives – to reassess the way that services are designed and delivered. Underpinning this change and transformation needs to be a realistic understanding of risk, informed by professional and political judgement. Failing to have regard to risk makes it more likely that changes will have unintended, unexpected consequences, and that they will not deliver the improvements (and/or savings) that policymakers and decision-makers expect.

Risk management is a dynamic activity. It is not about "deciding not to do something because the risk is too great", but about understanding the nature of a risk with a view to doing something to reduce, or mitigate, that risk. Because of this one of the most important aspects of risk management is *understanding the nature of a risk, in the first place*.

This should be informed by an understanding of risks in general – in particular, the different kinds of risks that councils face.

Different kinds of risk

Different councils categorise risk in different ways – the categorisation given below should therefore not be seen as conclusive. It is intended to give a framework to those coming to the subject as non-experts, to manage what might otherwise be a complex web of different kinds of factors. It is based on the HM Government "Management of risk in government" framework, produced by and for central Government non-executives[1].

Before we dig into these we need to briefly cover the importance of how risk is framed. The central issue here is whether the council is looking at risks institutionally (ie, how will this risk affect *this organisation* and how can we mitigate that effect) or from a community point of view (ie, how will this risk affect *the area and our residents* and how can we mitigate that effect). To be comprehensive, risk management needs to frame risks in a way that takes account of both of these dynamics.

A categorisation of risk

External risks	These are risks that may materialise because of wider national or global trends, and over which the council may have little to no control. Here the emphasis may be on anticipating these risks and having plans in place to mitigate their effects, rather than putting in place preventative action. Some of these issues may be managed and/or mitigated through the architecture put in place by the Civil Contingencies Act 2004. These cover short term "incidents" (extreme weather events, terrorism, cyber attack) and medium to long-term issues and trends (pandemic, recession, climate change)
Internal risks	These are operational risks within the control of the council – they may be issues specific to the local area and/or the authority itself. They are likely to relate to the operational delivery of services – the continuation of "business as usual" activity, and will usually be picked up and managed at that level, by managers working in the services involved. These may include staffing issues (high numbers of vacancies, staff turnover) in-year budget pressures (high demand, an inability to meet

[1] https://www.gov.uk/government/publications/management-of-risk-in-government-framework (Accessed 14 March 2024)

	income targets), or other service challenges (adverse public reactions to proposed council actions, poor performance of an external contractor)
Strategic	These are risks about the long term vision and ambition of the organisation – matters that relate to the administration's political vision, but also major change and transformation (for example, substantial shifts in the organisation's operating model). These kinds of risk may be closely related to the internal category described above. However, while they may be internal to the council, they have far-reaching consequences – they may therefore reflect the way that a mixture of related operational risks impact on a council's overall purpose and objectives. Risks here may relate to the ability of the council to deliver within a specific timeframe, or risks that the vision is not properly resourced, or that the way it is delivered has not been properly described.
Project based	There are likely to be a handful of projects on which a council is engaged that are sufficiently important that risks relating to them could have a corporate impact.

There may be risks that straddle two or more of these areas – for example, the unexpected closure of a large local employer may straddle the "internal" and "external" categories.

How risk is understood and assessed: impact and likelihood

The conventional (and, in local government, by far the most common) way to understand and assess risk is through a risk matrix.

The successful use of such of a tool is underpinned by the presence of a strong culture of risk management, which is discussed later in this paper. Because of this, the use of a risk matrix is not uncontroversial. The analysis of risk should be informed by evidence but this analysis will require subjective judgements. The use of a matrix, as described below, presents the result of this exercise in a quasi-scientific way, which could lead observers to assuming a level of objective rigour that might not be present. When considering the accuracy and sufficiency of mitigation, members and officers will need to satisfy themselves about the accuracy of the judgements made as part of this process.

The parameters that define how a risk matrix is used will need to be overseen by members – this will usually be a job for the audit committee.

