Dudley Metropolitan Borough Council

Agenda Item No. 9

Audit and Standards Committee 15th April 2015

Report of the Chief Officer, Finance and Legal

Risk Management

Purpose of Report

1. To update members on current Corporate Risks and other matters relating to risk management.

2. To approve the Risk Management Strategy for 2015/16.

Background

3. This Committee requested it should receive details of Corporate Risks three times per annum. This is the third such report for the current municipal year.

Corporate Risks

4. Corporate Board receives reports on Corporate Risks at least 3 times per annum and in addition, all Directors continue to review Directorate risks on a quarterly basis which form part of the Quarterly Corporate Performance Report. Appendix 1 shows details of Corporate Risks (as reviewed by Corporate Board on 10th March 2015) and therefore those appearing at the highest level on the Council's risk register. In simple terms, these risks are generally acknowledged as being the most significant facing the Council, impacting upon at least one or several of Council's key objectives. Corporate Board have identified one new risk (R.82) relating to the corporate organisational restructure and associated controls and made several additions/amendments to existing controls. All these updates are reflected in Appendix 1.

5. In addition to risks tabled in Appendix 1, this Committee may identify any additional risks that it considers should form part of the Corporate Risks list.

6. At its last meeting on 9th December 2014, this Committee agreed to scrutinise risk R.21 relating to fraud. The Head of Internal Audit will present to the Committee on this risk in the context of a separate fraud report on this agenda.

Risk Management Strategy

7. The Risk Management Strategy and guidance has been reviewed and is attached as Appendix 2.

Other matters relating to Risk Management

8. With regard to the practicalities of risk monitoring and reporting, at the time of writing, the corporate risk register is largely transferred to the corporate database known as *Spectrum.* This means the 'look and feel' of future risk reports will be very much in keeping with other performance management information appearing in the Quarterly Performance Management Report.

Finance

9. By transferring from the use of an externally supported risk database (JCAD) in favour of the Council's own Spectrum system, this will result in a small annual saving of around £5k.

Law

10. The Council has a statutory responsibility for managing risks as laid out in Section 4 of the Accounts and Audit Regulations 2003 (amended 2006).

Equality Impact

11. There are no equality issues arising from this report.

Recommendations

12. That this committee:

- Notes and comments on the Corporate Risks as set out in Appendix 1.
- Identifies any additional risks that it considers should form part of the Corporate Risks list.
- Identifies a particular risk for closer scrutiny the next time a risk report is scheduled (Provisionally July 2015).
- Approves the Risk Management Strategy and Guidance set out in Appendix 2

……

Iain Newman, Chief Officer Finance and Legal

Contact Officer: Sara McNally, 01384 815346. sara.mcnally@dudley.gov.uk

Risk Management Strategy incorporating Risk & Assurance Protocol Guidance

2015-16

Risk Management & Insurance
Directorate of Resources and Transformation

Risk Management Strategy and Assurance Protocol Guidance (Reviewed March 2015)

Dudley
Metropolitan Borough Council

Introduction and Key Principles

The Risk Management Strategy within Dudley MBC will follow recognised risk management principles, encompassing the Risk Assurance Protocol process, namely:

- Risk identification and analysis should be undertaken at the earliest opportunity in the business processes and should be forward thinking as well as reflective.
- Emphasis is placed upon assigning risk ownership and mitigating actions.
- A central, corporate risk register should be used by all directorates for recording and updating risks.
- Mitigating actions should be regularly reviewed and tested for efficiency and effectiveness.
- Project risks should be managed in accordance with best practice e.g. PRINCE2 (Projects in Controlled Environments)

Roles and Responsibilities

Primary responsibility for risk management sits with each Chief Officer. The Quarterly Performance Monitoring process seeks to report the most important ("corporate") risks to Corporate Board and to elected members, via the *Quarterly Performance Management Report*. Audit & Standards Committee will also receive 3 risk reports per municipal year and is remitted to provide scrutiny of risks and importantly their associated controls.

Monitoring and Audit

A Risk Assurance Protocol (R.A.P.) is in place. The purpose of this R.A.P. is that the appropriate Strategic Director or Chief Officer should give assurance that all the risks and mitigating actions for his/her directorate are being reviewed and monitored. The R.A.P is signed off electronically via Spectrum Risk. Audit Services assesses compliance with the R.A.P. when undertaking risk management audits.

