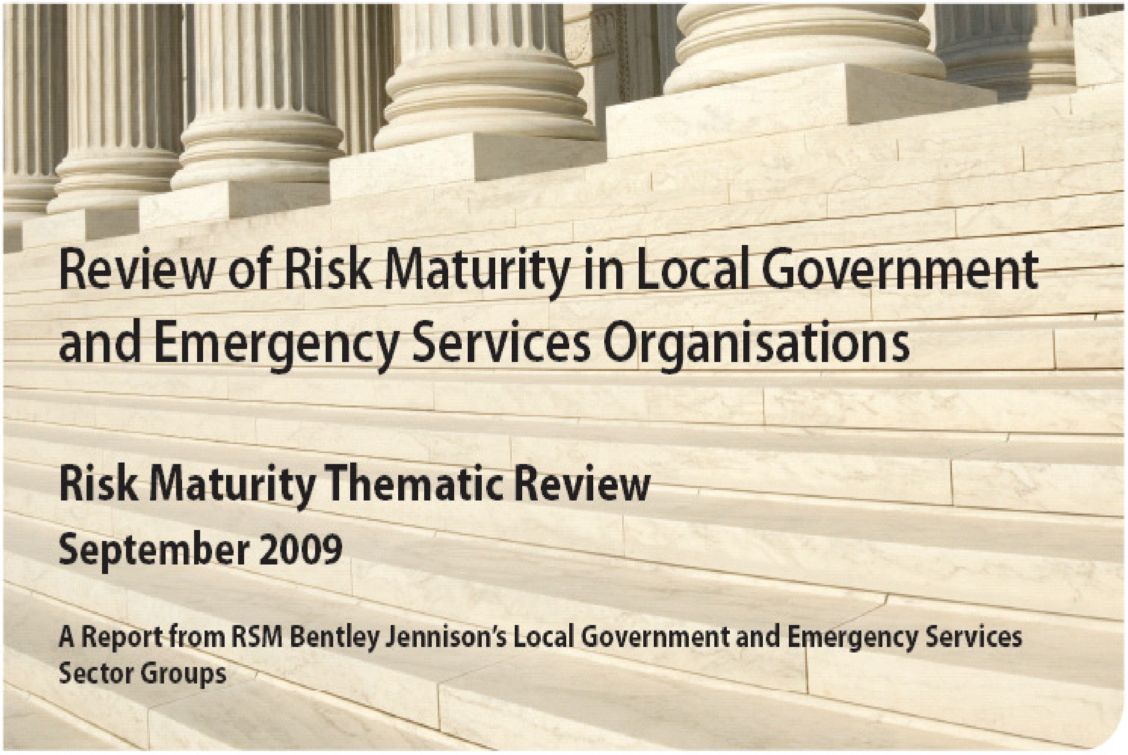
RSM Bentley Jennison



Review of Risk Maturity in Local Government and Emergency Services Organisations

Risk Maturity Thematic Review

September 2009

A Report from RSM Bentley Jennison's Local Government and Emergency Services Sector Groups

Intelligent Solutions

www.rsmbentleyjennison.com

Contents

Bentley Jennison Risk Management Limited
Bentley Jennison Risk Management Limited is wholly owned by RSM Bentley Jennison
Registered in England & Wales No. 3444889
Registered Office 1 Hollinswood Court Stafford Park 1 Telford TF3 3DE

IS YOUR ORGANISATION RISK MATURE?

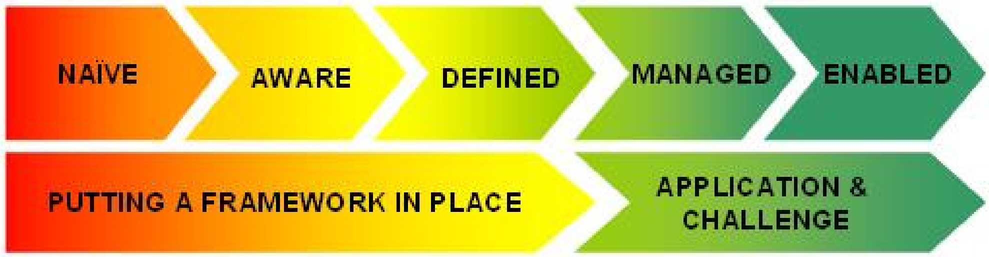
Risk management as a concept is not new, but just because it is familiar, does that mean it is effective?