A risk matrix should:

- Accurately describe the risk;
- Assess the likelihood of the risk materialising, and assign a numbered rating between one and five that describes this likelihood;
- Assess the impact of the risk, should it materialise, and assign a numbered rating between one and five that describes this impact;
- Set out a "score" for the risk that is these two numbered ratings multiplied together;
- Set out the mitigation being planned, and undertaken, to reduce impact and likelihood;
- Set out a revised "score" based on this mitigation being in place.

Risk should be identified at sufficient granularity to be meaningful to the organisation, and to maximise the opportunity for that risk to be managed. This may involve certain major risks with a national or global scale – such as a future pandemic – being broken down into risks that a council can do something about, and that reflect how that wider risk will play out at the local level.

The task of identifying, describing and assessing the risk will be undertaken by, and on behalf of, the person who "owns" that risk. This will usually be an officer – the seniority of the designated officer will depend on the risk itself. Members may also own particular risks (and will retain political accountability for risks generally).

An important part of this process is that the categorisation of risk allows for certain risks to be "escalated". For example, where a risk scores highly and cannot easily be mitigated, or attempts at mitigation for an ongoing risk aren't having the required effect, or a particular risk is materialising, it can be "escalated" to more senior officers, and to members, to "hold" and make decisions on. There are certain risks that may be of such importance that they are regularly considered by a council's corporate leadership team or its Cabinet. As we will cover in subsequent sections, the audit and scrutiny functions may also have a role in overseeing the management of these kinds of risk.

Describing the risk

- Understanding and accurately describing the nature of risk is the most important part of risk management. Members and officers will want significant assurance that risks are described in a way that is informed by evidence – and that all risks relevant to an issues, challenge or objective have in fact been identified. Councils should have a recognised and consistent way to identify, understand and describe risks which should be visibly consistent across all risk management material.
- Once a risk has been described, ownership of it should be assigned to a named individual, who will be responsible for the remainder of the activity involved in categorising, and mitigating, the risk.

Assessing the impact and likelihood of the risk

- The impact of the risk will usually be ranked between 1 and 5, where 1 means a negligible impact, and 5 means an impact that is catastrophic. The likelihood of the

risk will be ranked similarly, with 1 meaning "very unlikely" and 5 meaning "very likely". The parameters governing what terms are used, and how they are defined, is particularly important and should be set out in the council's risk strategy. Oversight of this is part of the role of the audit committee.

Assessing the likelihood of the risk

- The risk will usually be ranked between 1 and 5, where 1 means "very unlikely" and 5 means "very likely" – again, different words may be used.

Calculating a combined score

- Multiplying the two numbers together will give a score out of 25. Often, organisations will apply a threshold, over which detailed, active plans to mitigate are required – this will often apply to any risk scoring 12 or above (or the number may be 15). This is not to say that plans for mitigation should not apply to other risks – just that managers, and others in a position of oversight, are most likely to need to have reported to them the plans for mitigation of risks that sit beyond this threshold.

Management

- The risk's owner should – where necessary – design and describe a plan to mitigate the risk. This might be action that is planned, that is in train, or that has already been taken, or a combination of all three.
- A risk may also be managed by being transferred to another person. The most common method of doing this is through insurance, but a council may seek to transfer a risk to another organisation. Of course, the fact remains that even if a risk has notionally been transferred in this way, actual accountability for failure (if it arises as a product of a risk materialising) is still likely to sit with the council.

Calculating a revised score

- The presence of mitigation may allow the overall score – once recalculated – to fall below the threshold for further mitigation. If it does not, that suggests that the mitigation is not sufficient, and that either plans need to be revised, or – more likely - that further mitigation is not possible. In this case, the owner (and others) will need to actively engage so that, should the risk materialise, it is immediately identified so that what action *is* possible can be taken.

Risks are usually presented together in registers – tables that summarise individual risks, and often group them together by theme, for the benefit of senior managers and others exercising oversight. We will discuss risk registers (and how they usually operate in local government) in the next section. However, there is a danger that a focus on the aggregation of risks in registers – and the consequent focus of risk management as being about "the management of the risks in risk registers" – obscures the obligation to think about risk as a factor in decision-making, and in long-term planning. Members, both those on audit and scrutiny committees, should therefore expect to see that risks are referenced in other reports

in a way that aligns with risk registers, and that this happens in a way that reflects members' oversight roles. For example, members should expect to be able to see how the presence, impact and likelihood of given risks is being affected by a particular decision (and how decision-making on a particular issue is informed by those risks).

