Derby City Council

AUDIT AND ACCOUNTS COMMITTEE
24 September 2014

ITEM 14

Report of the Head of Governance & Assurance

Risk Management – Models of Performance/Effectiveness

SUMMARY

1.1 This report identifies examples of models to assess risk management performance of an organisation.

RECOMMENDATION

2.1 To note the report.

REASONS FOR RECOMMENDATION

3.1 The Audit and Accounts Committee is responsible for providing assurance to the Council on the effectiveness of the governance arrangements, risk management framework and internal control environment.

SUPPORTING INFORMATION

4.1 At its meeting on 9 July 2014, this Committee asked that the Head of Governance and Assurance bring a report to the next meeting which would outline 3 models of how the Council could assess the performance/effectiveness of its risk management framework.

4.2 The report to Committee on 9 July detailed the key elements of achieving a robust risk culture. The “LILAC” approach, although not really a model in itself, suggests that risk management activities will be embedded when the risk culture displays leadership, involvement, learning, accountability and communication.

COSO Model

4.3 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five US private sector organisations (including the Institute of Internal Auditors) and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

4.4 The COSO "Enterprise Risk Management-Integrated Framework" published in 2004 defines ERM as a "…process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

4.5 The COSO ERM Framework has eight Components and four objectives categories. It is an expansion of the COSO Internal Control-Integrated Framework published in 1992 and amended in 1994. The eight components - additional components highlighted - are:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

The four objectives categories - additional components highlighted - are:

- Strategy - high-level goals, aligned with and supporting the organization's mission
- Operations - effective and efficient use of resources
- Financial Reporting - reliability of operational and financial reporting
- Compliance - compliance with applicable laws and regulations

4.6 The framework suggests that effective risk management will be embedded when an organisation can demonstrate compliance with external drivers such as legislation, regulation etc. COSO is not intended to apply to the public sector.

ALARM Model

4.7 In 2009, the public risk management association (ALARM) produced a National Performance Model for Risk Management in the Public Services. The Model is designed to:

- Measure current performance against a recognised achievement level
- Provide the basis for clear performance indicators
- Act as a catalyst for improved performance within the organisation
- Inform assurance in corporate governance terms
- Demonstrate current maturity in terms of
  - External inspection expectations
  - National and international standards
- Allow for comparison with other organisations and learning from best practice through systematic benchmarking.

4.8. The Model breaks risk management activity down into 7 strands:

Enablers

- Leadership and management
- Strategy and policy
- People
- Partnership, shared risks and resources
- Processes and tools

Results

- Risk handling and assurance
- Outcomes and delivery

4.9 A detailed and comprehensive set of questions have been designed to test current performance against an Assessment Framework of 5 levels of risk maturity.

Level	Description
1	Engaging
2	Happening
3	Working
4	Embedded and Integrated
5	Driving

In 2009, a self-assessment exercise was carried out to ascertain where the Council was with its risk maturity. The result was level 2, with level 3 partly achieved. However, local authorities have gone through significant change in the past 5 years and it we believe that the ALARM model no longer reflects the nature of local government, in that external drivers are playing a more prominent role.

4.10 In the end, all that any risk management model will show is various interpretations of what good risk management looks like. Ultimately the issue is not what effective risk management looks like, but rather how progress can be evidenced and how an organisation wishes to measure its control environment / risk aware culture.

4.11 The varying models don't so much have strengths and weaknesses as opposed to areas of focus. For example COSO tends to be used by very large financial institutions. It is designed to provide reasonable assurance effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations such as Sarbane Oxley. The ALARM model was designed for the use of the public sector so they can determine how well risk is embedded, with its focus around all the internal elements of an organization.

4.12 The question posed within the Insurance and Risk team is why do these models/methods have to be mutually exclusive? Why not take the best ideas, techniques and concepts and combine them into what's most useful for the city Council?

Risk Ladder

4.13 To this end a "risk ladder" was developed. The idea of the risk ladder was to take the ALARM model and use it as a base. From this base we have built in elements from

- other models/methods,
- good practice
- our own knowledge and experiences (of both risk management and the council itself)

in order to create a system built specifically for Derby City Council. Care has been taken not to just cherry pick our favourite bits from other models thereby creating a mixture of ideas that conflict and contradict. There was also the problem that developing our own model could potential lead to gaps. However, by using the ALARM model as the template, this should reduce that risk.

OTHER OPTIONS CONSIDERED

5.1 N/A

This report has been approved by the following officers:

Legal officer	n/a
Financial officer	n/a
Human Resources officer	n/a
Estates/Property officer	n/a
Service Director(s)	n/a
Other(s)	n/a

For more information contact:	Richard Boneham, Head of Governance & Assurance 01332 643280 richard.boneham@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implications Appendix 2 – Risk Ladder

Appendix 1

IMPLICATIONS

Financial and Value for Money

1.1 None directly arising

Legal

2.1 None directly arising

Personnel

3.1 None directly arising

IT

4.1 None directly arising

Equalities Impact

5.1 None directly arising

Health and Safety

6.1 None directly arising

Environmental Sustainability

7.1 None directly arising

Property and Asset Management

8.1 None directly arising

Risk Management

9.1 The risks of using the “risk ladder” approach are outlined in paragraph 4.13.

Corporate objectives and priorities for change

10.1 The functions of the Committee have been established to support delivery of corporate objectives by enhancing scrutiny of various aspects of the Council’s controls and governance arrangements.