Effective risk management is far more than being able to tick the boxes of the relevant guidance or standard. Accordingly, we are interested in how local authorities and emergency services use, report on and, above all, understand risk. There is much talk of risk maturity, but few have defined risk maturity fully. The Institute of Internal Auditors defines risk maturity as[1]:

"The extent to which a robust risk management approach has been developed and applied, as planned, by management across that organisation to identify, assess, decide on response to and report on opportunities and threats that affect the achievement of the organisation's objectives."

We have adopted this model as it is straightforward and applicable to any organisation, regardless of size or complexity. Put simply, the more risk mature an organisation is, the more it uses risk information to manage the business instead of simply putting a framework in place to record risks. However, getting the *right* framework in place is also important as this forms the foundation for the organisation to work from. Does the organisation really understand risk, does it think about missing opportunities as well as adverse risks and does it use that information to take informed decisions (and ultimately to even take risks in an informed way)? Therefore, the culture of an organisation and its attitude to risk is a key element of moving along the risk maturity spectrum.

The risk maturity model defines five stages of risk maturity:



A risk management framework is by definition "a surrounding support" and "a combination of parts". Therefore risk maturity is firstly dependent on the robustness of the framework put in place, but secondly on how that information is used to understand and reduce the risks facing the organisation.

[1] Institute of Internal Auditors, *The Role of Internal Audit in Enterprise-Wide Risk Management*, 2004 position statement

THEMATIC REVIEW

During 2008/2009 we undertook a review of risk maturity across a large proportion of our public sector clients. The purpose of the risk maturity review was to establish the extent to which organisations have developed risk management processes beyond putting a basic framework in place. The overall aim of the review was to gauge risk maturity across the participating organisations and to collate comparative information and examples of good practice and innovation to allow our clients to compare themselves against others in the public sector. This report sets out our findings for local authorities, police authorities and fire and rescue authorities (in both England and Wales). This review has been undertaken in a number of other sectors, and cross-sector findings will be published in our main risk maturity report later this year.

As part of the review we considered:

- The types of risk registers that are typically in place.
- Roles and responsibilities for risk management.
- How often and to whom risks are reported.
- How well risks and associated information are communicated.
- What local authorities and emergency service authorities perceive as their key risks.
- How organisations set their risk appetite and use this to support their decision making.
- What organisations do to make risk management work for them.

WHAT MAKES FOR GOOD RISK MANAGEMENT?

The following key features were visible in those organisations that are most risk mature:

- The profile of risk management.
- A risk management strategy that delivers value.
- Risk management directly informing and being linked to business planning.
- Use of risk management information systems.
- Non-performance is treated as a serious management failing.
- Internal audit and other assurance work is driven by the risk profile of the organisation.

Some of the best practices in risk managed and enabled organisations are set out below. These link to our wider client base rather than just to the local government and emergency services sector.

BEST PRACTICE: PROFILE OF RISK MANAGEMENT

- Outcomes from risk management are clearly defined.
- Risk appetite is defined.
- Consistent identification and risk measurement criteria.
- Roles and responsibilities of the Board / Authority, Management and Staff are defined, including internal audit and other assurance providers.
- The effectiveness of the strategy is subject to on-going review by the audit committee / non-executive directors. The outcome of the assessment is the basis of the annual report on risk management.
- At least twice yearly the Board or Authority will formally consider the key risks being faced by the business.
- The review will also involve non-executive directors.
- The business risk profile is a regular feature in reports to the Board.
- The Chairman of the Board or Authority will meet with the Chairman of the Risk Committee / Lead Non-Executive Director to discuss risk management matters and are encouraged to challenge the organisation's understanding of risk and its on-going management i.e. why is this a high risk? Or why has this been a high risk for so long (yet there has been no detrimental effect on the organisation)?
- Lessons learned exercises to establish why and how risks are realised and what changes / improvements are required in existing business processes to ensure this does not re-occur.
- There is a formal annual report on the management of risk by the business and actions required to enhance existing arrangements presented to the Board / Authority for consideration for adoption and implementation. This will include funding approval where required.

BEST PRACTICE: RISK MANAGEMENT IS LINKED TO BUSINESS PLANNING

- Risk Management actions required are integrated into corporate and business unit plans.
- Budgeting is informed by the cost of implementing risk management actions.
- Proportionality is essential to ensure best use of resources.
- Used to inform insurance methodology, including discussions with brokers.