Different kinds of control

In section 4, we go into more detail on the "ownership" of risk, and members' and officers' roles. In section 3, we go into detail on the respective roles and audit and scrutiny. Before doing this it is important to set out the overall environment of controls within which these roles sit.

Control is usually described as sitting around three "lines of defence" in which:

- The first line is management controls – officer interventions that will usually be sufficient to manage most risks at an operational level;
- The second line is corporate oversight – the duties held by corporate management bodies, by the internal audit function and by members – on the audit committee and scrutiny committees, and on Cabinet;
- The third line is independent assurance. This will usually relate to the outcome of inspections and the advice, or directions, given by the external auditor.

These arrangements will be described in the local code of governance, with the council's Annual Governance Statement being used to set out an assessment of the arrangements' effectiveness.

2. The respective roles of audit and scrutiny

Although at its heart risk is about the description, categorisation and mitigation of risk, in truth there is a significant amount of work that needs to sit around and support this role.

This section explores what systems should exist to oversee this support, and where and how this task can be carried out at member level.

It also explores the practical issues that will need to be worked through in order to ensure that audit and scrutiny's respective roles are mutually understood, and that they fit within the wider authority's risk management framework.

Agreeing complementary tasks and functions

There is – and should be – overlap between the audit and scrutiny functions. However, without co-ordination, this can lead to:

- Duplication. The two functions may end up trying to carry out the same work. So both scrutiny and the audit committee might end up regularly reviewing risk registers, or (worse) trying to investigate individual risks in a way that is not co-ordinated;

- Gaps. Key, member-level oversight and challenge of risk management may not be carried out at all, because neither audit or scrutiny function considers certain tasks to be within their purview.

In our publication "Audit committee and scrutiny committees: working together" (CfGS, 2021), we set out what we saw as the main components of joint working between the three functions on the oversight of risk management.

- Assurance on governance of risk. This is about strategic oversight of the framework. It will involve developing familiarity with where leadership and responsibility lies on risk, and action on risk culture. Member action here will generally be led by the audit committee;
- Reviewing the risk profile. Understanding where and how strategic risks are emerging and being managed is an important audit committee task, but scrutiny has an important role in gauging the impact of risks' materialisation from a policy perspective – understanding the impact on the ground and if assumptions made about certain risks are accurate;
- Monitoring the effectiveness of risk management arrangements, in part by reviewing the treatment of specific risks "by exception". Members action here will be usually led by the audit committee. However, it is likely that scrutiny can, through wider reviews of policy development, integrate an awareness of risk management into its work – ensuring that audit committee can be supported with a grounding in what is likely to constitute the most efficacious approach to understanding evaluating risk management arrangements.

Planning how the relationship will work relies on having an understanding of the respective roles of the audit and scrutiny functions.

Audit	**Oversees systems, processes and controls** **Do we have the right systems in place?** **How can we assure ourselves that those systems are working?** Audit looks at questions like: • How can we assure ourselves that we have a "risk management culture" in place – a set of behaviours that support an approach to risk management that is honest and rigorous? • How do those with duties relating to risk communicate with each other to ensure that they have a shared understanding of the key issues? • Overall, how confident are we that there is a process in place to assign ownership to specific risks? • How confident can we be that the risk management systems that we have are identifying and escalating the "right" things to be dealt with by senior officers, and members?