Appendix 2

	Risk Leadership	Risk Strategy & Policies	People	Partnerships & Resources	Risk Management Processes	Risk Handling	Outcomes	
Level 4 Excellent capability established	Senior Managers reinforce & sustain risk capability, organisational & business resilience & commitment to excellence.	Risk management capability in policy & strategy making is reviewed and improved.	All staff are risk aware & capable of using basic risk skills, tools & techniques. They feel empowered to take well managed risks.	Information integrity and asset security are assured. Financial and other resources are effectively managed.	Management of risk & uncertainty is well integrated with all business processes.	Excellent evidence that risk management is being highly effective in all areas & improvement is being pursued.	Excellent evidence of risk management contributing to markedly improved outcome performance, better value for money & new opportunity realisation	Level 4 Organisations have a risk-aware culture with a pro-active approach to risk management in all project activities. As a result, the consideration of risk is inherent to routine project processes. Risk information is actively used and communicated to improve processes and gain competitive advantage.
	Leaders invited to speak about their success.	Overall risk appetite achieves balance between opportunities and threats.	Core group of people are highly skilled in managing risk effectively.	The supply chains are tested	Arrangements in place to identify opportunities which might be available if risks are well managed.	Higher risk opportunities being successfully pursued.		
	There is strong support and reward from Senior Managers for seizing opportunities & for well managed risk taking.		Specialised risk training an integral part of on-going personal development plans.		Risk management standards applied in all areas.			
	A Senior Officer and member jointly champion and take overall responsibility for embedding risk management		All Members receive risk management awareness training		The organisation considers opportunities as well as threats			
					Risk metrics are collected and used to inform decision making			
					Evidence that it's has embedded risk management in its corporate business process including; Strategic planning, Financial planning, policy making and review and performance management			

	Risk Leadership	Risk Strategy & Policies	People	Partnerships & Resources	Risk Management Processes	Risk Handling	Outcomes	
Level 3 Embedding & Improving	Top-down commitment with embedding & integrating risk management as routine business practice.	Risk handling is inherent feature of all policies & strategy making processes.	People encouraged & supported to be more innovative. Regular training is available for people to enhance their risk skills. CPD training in place for core group of people.	Sound governance arrangements established; partners & suppliers selected on basis of risk capability & compatibility.	Risk metrics are collected and used to identify and mitigate weaknesses	Clear evidence that risk management is being effective in all areas and that risk opportunities are being pursued.	Clear evidence of risk management contributing to significantly improved performance for all relevant outcomes, better value for money, showing positive & sustained improvement & new opportunity achievement.	Level 3 Organisations have built the management of risk into routine business processes and implement risk management throughout the project. Generic risk management processes are formalised and the benefits are understood at all levels of the organisation, although they may not be consistently achieved.
	Members & Senior Managers ensure that staff are suitably skilled to achieve continuous improvement.	COG in conjunction Audit & Accounts committee have set an overall risk appetite	Members with specific risk responsibility have had risk management awareness training	Consideration of risks in significant partnership and assurances that they are managed	Staff accept risk management as standard requirement of good management.			
					The process is reviewed and updated annually			
					Members responsible for corporate risk management receive regular reports and take action to ensure that business risks are being managed			

	Risk Leadership	Risk Strategy & Policies	People	Partnerships & Resources	Risk Management Processes	Risk Handling	Outcomes	
Level 2 Implementation in progress for all key areas	Senior Managers act as role models and take the lead to ensure that approaches for addressing risk are being developed & implemented consistently & thoroughly across the organisation.	Risk management principles are being reflected in the organisation's policies & strategies, communicated effectively & made to work through a framework of processes.	Core group of people have skills & knowledge to manage risk effectively. Suitable guidance is being made available & training programmes being implemented to develop risk capability.	Risk with partners is being managed consistently for all key areas & across organisational boundaries for managing assets & financial & other resources.	Risk management processes being implemented in key areas.	Some evidence that risk management is being effective in at least most relevant areas if not in all relevant areas.	Some evidence of risk management contributing to improvement in outcome performance, demonstrated by measures including, where relevant, stakeholders' perceptions and potential for new opportunities.	Although aware of the potential benefits of managing risk, Level 2 Organisations have not implemented risk processes effectively and are not gaining the full benefits. The organisation is either experimenting with the application of risk management or is operating a risk management process that has fundamental weaknesses.
	Strategy/policy approved by members.	All Policy/Strategy development include a risk assessment			Register of risk linked to objectives and assigned owners			
	Audit & accounts take an active role in the managing of governance and RM	Risk appetite is understood and considered to inform the SR register			Risk capability self-assessment tools being used in some areas.			

	Risk Leadership	Risk Strategy & Policies	People	Partnerships & Resources	Risk Management Processes	Risk Handling	Outcomes	
Level 1 Awareness & understanding	Top management are aware of need to manage uncertainty & risk & have made resources available to improve.	All Policies & strategies are reviewed against risk principles.	Key people are aware of need to assess & manage risks & understand risk concepts & principles.	Key people are aware of areas of potential risks with partnerships, suppliers & management of significant resources & understand the need to agree approaches to manage these risks.	Some stand-alone risk processes have been identified.	No clear evidence that risk management is being effective.	No clear evidence of improved outcomes or any opportunities identified.	Level 1 Organisations are unaware of the need for the management of risk or do not recognise the value of structured approaches to dealing with uncertainty. Management processes are repetitive or reactive, with insufficient attempt to learn from the past or to prepare for future threats or uncertainties.