The corporate risk register is located within Spectrum. Spectrum requires no specific password and is available to all users via Outlook.

Practical Guidance and processes

The purpose of this guidance is to assist with the identification, scoring, review and management of risks. Accordingly it considers:

- Moderation of risks – to ensure that a complete range of risks are managed at an appropriate level and that risks are ranked consistently.
- Corporate risks – definition of the criteria to ensure that the most important risks (and only those) are reported to Corporate Board and elected members.
- Partnership risks where applicable

A sample R.A.P. is attached as an Appendix. The sections in this guidance are structured around the questions in the R.A.P.

Have risks been clearly identified and adequately described?

What is a risk? The corporate definition is

"Uncertainty of outcome, whether positive opportunity or negative threat"

Priority risk considerations should be:

- New legislation/developments etc.
- Volatile/transient e.g. extreme weather/political change
- Historical evidence e.g. past problems
- Persistent but serious Audit breaches
- Prosecutions
- Early warning indicators
- Wider intelligence

The following would **not ordinarily** be included within the risk register:

- Routine operations running well with no evidence to the contrary.
- Areas giving little or no historical evidence of volatility.
- Not merely due to a 'general lack of resources'.

Risk identification is concerned with identifying the events that can impact on the business objectives. It may be helpful to think in terms of the following phrases and to maintain focus around Dudley M.B.C. and its responsibilities in the first instance

EVENT	⟶	**CONSEQUENCE**	⟶	**IMPACT**
There is a risk that / of….		leads to…		results in…

A risk simply expressed as "failure to complete project x or achieve objective y" is unlikely to be a meaningful risk and is also unlikely to fruitful when formulating mitigating controls. Therefore all risks should be articulated in a way that makes them understandable to the layperson and **not** written in jargon or acronyms.

In order to ensure the completeness of risks, it **may** be helpful to consider the following categories (not all of these will be relevant and some risks will fall into more than one category):

- Environmental
- Financial
- Partnership/Contractual
- Service Delivery
- Fraud/Corruption
- Legal governance and compliance
- Political
- Reputational

Risk identification should be repeated regularly to ensure that new risks arising are identified and brought into the risk profile as appropriate, for example:

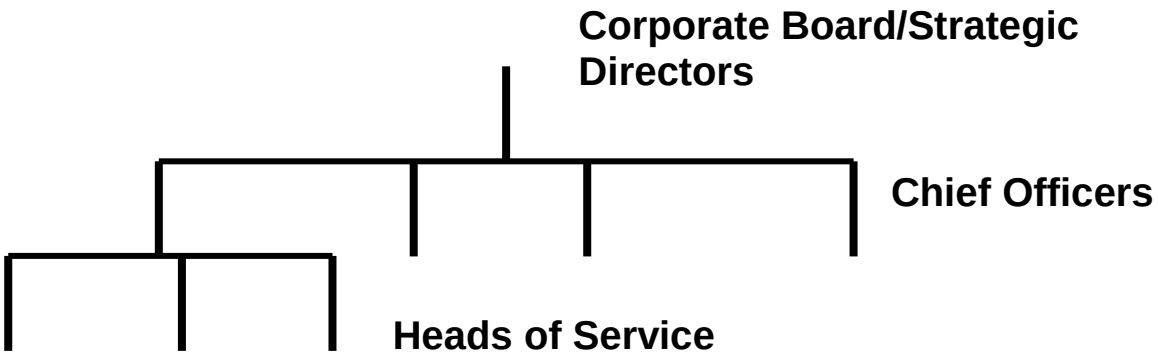
- An adverse event (or a "near miss" event occurring either within Dudley MBC or another organisation).

- Something new e.g. a project, partnership, or very different service and/or new funding stream.
- As a result of ongoing management review, e.g. budget pressures, unexpected demand for service, etc.
- Changes in legislation.

Where appropriate risks should be recorded on Spectrum. Training and support in the use of this system is available from the Risk Management and Insurance Team.