	Audit may also look at the way that the most significant individual risks have been treated and managed, and check that the right evidence has been used to categorise and describe that risk. The committee will usually review this information based on the existing risk score, and may change the risk score, in light of their analysis. Audit will also direct a work programme for the internal audit function that is informed by risk.
Scrutiny	**Oversees policies, and outcomes** **Are the outcomes that we are trying to deliver, deliverable?** **Are they, therefore, the right outcomes?** Scrutiny looks at questions like: • How does our culture of risk management influence and inform our overall priorities – how are we using our appetite for risk to determine what we should, and should not, be doing? • Where, and how, do different politicians', and different officers', approach to and understanding of risk diverge? What is the implication of that divergence, where it exists? • How do members, and officers, in decision-making roles account publicly for their decisions? How does scrutiny know where political, and operational, choices have been made in a way that is informed by an understanding of risk? Have decisions been made with appropriate consideration of current and future risks? • What lessons have we learned from specific events, or series of events, that have had adverse consequences? How have these lessons informed our approach in the future? Scrutiny may also look at the policy implications of specific risks should they materialise – and the policy implications of putting certain mitigations in place. Scrutiny's own work programme should be informed by risk – by exploring policy options and priorities in service areas where the council may be particularly exposed to risks. This may be particularly important where the council is exposed to external risks, such as high demand – or internal risks, such as a fragile financial position.

3. A practical model for joint working

This section works through some practical examples of what joint working might look like. This is about planning and communication – both audit and scrutiny having a shared understanding of what their mutual roles are. It is also about acting proportionately. Proper joint working requires trust that the system is working properly and that the information that the system provides to members is accurate. This is why the first step is to baseline an understanding of those systems, and subject them and the assumptions that underpin then to scrutiny.

Once this has happened, and once there is agreement about audit and scrutiny's mutual roles, the main focus for co-ordination will be regular conversation between the chair of the audit committee, and the chair of the relevant scrutiny committee – this might be a dedicate finance, or resource, overview and scrutiny committee, or a "co-ordinating" or overarching scrutiny committee.

The process should not involve the convening of joint audit/scrutiny meetings involving a lot of members and officers, or the formal circulation of identical reports and information to both sets of members. However, it should include regular, more informal, co-ordination between the respective committee chairs.

Step 1: Baselining an understanding of risk management systems, and the organisation's risk culture

First, it will be important for the audit and scrutiny committees to independently, and together, determine whether the right managerial and political systems exist for the monitoring and escalation of risk.

If those systems exist, audit and scrutiny can each design a role for themselves which is proportionate, and which relies on the right issues being escalated for member consideration at the right time. They can also work to ensure that, overall, the council is identifying and dealing with emerging risks appropriately.

If audit and scrutiny consider that risk management processes do not meet their expectations – for example, if ownership is muddled, if systems feel like they are interpreted differently by different parts of the council, if the identification and categorisation of risk feels subjective and lacking in consistency – then one or both functions might want to delve into *the system* in more detail.

For example:

- Audit might want to undertake a desktop exercise to understand how risks are managed through the system, to identify points of weakness and uncertainty, and work with the Head of Internal Audit, s151 officer, Monitoring Officer, Head of Paid Service and Cabinet to strengthen systems;

- Scrutiny might want to "dip test" the policy landscape around individual, systemic risks, by considering them as items on scrutiny agendas. In doing so, scrutiny may be able to identify risks that may not yet have been conceptualised, or reframe the council's thinking on other risks.

Through this activity both audit and scrutiny can work together to support officers, and executive members, to improve the risk management systems of the council.

While audit technically "leads" on this activity, scrutiny has a stake too – because those risk management systems involve challenge on political priorities, where the answer to "what is a priority" is informed by the administration's understanding of what the greatest risks are.

For example, an administration seized of the need to act to mitigate and adapt to the risk of climate change might want to take a range of steps in planning and economic development policy – and transport policy – that reflect their perception of the size of that risk. Scrutiny is able to look into the evidence informing that decision, and the risks associated with alternative decisions and solutions.

Integrating an understanding of risk in the audit and scrutiny work programmes

Once audit and scrutiny have some justified confidence in the quality of the systems in place, risk registers can be used to inform the content of work programmes.

- Audit might want to perform a role in regularly testing the processes in place around the most significant risks affecting the council;
- Scrutiny might use an understanding of risk to prioritise their own work – possibly informed by audit's process-based analysis. For example, the audit committee might consider that a weakness in the authority's understanding of risk relates to a possible misunderstanding of the preferred outcome of a certain policy (for example, because there is not compelling evidence of local need, or because it may be unclear why a certain thing has been prioritised).