BEST PRACTICE: USE OF RISK INFORMATION SYSTEMS

- Risk enabled entities have all implemented a risk management information system or are currently researching such a system.
- Used interactively with risk / audit committee and non-executives.
- Key features of the risk management information system include:
  - based on Turnbull (or equivalent) principles
  - ease of use (for business managers)
  - cost
  - national / global use
  - ease of reporting
  - risk controls assurance and task management functions

BEST PRACTICE: NON PERFORMANCE IS A SERIOUS MANAGEMENT FAILING

- Regular risk management action tracking is in place.
- Risk management is a key element of management performance appraisal.
- Business risks identified by staff can attract reward and recognition (not necessarily purely financial reward).
- The risk / audit committee, non-executives and / or risk management group have a clear role and remit in the management of risk.

BEST PRACTICE: INTERNAL AUDIT WORK IS DRIVEN BY THE RISK PROFILE

- Internal audit plan based on providing assurance over key risk controls, particularly where significant shift between inherent and residual risk profile.
- Regular review with risk manager of changes in risk profile so the internal audit plan can be updated.
- Assurance providers are identified and assessed for levels of confidence. Internal audit work is clearly mapped to the organisation’s key risks.
- Internal audit reporting is put in context of the risk management strategy when reporting to the audit / risk committee or non-executives.

PERCEPTIONS OF RISK MATURITY

During the review we have not only assessed what we consider to be organisations' risk maturity, but have asked managers, executive and non-executive board members for their perception of the organisation's risk maturity. Perhaps unsurprisingly, this did not always align with our findings.

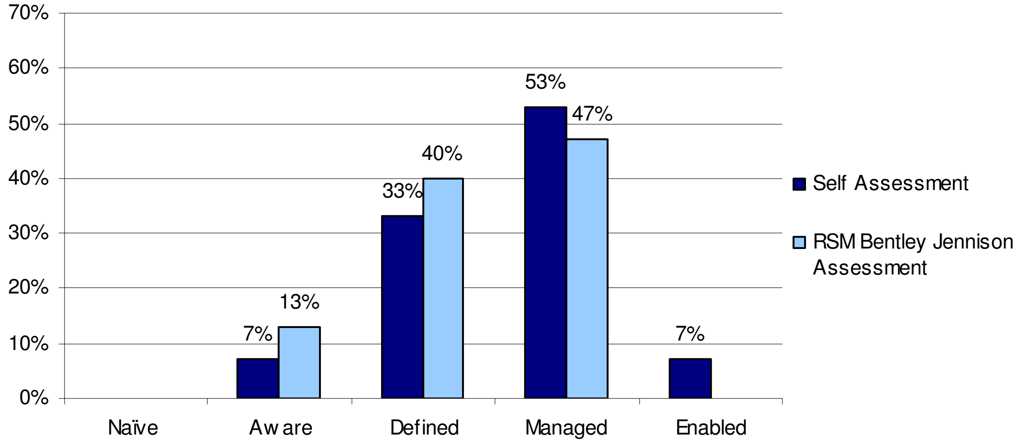


Chart 1: Assessment of Risk Maturity across Local Authorities and Emergency Services

Chart 1 shows a slight disparity between our assessment and organisations' self assessment. This is further analysed below where we analyse those organisations that consider themselves to be risk managed or risk enabled against our assessment of their risk maturity following our review at those organisations. Of those organisations that rated themselves as risk 'managed' or risk 'enabled', our reviews concluded that 78% were in fact risk 'managed'.

% for All Organisations	Our perception of risk maturity of organisations that thought they were risk managed
0	Risk Naïve
0	Risk Aware
22%	Risk Defined
78%	Risk Managed
0	Risk Enabled

We also asked those people interviewed about their organisation's target risk maturity. As expected, most organisations (73%) aimed to ultimately be risk 'enabled'. However, some had a more pragmatic view of aiming for risk 'managed' (perhaps reflecting the challenges that local authorities and emergency services organisations face such as making savings while also dealing with other challenges such as major organisational change management). Some bodies want to take incremental steps towards the overall aim of becoming risk 'enabled' at some point in the future and therefore risk 'managed' is their short to medium term goal.

The charts and tables below break down the findings for local authorities and emergency services.