Risk Register Tiers and Reporting

For manageable reporting, Spectrum Risk is flexible in terms of structure. Subject to finer points of the Council's restructure that may yet emerge, it is expected that the hierarchy of risk registers will follow as below i.e. 3 tiers. Requirement to have formal risk registers below these levels are at the discretion of team managers/section heads but regardless of formal risk registers, consideration of risk management must be evidenced.



Corporate - risks at this level will be **owned by Corporate Board / Strategic Directors** and should be:

- Primarily strategic, relating to key objectives or functions. Usually spanning several business planning years and several or all directorates - e.g. future funding scenario, demographics, pay structures, asset utilisation/disposal and high-level business continuity/emergency planning. It is expected that Directors/Board will identify this level of risks and will formally review them at least 3 times per annum. Audit & Standards Committee will also receive details of corporate risks 3 times per annum and on a rolling basis will scrutinise particular corporate risks of its choosing. This may entail directors and other senior officers attending this committee to provide members with advice and guidance on how particular risks are being managed.

Chief Officers- risks at this level are to be owned by the senior management within directorates and should include:

- Probably fundamental to one or several key objectives of individual directorates. Expectation that Directors/Assistants would own and report to Board at his/her discretion - e.g. Waste disposal, Children in Care, Transforming Social Care

Heads of Service- risks at this level should be:

- Mainly key operational, unique to that service but would encompass most important or escalated risks from team levels where appropriate. Escalated to Chief Officer level at the discretion of DMT/DMG's.

It may not be necessary to make a formal risk register entry below divisional level but documentation of risk review/processes is required.

Existing risks - Are they valid?

Existing risks **must** be reviewed to ensure all aspects of the risk and its management are still valid. In this regard, risk owners should remain cognizant of risk volatility, new or revised controls and the need for accurate ratings with regard to impact and likelihood. In other words the transient and volatile nature of risks must be acknowledged and managed accordingly.

Consider emerging risks -

A key principle of good risk management is that it should be forward thinking, it is vital to therefore to consider emerging risks. In this regard, management processes **must** ensure mechanisms are in place to facilitate this, e.g. at management meetings or business planning sessions. In this context 'emerging' will generally consider the future as 12 to 36 months, in other words in keeping with other medium/long term strategies. The R.A.P. will also require this explicit consideration.

Obsolete Risks -

It is also important that obsolete risks are withdrawn from risk register. Ongoing review of all risks should identify risks that are no longer valid. In other words risk registers should not be cluttered with obsolete items where risks have safely past or no longer fit with the corporate definition of a risk.

Risk ownership

In determining risk ownership, there is a balance to be struck:

- Ownership of a large number of risks at too high a level may be ineffective.
- Ownership at too low a level would lead to the proliferation of risks and confuse the reporting to senior levels.

A risk owner should be an officer with authority to review and enforce processes to manage the risk in question. It is possible that someone other than the owner of the risk may own mitigating actions; however overall responsibility remains with the risk owner.

Risk ownership should be recorded in Spectrum, an individual owner or owning team can be accommodated.

Risk reporting in the Corporate Quarterly Management Report

Spectrum Risk reports look similar to other management information in the Quarterly Management Report. Risk management principles built in to this system mean that:

- The risk owner/owning team must assess the current risk rating at each review time, the system makes this mandatory.
- Comments **must** be provided to demonstrate review has taken place, i.e. a simple tick with no commentary will not allowed by the system.
- Mitigating controls must be identified, if they are not, blanks will show and the risk owner will be required to address this.

Reviewing risks

Review dates for risks and their associated mitigating actions should reflect the status of the risk. See guidance on the status of risk below. In practical terms, it is unlikely that the majority of risks will require any more than quarterly updates.

The Risk Assurance Protocol is signed quarterly and should be done electronically via Spectrum. Spectrum retains this document on a 'point in time' basis and Audit Services will review this as part of its risk audit programme.

Have all mitigating actions been identified and are they operating as intended?

Having ensured that the relevant risks have been identified, the main focus of risk management should be on the implementation of relevant mitigating actions and review of their effectiveness. Ownership of mitigating actions should be guided by the same considerations as are set out for risk ownership – i.e. officers with authority to review and enforce.