Step 2: Periodic formal review at Audit Committee

On a regular basis the audit committee will:

- Review risk registers, and risk heat maps;
- Undertake planned reviews of individual projects, and programmes, and issues, that present major and systemic risks. These may be risks that have already been agreed as ones requiring this oversight;
- Review and oversee the effectiveness of the risk management strategy and framework itself (with this probably being a periodic activity carried out to inform the Annual Governance Statement).

Step 3: Periodic informal review by Audit and scrutiny committees

Outside committee, both audit and scrutiny will want to liaise to ensure that emerging issues are dealt with properly.

The Chair of audit and the chair of the relevant scrutiny committee (usually a "main", co-ordinating or "corporate" scrutiny committee, or the scrutiny committee with lead responsibility for corporate finance and resources) might want to meet informally every couple of months to:

- Check and align their work programmes;
- Consider any emerging issues which might need to be escalated.

This conversation would be informed by considering corporate and departmental risk registers, with the s151 officer, officers with skills in risk management, and possibly the Monitoring Officer.

Where those chairs consider that:

- A critical risk is materialising;
- A risk with high impact and likelihood exists and while mitigation plans are present, those plans may not have been put in place or may not sufficient to "treat" the risk sufficiently;

Then it might be appropriate to escalate that risk to committee for detailed consideration.

Step 4: Investigation of specific escalated risks

Escalation: process and substance

This is a "by exception" process, and is not something that we think would affect more than a few risks a year. Depending on the nature of members' concerns the risk could be considered by audit, or by scrutiny. We would not necessarily recommend the convening of joint meetings because it is important to keep the duties of the key sets of committee distinct, for regulatory reasons.

Drawing in evidence to support formal consideration at a scrutiny committee, or audit committee

Members could draw in evidence from:

- The member and/or officer "owner" of that risk;
- Frontline officers, and others with technical knowledge of the service or issue in question;
- Council partners who might be impacted by the risk;
- Potentially (and certainly in respect of scrutiny investigations) service users, or others affected by a risk materialising.

In order to participate in a discussion about:

- The overall nature of the risk;
- Whether the risk is described in a way that everybody understands, and everybody agrees with;

- Whether the impact and likelihood of the risk materialising are what the council thinks – and the various perspectives and assumptions that sit behind that judgement;
- What mitigation measures could be designed and put in place that look different to what exist now;
- If mitigation is not possible, how the situation might be recovered;
- How members wish to monitor the situation.

In essence this is about performing the process of assessment of the risk in a public space, with a wider cohort of people, in order to test the council's assumptions and in order for the member body to refine the council's understanding.

5. Questions for members to ask that relate to specific areas of risk management

This section explores some of the more detailed aspects of risk management (introduced in the previous sections) and sets out some questions that might be asked in relation to each.

Who asks those questions – audit, or scrutiny – will depend on how the tasks of the two bodies are shared, as set out in the section above.

<u>The impact of culture and behaviour on risk management</u>

Risk management looks objective and scientific but we should be sensitive to the possibility that it can be driven by bias, unquestioned assumptions and preconceived ideas.

Where an organisation requires staff to conform with an array of risk management methods without thinking about the purpose of those methods, the result can be a compliance-driven approach where the process and mechanics of risk management are present, but without a meaningful culture to support it. In this world, risks are managed on paper, but not in practice.

Both audit committees and scrutiny committees have an important role to play here. Firstly, they can assess the extent to which the authority has a positive risk culture – they can dig into the attitudes, behaviours and assumptions of other members, and staff. Secondly, they can play an active part in that culture itself – by exercising member leadership, promoting positive behaviours around risk and being part of an environment where weakness, and the risk of weakness, is quickly acknowledged and acted on.

Although "risk culture" is a theme covered extensively in the management literature – we provide links to some key documents in the bibliography – much less time is spent in thinking about risk culture in a political environment. Here, the presence of councillors can have positive and negative consequences:

- Positive, because councillors have a direct connection to local people and can bring this experience to bear – councillors also have the credibility, legitimacy and duty to challenge (in public) assessments that the council has made on risk, through scrutiny committees and audit committees, in a way that is arguably broader and deeper than non-executives in other organisations;
- Negative, because the political dynamics that come into play in these discussions might dissuade people to be candid in formal, public meetings when talking about live risk issues.