LOCAL AUTHORITIES – PERCEPTIONS OF RISK MATURITY

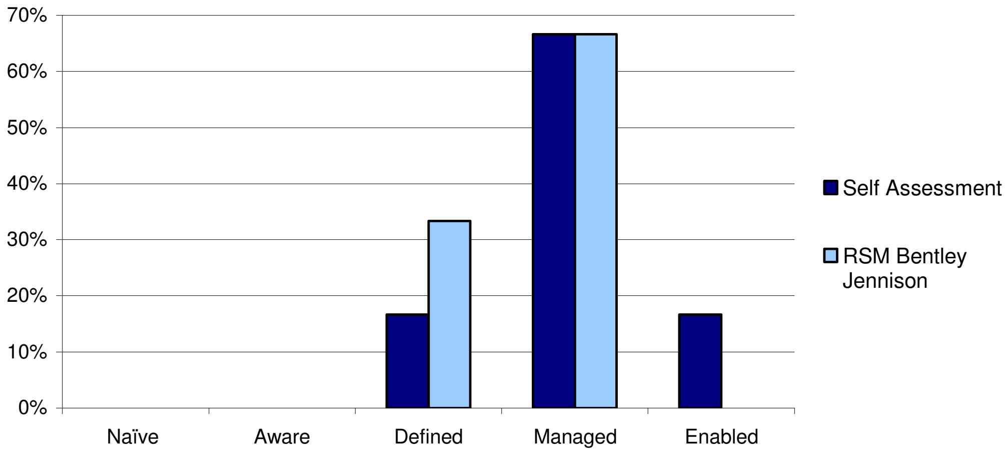


Chart 2: Assessment of Risk Maturity across Local Authorities

% of Local Authorities	Our perception of risk maturity of local authorities that assessed themselves as risk managed or risk enabled
0	Risk Naïve
0	Risk Aware
25%	Risk Defined
75%	Risk Managed
0	Risk Enabled

POLICE AND FIRE AUTHORITIES – PERCEPTIONS OF RISK MATURITY

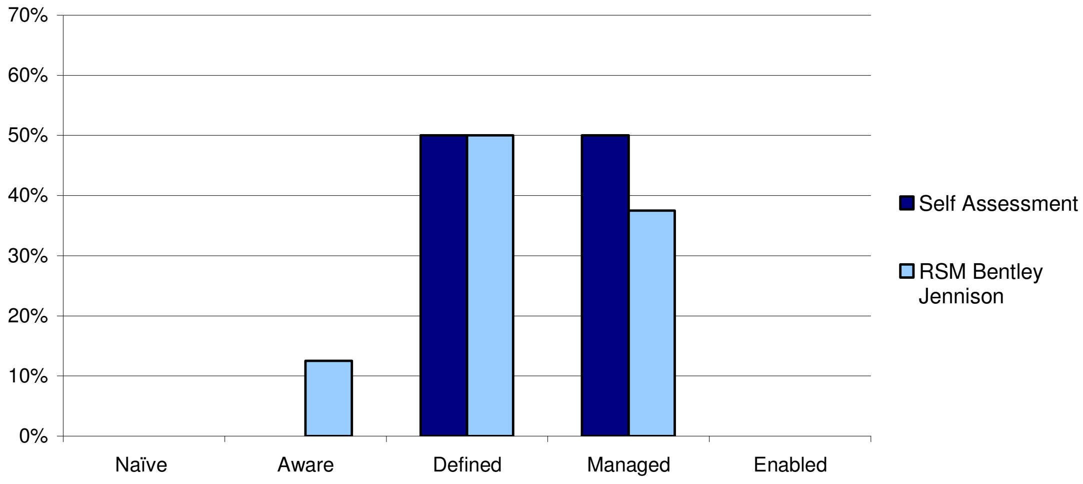


Chart 3: Assessment of Risk Maturity across Local Authorities

% of Police and Fire Authorities	Our perception of risk maturity of police and fire authorities that assessed themselves as risk managed or risk enabled
0	Risk Naïve
0	Risk Aware
25%	Risk Defined
75%	Risk Managed
0	Risk Enabled

RISK REGISTERS

Risk registers should document the perceived risks to an organisation and capture how the organisation manages those risks. When undertaking the review we looked at the different types of risk registers typically maintained in the sector. All of the authorities within our survey had a corporate risk register in place and 93% operated separate departmental or directorate risk registers.

At the time of our reviews, 64% of authorities were maintaining a risk register for an ongoing major project. We were surprised to find that only 29% of organisations had a specific IT risk register.

Information and Technology (IT) is a critical component in achieving an organisation’s overall strategy and operational objectives. IT risk management is a multi-disciplinary undertaking, and covers a variety of functional domains, ranging from data protection to change management. It is also a multi-faceted and complex undertaking that entails consideration of a wide array of compliance requirements.

IT risk management must be effectively implemented to fully address the myriad legal, regulatory, contract, and compliance requirements, otherwise, IT risk issues left unaddressed could fundamentally affect the overall organisational strategy and business operations. To facilitate this process, an IT risk register is an important mechanism to help ensure that IT related risks are identified and appropriate mitigating actions are planned and assigned, in order to facilitate the achievement of an organisation’s objectives, overall risk management processes and business operations.