In many cases it will be possible to cite an entire business process as a mitigating action. For example, the FMMR process is a mitigating action against the risk that the Council does not manage within its available resources. Health and safety reviews are a mitigating action against the risk of physical or psychological harm to employees and the public. In these cases it is not necessary to record all the details in *Spectrum*.

Costs and logistics of implementing mitigating actions should be in perspective. If risk measures are particularly complex then a formal cost benefit analysis will need to be undertaken i.e. controls measures should remain commensurate with the risk.

The higher the current assessment of a risk (see below), the more active consideration there should be of additional mitigating actions to reduce the risk.

Is the CURRENT assessment of the risk still valid?

The current assessment of risk is the combination of impact and probability (likelihood) and is **after** consideration of mitigating controls operating as intended i.e. it is the **net** risk.

Criteria for assessing impact (as insignificant, minor, moderate, significant or major) are set out below:

	IMPACT DESCRIPTIONS				
	1 Insignificant	**2 Minor**	**3 Moderate**	**4 Significant**	**5 Major**
Service, Partnership & Project Delivery	Minor errors in systems and processes handled within normal daily routine.	Short-term disruption and action required. Managed by intervention from Head of Service/ Block Leader or Project Manager.	Noticeable disruption affecting customers. Intervention and management by local management team.	Disruption of core activities. Key targets missed, some services compromised. Intervention by DMT or Project Board or Block Leaders Group required	Loss of core activities. Strategic aims compromised. Intervention by Cabinet/, etc.
Financial	Not exceeding £10k losses or negative variance against annual revenue budget or capital budget	£11-50k losses or negative variance against annual revenue budget or capital budget	£50k to £250k losses or negative variance against annual revenue budget or capital budget	Between £250K to £750k losses or negative variance against annual revenue budget or capital budget	Greater than £750k losses or negative variance against annual revenue budget or capital budget
Reputation	Event or decision not in the public domain that has little impact outside of DMBC	Event or decision in the public domain that receives minimal or no negative coverage by local media	Event or decision in the public domain that receives some negative coverage by local media and/or pressure groups	Event or decision in the public domain that receives significant negative coverage by national media and/or pressure groups	Event or decision in the public domain that receives extensive negative coverage by national media and/or pressure groups

Impact descriptions above should be taken, where appropriate, to include the risk of lost opportunity. For example, there may be the risk of missing an opportunity to make significant financial gains or achieve extensive positive media coverage.

Probability should be assessed into one of five bands ranging from Rare (<10%) to Almost Certain (>90%).

Spectrum calculates a current rating, based on a combination of impact and probability, as follows:

PROBABILITY (Over next 12 months)							
	Almost Certain >90%	**5**	Minor (5)	Moderate (10)	Significant (15)	Major (20)	Major (25)
	Likely 50%-90%	**4**	Minor (4)	Moderate (8)	Significant (12)	Major (16)	Major (20)
	Moderate 30%-50%	**3**	Insignificant (3)	Minor (6)	Moderate (9)	Significant (12)	Significant (15)
	Unlikely 10%-30%	**2**	Insignificant (2)	Minor (4)	Minor (6)	Moderate (8)	Moderate (10)
	Rare < 10%	**1**	Insignificant (1)	Insignificant (2)	Insignificant (3)	Minor (4)	Minor (5)
			1 Insignificant	**2 Minor**	**3 Moderate**	**4 Significant**	**5 Major**

Dependant upon the score of the risk, the following reporting and review standards are **recommended**

RISK COLOUR	RISK SCORE	REPORTING LEVEL	RECOMMENDED REVIEW PERIOD
RED	**MAJOR** (score of 16-25)	Directorate & Corporate Board via the Quarterly Corporate Performance Report but only if also deemed a 'corporate' risk	At least quarterly
ORANGE	**SIGNIFICANT** (score 12-15)	Directorate	At least quarterly
YELLOW	**MODERATE** (score 8-10)	Directorate	At least six monthly
BRIGHT GREEN	**MINOR** (score 4-6)	Division	At least annually
DARK GREEN	**INSIGNIFICANT** (score 1-3)	Risk Owner	At least annually

Nothing in the above should prevent risks being from time to time reported to a higher level or reviewed more frequently if required should they become volatile.