To be part of a strong, positive and challenging risk culture, councillors will need to think about their role *within* that culture, not as overseers of it or people looking in from outside.

Building a risk management culture

A risk management culture is, at its heart, a culture of candour and frankness. It is one where an appropriate approach to risk management is led from the top, and involves everyone – not just professionals with a specific technical risk management duty.

A positive risk culture is a positive organisational culture. It is one where information is shared freely and honestly – including where information highlights weaknesses and shortcomings. It is one where risk is understood, and acted on appropriately. It is one in which accepted opinion is challenged through the presence of many different perspectives – with those perspectives often being brought by members sitting on audit and scrutiny committees.

Communication and consistency

Councils need a clear and consistent framework to ensure that everyone with duties around the identification and management of risk understands those duties, and is able to carry them out consistently. A failure to do this will mean that gaps, and duplication, are likely to emerge. It also makes it more likely that councillors will see a need to "reach in" to the operational management of service-based risk.

A framework like this will determine who owns specific risks, who is responsible for designing and deploying mitigations, and who takes charge in the ongoing review and revision of plans for when and how to use those mitigations. A framework like this will also make clear who is responsible for developing, and agreeing, the authority's risk appetite – a critical task that we describe in the section below.

Officers and members need to work together to frame, and understand, the nature of risk. Into this work officers will bring their professional expertise, and technical knowledge of the issue in question. Members will bring their political perspective and judgement.

Questions to ask about culture and communication

- How can we assure ourselves that members and officers have a shared understanding of the importance of risk management, and its key components?
- How do mechanisms like the Annual Governance Statement validate that?
- How do we use external mechanisms – the judgement of our external auditors, assessments by CIPFA, reviews carried out by the LGA – to provide independent assurance of our mindset and behaviours with regard to risk management?
- How does our risk management framework spell out the shared responsibilities of officers, and of members?
- How are risks investigated within our governance arrangements?
- How do we manage the implications of risk that we have sought to transfer to other organisations to hold, whether that be through insurance or contract?
- How do we deal with cultural barriers – instances where officers (or executive members) might challenge risk management action?
- How do we ensure that we are capturing all the risks that the authority might face?

Building capability

Members and officers, in all roles, need to support each other to develop the skills and capabilities they need in order to perform their roles. Officers have an important role in supporting members to understand some of the technical features of risk management – but members can help officers to better understand the political dynamics within which they operate and can bring an understanding of local communities as well. Both of these things will significantly affect professionals' assessment of the impact, likelihood, and mitigations around specific risks.

Scrutiny can play a role here, by challenging and questioning the evidence and assumptions officers use to form the basis of their risk management activities.

Questions to ask about capability[2]

- What are the key roles within the council that bear responsibility for risk management?
- What are the skills profiles of the roles holding those responsibilities?
- How can we be sure that we have learning and development arrangements in place to ensure that people have the right skills, and that those skills are up to date?
- What are our succession planning arrangements for these key roles?
- Beyond people in key positions of responsibility, how do we ensure that members generally, and officers generally (especially those with management and budgetary

[2] We ask related questions – on ownership, and leadership on risk – in the section below.

responsibility) have the skills and mindset necessary to understand, and to be proactive, on risk?
- To what extent do officers have a grip on the political risks, as well as the practical risk, that impact on the services for which they hold responsibility?
- How do we handle multiple different (conflicting) priorities when dealing with risk across the organisation, and across the wider community?

Learning lessons and debriefing from adverse events / experiences

After adverse events, it is usual to debrief – to understand the experience and take action to improve as a result.

This form of "washup" or post-hoc analysis is fairly common for traditionally delivered projects. It might also be common for risks which can be said to have played out – perhaps because they relate to a specific event or issue, such as a major cyberattack.