REVIEWING AND UPDATING THE RISK PROFILE

The vast majority of our sample had risk strategies and policies in place setting out the organisation’s headline approach and attitude to risk, as well as clarifying responsibilities. These often include minimum requirements about how information regarding risk will be identified, captured and reported. On the whole, the majority of organisations tend to review their risk strategies and policies on an annual basis.

Risk registers should be kept under review to ensure they are living documents and therefore are a record of the organisation’s risks at any one point in time. As part of our reviews we gathered data to assess how long it had been since organisations had updated their corporate risk registers. On average, corporate risk registers had been updated within the two months prior to our review.

RISK APPETITE

64% of local authorities and emergency services organisations surveyed set out either a statement or guidance on the organisation’s risk appetite within a corporate document such as a risk strategy. Across the organisations surveyed there are often statements included within risk strategies about responsible risk taking, however few organisations have clearly defined processes which identify a criterion for determining acceptable and unacceptable risk.

Escalating Risks

As part of its risk strategy Kent Police Authority assesses and communicates its risks as follows:

- A risk score of between 9-14 is classed as medium risk and management are required to address this.
- A risk score of between 15-19 is classed as high risk and senior management are required to both address the risk and report it to the Audit and Finance Committee.
- A risk score of between 20-25 is classed as very high and any risk score at this level is not tolerated. Both the Chair and Chief Executive are informed of the risk and urgent action is taken to reduce the risk.

A number of organisations operate a system whereby risks are scored and those risks that are deemed too high are not tolerated. However many local authorities and emergency services organisations could not or do not fully define risk appetite, this is perhaps because much of the guidance publicly available regarding risk appetite is self-referencing and defines risk appetite as the appetite that organisations have for risk. A simple approach is to ensure that risk appetite is part of the challenge process when identifying and assessing risks. In this situation, risk appetite becomes something to be considered for every single risk rather than an over-arching conecpt for the entire organisation. Questions to ask are:

- What is the level of risk we think we are facing?
- What is the impact?
- Can we tolerate the possibility of that risk actually happening?
- If not, do we want or need to do more?
- Will the cost of managing this risk outweigh the benefit?

ASSESSING RISK

The majority of authorities surveyed (93%) use some form of risk matrix to gauge the potential likelihood and severity of a risk actually occurring. Some organisations consider risk in terms of potential impact and projected likelihood (29% use a 5x5 matrix and 21% use a 4x4 matrix).

It is important that an organisation not only sets a matrix that they find useful for assessing the impact and likelihood of risks, but also that this matrix is meaningful. One common pitfall of using a matrix is that some organisations do not clearly define what each element of the matrix means, and therefore the assessment of risks may not be consistent or well informed. The more successful risk management frameworks not only set out the model that the organisation uses to assess risks, but also clearly define what is meant by descriptors such as *low impact*. This should not only be agreed, but clearly communicated alongside the risk register to help the reader or reviewer. A matrix with an even number of elements can be useful so that those assessing risk do not simply opt for the middle option if they are unsure of the impact or likelihood of the risk they are considering.

86% of authorities also categorise risks, the most common categories being:

- Financial / costs
- Reputational
- Legal
- Safety
- HR and diversity
- Performance
- Service delivery
- Quality

We believe that good risk management is clearly linked to organisational and departmental objectives. Therefore, while categorising risks can be useful (and can provide helpful reporting opportunities if the organisation has a flexible risk register or risk management system), there should always be clear linkage back to objectives for the risks to be meaningful.

Use of a risk register is not the ultimate key to effective risk management, but is a useful tool to capture information about risks and to facilitate reporting. In terms of maintaining the risk register, the tools used vary from excel or word documents to specific software packages such as Covalent, 4Risk, Performance Plus, Risgen or Orchid Electronic.

ROLES AND RESPONSIBILITIES

This section looks at the specific roles and responsibilities of those responsible for risk management within their organisation; noting the difference between being responsible for facilitating the process (such as the role of the risk manager) and being responsible for taking action to minimise risk (such as the role of management).

71% of authorities in our review had a nominated risk manager. Of the 29% of organisations that do not have a risk manager most had a designated person within the organisation that is responsible for taking a lead on risk management.

Having a formal risk manager is by no means a pre-requisite to becoming risk ‘managed’ or ‘enabled’ and for smaller organisations the cost would not always be outweighed by the benefit. Indeed it is more important for an organisation to identify the best person to take a lead on the risk management process and ensure that risk management is embedded throughout the organisation generally.