Moderation

As with any system of criteria, the impact and probability criteria set out above are open to interpretation. Risk Champions and relevant DMG/DMT's and/or directorate Risk Groups have a role in moderating those interpretations and using their discretion.

It is not possible to define the types of risks that should appear as major risks – to do so would prevent each risk from being considered on its own merits. However, if the process is operating as intended, the risks that are considered by Corporate Board and Members should be those that are not capable of being contained at directorate level and will become known as *Corporate Risks*. As a matter of course, these risks will be published in the Quarterly Corporate Performance Report.

The Risk Management process should include the following:

Risk identification – by all employees

Employees should highlight risks to their line manager, e.g. through supervision, team meetings and/or planning processes. Risks are included in team/service plans, along with mitigating actions and referred to immediate line managers. It may not be necessary to enter risks on the risk register at this point. This should be something that managers and respective teams should establish and at which level they should be entered on the risk register. At this level, risks are likely to be at team level so entry on the risk register is optional but risks should be managed regardless.

▼

Risks communicated and entered onto the corporate risk register (Spectrum)

Following validation by line managers / heads of service, risks are entered onto Spectrum The Risk Owner must ensure that valid controls have also been entered and review periods aligned with the risk score as outlined above.

▼

Risks reviewed (Service Level Teams (S.L.T's), Departmental Management Teams (D.M.T.'s) / Directorate risk groups)
S.L.T. members review and identify new risks at Quarterly Performance and/or Risk Management meetings. This provides a challenge process in order to review and monitor volatile and major risks as well as assisting with the quarterly assurance protocol process.

▼

Escalation of risks to corporate level.
It should be borne in mind that any risks which are primarily strategic relate to key objectives or functions and span several business planning years and/or several or all directorates may need to be brought to the attention of Directors for possible escalation to 'corporate' level. There is formal opportunity to bring these risks to Corporate Board 3 times per annum but Directors should raise awareness at any time they consider appropriate.

Partnerships

Partnership working continues to be an important part of the Council's operations; however, experience indicates that partnerships rarely give rise to risks in isolation. Accordingly there is no longer a requirement to make a risk register entry uniquely associated with a partnership and these risks should be considered in the normal scheme of risks. Should a partnership give rise to explicit risks that cannot be appropriately accounted for elsewhere in the risk register, then a unique risk register should be created for that partnership.

Director's sign off – Risk Assurance Protocol

Director sign off should be based on an escalation of assurances from heads of service up to Assistant Directors and, in turn, to Directors themselves to enable sign off to take place. This may be a quarterly or more frequent DMT item. R.A.P.s can be created (within Spectrum) at any level and this should be determined within individual teams and Risk Champions. As a minimum requirement a R.A.P. will be required at Directorate level.

Performance/Risk Management Assurance Protocol – 2015/16

This protocol is available electronically via Spectrum

Directorate: ..... Quarter:……

	Review criteria	Y	N
1	Have you proactively considered and identified all significant risks? This should include **emerging** (3) risks and their proximity		
2	Are all risks suitably articulated/ described?		
3	Are appropriate risks owners identified for all risks?		
4	Are the risks still valid? *E.g. still **current (4)** or can they be withdrawn?*		
5	Have all mitigating actions been identified and operating as intended, this should include valid owners.		
6	Are you satisfied that risk have been appropriately scored in conjunction with the scale contained in the *Risk Management Strategy?*		
7	Where you consider any risks have significantly worsened since the last review, have you reported this via the appropriate hierarchy e.g. line manager, Chief Officer or Corporate Board?		

Additional information/notes:

1/ The Assurance Protocol will need to be completed by the relevant Director liaising with the Risk Champion to determine the arrangements are place to ensure compliance.
2/ Where significant worsening of risk/s has occurred, directors will also consider additional, formal reports to appropriate committee/s and/or escalation to Corporate Board if appropriate.
3/ Emerging will mean 12 to 36 months hence.
4/ Current will mean known and existing risks

List of significant partnerships and projects assumed included in the above:

Significant partnership/project	Lead Officer

Director…… Date……