But many risks do not materialise in this way – they are ongoing, and shift and change over time. There may not be a moment at which a risk – as an event – can be said to have passed, and to have been dealt with. This means that review of mitigation, and of the continued presence of the risk itself, needs to be more dynamic. The act of learning lessons needs to be part of a more iterative approach, in which members and officers work together to understand what is happening, whether management of risks in given areas is appropriate and delivering the expected mitigations, and what might need to change in consequence.

There is an important role in learning for both audit and scrutiny committees.

Questions to ask when debriefing

- How did we initially identify that this risk was materialising?
- How did we identify the impacts that the risk was having, and how did they compare to the impacts that we predicted?
- How well did our existing plans to mitigate the likelihood of the risk help us?
- How well did our existing plans to mitigate the impact of the risk help us?
- How did the risk evolve over time? How did we adapt our plans accordingly?
- What were the implications for business continuity, and how did we deal with those impacts?
- Who was involved in mitigation activities, what did they do and how did plans and activities adapt to accommodate an emerging situation?

<u>Leadership, ownership and accountability overall</u>

Risks have to be owned, and owners should:

- Be held to account for their work in understanding, and mitigating, those risks;

- Hold others to account for their own role and responsibility in that activity – and for related activity on adjacent risks.

Both individual and collective responsibility are important here. Named ownership of risk does not mean that one person and one person only has responsibility for managing and mitigating that risk – it is a statement of leadership, and the expectation will be that a range of people will need to play an active role.

Questions to ask about the ownership of risk

- How is political accountability for risk – held by the Council, Cabinet, the Leader (or by certain committees and their Chairs, under the committee system) assigned and understood?
- How is this political ownership shared with the strategic/operational ownership held by officers?
- How do key members, and senior officers, "lead" on risk?
- How do audit and scrutiny impact positively on good governance of risk?

Strategic risk management

In a local authority, ownership of risk is shared between elected members and officers.

Risk management is not an operational task, and as such elected members and senior officers will need to regularly not only consider aggregated information about risk, but will also need to set overall policy on it. An important part of this is the need to set risk tolerance, or "risk appetite".

Setting risk appetite

Risk appetite is defined by the Institute of Risk Management (IRM) as, "the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives".

The IRM's guidance paper, "Risk appetite and tolerance"[3] sets a number of key principles.

Principles underpinning risk appetite (IRM)

- Risk appetite can be complex. "Excessive simplicity, while superficially attractive, leads to dangerous waters: far better to acknowledge the complexity and deal with it, rather than ignoring it";
- Risk appetite needs to be measurable. For councils this means understanding their core drivers – the contents of their corporate plan, and the duty to deliver Best Value, are likely to be central here, and provide an opportunity to gauge where risk might lie in respective of those objectives;

[3] reference

- Risk appetite is not a single, fixed concept. Different appetites will apply in different circumstances, varying over time. We discuss this in more detail in the section below when we talk about risk management being dynamic in nature;
- Risk appetite should be developed in the context of an organisation's risk management capability. We talk about risk management capability in the section below – where officers and members understand their mutual roles and are comfortable and confident in those roles, a more sophisticated approach to risk might be taken that allows for a greater appetite for certain risks. Where capability is lessened, a clear-eyed understanding of that weakness may lead an authority to retrench;
- Risk appetite must take into account differing views at a strategic, tactical and operational level. This echoes what we said in our opening section about the different types of risk that exist;
- Risk appetite should be "integrated with the control culture of the organisation". When we talk about the "control culture", we talk about the need to take tight control of certain risks at operational level (children's services, health and safety – areas where risks are more easily quantified, replicated and managed), while at the strategic level there is more acceptance of risk (because of the uncertainty of some strategic choices and because strategic decision-making is informed by policy-based decision-making).

Risk management policy overall also needs to recognise and act on the fact that risk (and risk appetite) is dynamic. External circumstances may lead a council to reassess its appetite for risk – for example because financial constraints have tightened, or because of a significant event like a change in national Government.