Of the organisations surveyed, 36% have a separate risk management committee or group. Of those local authorities and emergency services organisations that do not have a risk management committee / group all have a sub-committee of the Authority that has delegated responsibility for overseeing risk management. Within the sector we found that the sub-committees and groups that oversee risk management typically include:

- Audit / Audit & Finance Committee
- Corporate Governance Committee
- Programme Management Board
- Finance, Audit & Performance Management Committee
- Performance & Scrutiny Panel
- Strategic Risk Management Group

All organisations set out their formal risk management responsibilities within the risk policy (or similar document) for Authority Members, Executive Management and the senior management team. The responsibility for risk management for the Authority is set out within 93% of risk policies and is formally identified within the Authority's terms of reference in 57% of organisations. A full breakdown is shown below in Chart 4.

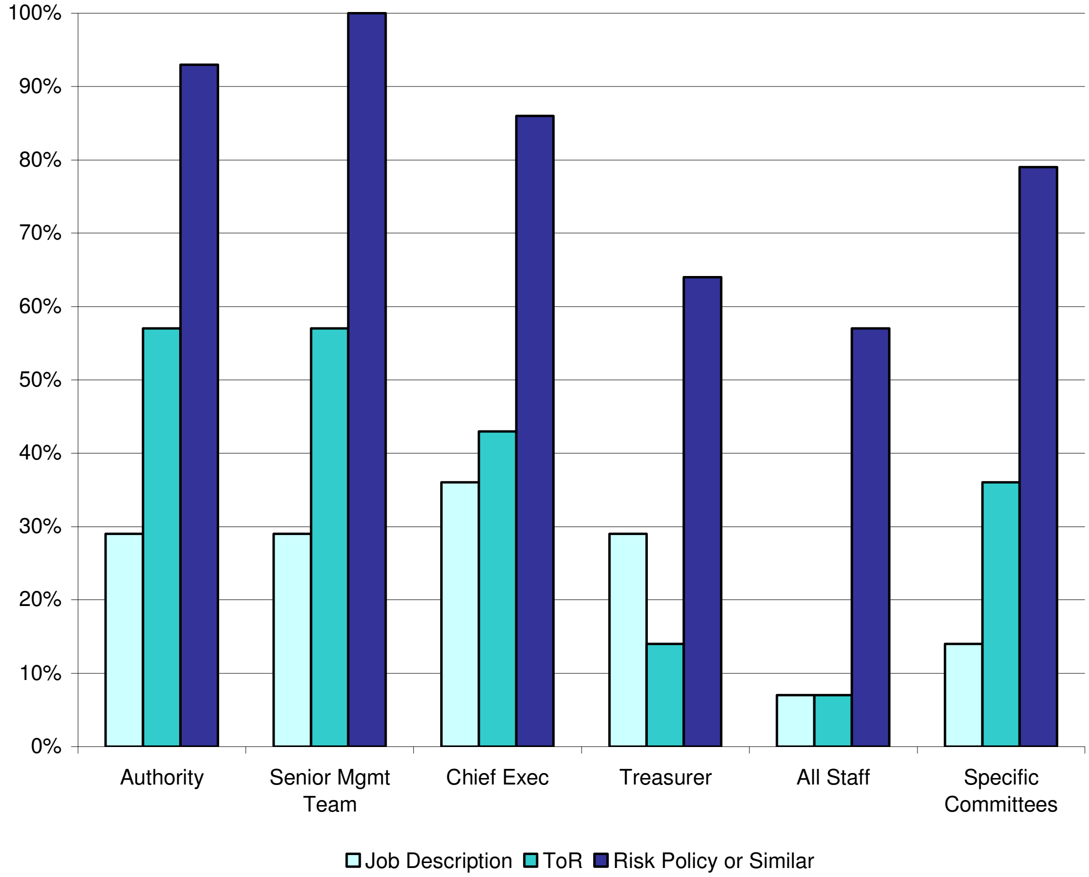


Chart 4: Where Responsibilities for Risk are Outlined

REPORTING AND MONITORING CORPORATE AND OPERATIONAL RISKS

It is important to have clear guidelines in place regarding how risk information will be monitored, reviewed, updated and reported. This section outlines our findings in relation to the reporting and monitoring of risks through the use of risk registers.

A number of organisations review and report their risk registers to the Authority, however our survey showed that 37% of Authorities do not see the corporate risk register at all. Our survey also showed that 22% of audit committees (or equivalent) do not review or receive the corporate risk register. 64% of senior management teams review and report on corporate risk registers. The tables below provide a breakdown of the results we gathered for local authorities and emergency services organisations.

	Corporate Risk Registers: Frequency of reporting to the Authority, sub-committees and Management Team within Local Authorities (% of organisations surveyed)				
	Monthly	Bi-monthly	Quarterly	Half-yearly	Annually
Authority	17%	-	17%	33%	-
Audit Committee	-	-	50%	17%	17%
Senior Management Team	50%	-	33%	-	-

	Corporate Risk Registers: Frequency of reporting to the Authority, sub-committees and Management Team within Emergency Services (% of organisations surveyed)				
	Monthly	Bi-monthly	Quarterly	Half-yearly	Annually
Authority	25%	-	25%	-	12%
Audit Committee	-	25%	37%	-	12%
Senior Management Team	25%	12%	12%	-	-

Other committees / meetings where risk registers are reviewed include:

- Corporate Governance Committee
- Performance Management Board
- Process Group
- Risk Management Group
- Performance Panel

Monitoring Risks

At Cambridgeshire Police, a database is used through which all risks identified have an action plan for improvement. Updates for this are notified as required through the email system (linked to the database for ease of use).

Where updates have not been provided or are overdue the Risk and Opportunities Manager chases responses or reasoning to ensure that all improvement actions are taken and the controls to mitigate the risk improved. If this is not actioned in a timely manner the issue is escalated through the management team to the Deputy Chief Constable and Chief Constable as necessary.

As part of the review we also examined the extent to which operational / departmental risk registers were reviewed and reported by committees. As we expected, authorities do not have a great deal of involvement in reviewing directorate risk registers; it is typically the senior management team that use this information. The chart below reflects the level of reporting and review of directorate and departmental risk registers.

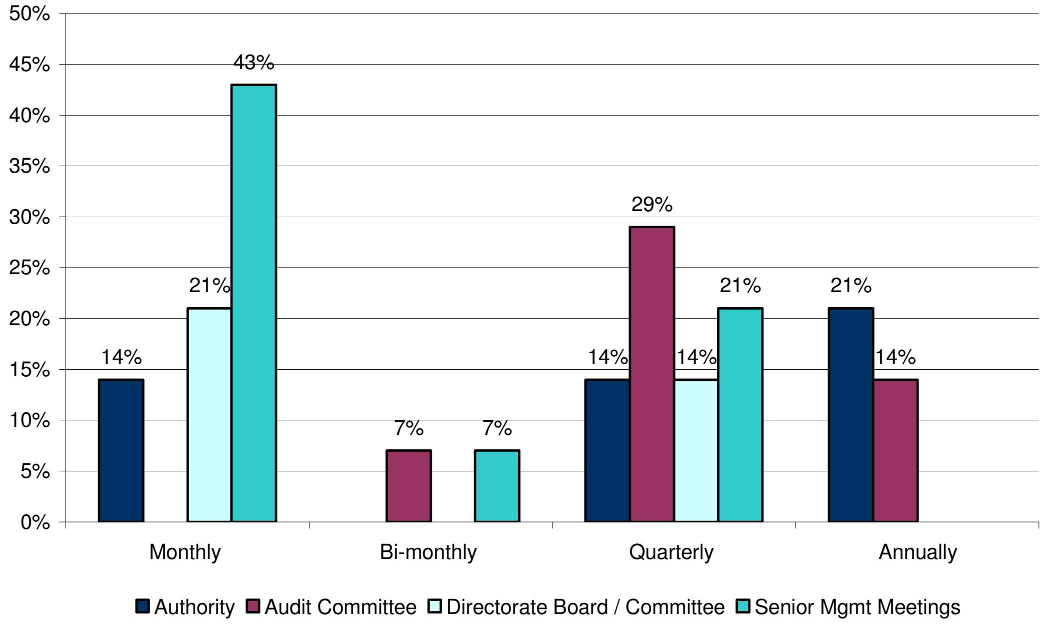


Chart 5: Where Departmental Risk Registers are Reviewed

WHAT INFORMATION DO RISK REGISTERS CONTAIN?

Having a risk register in place does not mean that the organisation has identified all of its risks, or that it is managing all of those risks. However, a document such as a risk register provides a framework to facilitate capture, assessment, monitoring and reporting of risks and associated information.

The following table identifies elements that we consider to be good practice for inclusion in risk registers and reflects the proportion of organisations which include these in their risk management registers. We have also included comparative data for those organisations we consider are risk 'managed'.