Questions about risk appetite

- How have we arrived at a settled appetite for risk?
- How do we keep our risk appetite under review? What part do members, and officers, play in this ongoing activity?
- How do we draw different perspectives, and evidence from difference sources, into discussions on our risk appetite?
- To what extent does our risk appetite differ from directorate to directorate /service to service – on the basis of what evidence, and how does this impact on our corporate understanding of the risks we face?
- How are our policymaking choices informed by our risk appetite?

<u>Using risk registers and "heatmaps"</u>

In local government the use of risk registers is central to the management and oversight of risk. Risk registers bring together series of risks which are identified, understood and

mitigated using the "risk matrix" system we described in the section above. The use of risk registers is an important part of the regular, routine processes that are used to ensure that risk is being dealt with.

Councils will usually have both corporate risk registers (covering the whole council) and departmental risk registers (covering a specific service or directorate). Councils will also have risk registers for specific projects, and programmes (covered in more detail below).

The corporate risk register will usually cover systemic, cross-cutting risks and major service-specific risks whose management has implications for the council corporately.

Risk registers allow managers (and others) to take a general view of what risks are most important, and where and how they are being acted upon. Usually, individual risks will be coded red, amber or green, with those marked red being those with the greatest impact and likelihood and where insufficient plans for mitigation exist (or where meaningful mitigation is not possible).

Many councils will also use "heatmaps" to describe and categorise risks. Under this model risks are placed on a scatter-plot graph, with the most significant risks in the top right hand corner. This makes it easy to see, at a glance, where the most significant risks arise.

These tools allow the most significant risks to be identified and discussed in more detail by senior officers, and members. When we talked about risks being "escalated" for discussion this is the mechanism by which these happens – many councils will have standard operating procedures providing for "red" rated risks to be highlighted, discussed and overseen more regularly because of the impact they will have, should they materialise.

This material may be brought to the audit committee quite frequently – but often in the form of a generalised update. Members need to be clued in to the right questions to ask about what sits behind this information.

Questions to ask about risk registers (and the individual risks present in them)

- What are our "top" risks? What is their impact and likelihood of materialisation?
- Do we understand how our corporate culture informs our risk appetite, and also influences and informs the quality of our risk registers – positively and negatively?
- How likely is it that we have "blind spots" with regard to certain risks or areas of risk?
- With what frequency is the information in risk registers updated, and on the basis of what evidence?
- Are all the risks identified in the register clearly defined, and owned?
- How have trends in the identification and materialisation of risks been understood and dealt with (for example, clusters of high risk issues with insufficient mitigations; a particular risk or risks that have wider corporate implications);
- How are risks escalated between departmental and corporate risk registers, and how are particular risks escalated between, and from, these registers for more senior officer (and member) intervention?

- How do the risks we have identified connect to our key performance indicators (KPIs)? How do they impact on the delivery of the KPIs?
- How do they connect to our budget?
- Are we confident that mitigating action that we are taking, or that we propose to take (in respect of a particular risk), will have the impact that we expect and how will we test this? Are actions actually being delivered?
- Overall, how are we testing and learning from the accuracy, or otherwise, of our assessments on risks overall?
- Are we comfortable that the risk owner's assessment of the steps needed (and possible) to mitigate an individual risk reflects our organisation's risk appetite?
- Where intervention happens as a result of the escalation of a risk, what did it look like? *It might be appropriate for audit, or scrutiny, committees to play a formal role in the treatment and oversight of specific risks on a by-exception basis – if so, there should be a formal mechanism for this;*
- How does insight from operational risk management feed back in to our broader business strategy?

Risk as a component of programme and project management

Risk management is an important part of the wider discipline of programme and project management. Where council officers are designing projects (particularly when they are using traditional tools and methods to do so) they will need to articulate and deal with risks that may arise.

Questions to ask about programme and project management

- In determining the objectives / outcomes for the project or programme, how has an understanding of risk helped us to be realistic?
- How did we identify, and categorised, the various risks that arise in an individual project, and how has that suite of risks been integrated within our wider risk management approach?
- Do we have proper thresholds in place to manage the escalation of risk to an appropriate level, in a way that makes sense for wider project/programme governance?
- How did an understanding of risk help us to be more efficient in our programme management?