	% of authorities that include this element		
Elements included within Risk Registers	**All Authorities in survey**	**Local Authorities**	**Police & Fire Authorities**
Cross reference to objectives	86%	83%	75%
Provide an assessment of the likelihood of a risk	86%	83%	87%
Assessment of the impact of risks	86%	83%	87%
Controls and mitigating processes	86%	83%	100%
Assessment of residual risk	100%	67%	87%
Sources of assurance	71%	50%	37%
Early warning / monitoring mechanisms	71%	4%	25%
Officer responsible for the risk	100%	100%	87%
Action plan to improve the treatment of risk, which should include:	100%	83%	87%
a) Dates	86%	67%	62%
b) Responsible officer	86%	67%	75%
Action plan to improve assurances, including:	43%	50%	12%
a) Dates	43%	50%	12%
b) Responsible officer	43%	50%	12%

Effective consideration of risk and risk management is likely to include sources of assurances and early warning / monitoring mechanisms. As such it is not surprising that more risk ‘managed’ organisations include these within their risk documentation. However, many organisations still do not link assurances back to their risk profile and therefore could be missing a useful source of information to feed into performance management and risk management frameworks.

Ensuring that the risk register adequately covers all of the risks applicable to the organisation is important, however it is just as important to ensure that it is kept up to date and reviewed at appropriate times. The majority (36%) of organisations review their risk register whenever an issue is identified that needs to be included, while 29% of organisations review their risk register on a monthly (or more frequent) basis. 29% of local government and emergency services organisations also review their risk register on a quarterly basis. A small number of organisations review the risk register at specific points throughout the year but above this standard review also update the register whenever a new issue is identified.

FACTORS AFFECTING RISK MATURITY

Some of the findings from our risk maturity reviews can not easily be provided as comparative data, as they relate to how individual organisations work or what they are aiming to achieve. Notably, we found the following issues that reduced our risk maturity ratings:

- Instances where senior post holders and management were aware of major issues or significant risks but these had not been formally captured to make sure that they are on the organisation’s risk radar.
- Lack of challenge by the Audit Committee regarding the organisation’s risk profile, assurance framework or corporate risk registers, including little challenge regarding how risks are being managed or how the organisation knows that risks are being managed as well as they could be.
- Inconsistent approaches to recording and assessing risks.
- Risk appetite seen as a statement in a policy instead of requiring challenge regarding acceptable risk levels.
- Risks that are ambiguously worded or vague, which could lead to different people having a different understanding of what that risk is.
- Limited levels of follow up to ensure that actions are implemented.

QUALITY OF RISK INFORMATION

One of the things that organisations can do to improve their understanding of risk and therefore begin to become more risk mature is to improve how they communicate risk. We have seen a number of organisations with risks that are vague, and therefore open to various interpretations. This was also the case for some controls and for sources of assurance recorded within risk registers.

The tables below reflect the types of risk areas that local authorities and emergency services organisations combined reflected as their most significant risks at the time of our review.

RISKS RELEVANT TO ALL LOCAL AUTHORITIES AND EMERGENCY SERVICES ORGANISATIONS

- **Credit crunch** and the recession where there are risks that programmes may not be delivered because of a lack of financial resource. This links into wider financial concerns regarding budget over and under spends and the absence of a robust business continuity plan.
- **Partnerships** where there may be a risk that local area agreements are not established effectively and that partnerships are ineffective.
- **Poor inspection** results.
- **Data security** problems where confidential records may be lost or information is leaked as a result of an attack. There are also risks around ensuring that correct records are held electronically and that the ICT infrastructure as a whole is robust.
- **Human Resources** i.e. recruitment and retention problems, the loss of key staff, the risk of staff strikes and the potential for fraud and corruption from dishonest staff.
- Ineffective **project management** and an inability to deliver projects.
- **Health and Safety** i.e. where a serious incident such as a death has occurred and there is non compliance with health and safety legislation.
- **Pandemic Flu** and the consequences of this across the community and the workforce.
- **Reputational** risks (much of which is linked to the risks listed above).

The following tables set out the key risks specifically for local authorities and emergency services organisations.

TOP RISKS FOR LOCAL AUTHORITIES

- Credit crunch and the inability to maintain a balanced budget.
- Failures in health and safety, which may result in an avoidable death.
- Human resources.
- Ineffective partnership working.
- Risk of fraud.
- Inadequate organisational business continuity planning.

TOP RISKS FOR POLICE AND FIRE

- Major sporting events coupled with the extra strain on financial and people resources.
- The threat of a serious event such as a terrorist attack.
- Failure of care in police custody.
- Failure to undertake adequate community engagement.
- Collaborative partnership working fails to realise expected benefits.

DETAILS OF OUR SAMPLE

The results within this report are based on the information from a sample of local authorities and emergency services organisations in both England and Wales as follows:

Type of organisation	Number of participants	% of participants
Local Authority	6	43%
Police Authority	6	43%
Fire and Rescue Authority	2	14%
Total:	**14**	