INTERNAL AUDIT REPORT

RISK MANAGEMENT 2016/17

Issue Date:	7th July 2016	***Issued to:***	Simon Riley	Head of Finance and Corporate Services and S151 Officer
Author:	Heather Fraser		Richard Ellis	Service Manager – Corporate Services
			Brian Degruchy	Business Development and Programme Manager
			Edward O'Neill	Business Planning Officer
			Beverley Jolly	Corporate Director – Resources (copy of final draft and final report)
			TBA	Chair of Governance & Audit Committee (copy of final report only)

RISK MANAGEMENT 2016/17
EXECUTIVE SUMMARY

1. INTRODUCTION AND INTERNAL AUDIT OPINION

The Council's Risk and Opportunity Management Framework provides a structured and coherent approach to risk management and is available to all staff. The Framework is subject to review on a biennial basis and was last reviewed and approved by the Executive in January 2016.

Arrangements for ensuring accountability and ownership of risks are sound. Roles and responsibilities are clearly specified in the Risk and Opportunity Management Framework. Arrangements could be strengthened further by updating the Framework to include the role and responsibilities of the Programme Board in respect of project risks.

Appropriate controls are in place to ensure that risks are identified and all corporate, business and operational risks are recorded on the TEN Performance Management System. Furthermore, Auditor review of the corporate risk register confirmed that all 18 risks detailed were linked to the Council's critical outcomes.

The Council recognises that all risks should be clearly defined to ensure that the potential effects of each risk are clearly understood. The Risk and Opportunity Management Framework refers to the *Cause, Event and Effect* method in order to achieve this, however, Internal Audit identified that in 44% of cases, only the *Cause* or the *Effect* of the risk had been detailed in the corporate risk register.

The Council is able to demonstrate that it has an appropriate Framework in place in order to manage its risks effectively. The Scrutiny – Resource and Performance Panel receive quarterly reports in relation to the Council's corporate risk register, it was noted, however, that the role and responsibilities of the Panel with regards to risk had not been detailed within the Council's Constitution. The Business Planning Officer advised that a new version of the Constitution would be in place during 2016/17.

Based on these findings, the framework of controls currently in place provide ***Sufficient Assurance*** that the identified risks have been appropriately mitigated. Detailed findings are set out in section 2. The assurance opinion is based upon testing of the design of controls to manage the identified risks and testing to confirm the extent of compliance with those controls, as summarised in the table below:

Internal Audit Assurance Opinion	Direction of Travel				
Sufficient Assurance	**N/A**				
Risk	**Design**	**Comply**	**Recommendations**		
			H	**M**	**L**
Risk 1: Lack of accountability and ownership of risk management within the Council.	**Substantial Assurance**	**Substantial Assurance**	0	0	1
Risk 2: Risks facing the Council are not identified and / or effectively managed or controlled.	**Substantial Assurance**	**Sufficient Assurance**	0	1	1
Risk 3: Lack of / no assurance that risk management is effective.	**Sufficient Assurance**	**Substantial Assurance**	0	1	0
Total Number of Recommendations			**0**	**2**	**2**

2. SUMMARY OF FINDINGS

Risk 1: Lack of accountability and ownership of risk management within the Council

The Council's Risk and Opportunity Management Framework provides a structured and coherent approach to identifying, assessing and managing risk and is available to all staff. The Framework is subject to review on a biennial basis and was last reviewed and approved by the Executive in January 2016.

Risk management training is available to all staff via the intranet. It was noted that only two managers had completed the online training module during 2011 and 2014, however, a training session titled 'Good Governance – Managing Risks and Opportunities' was held on 22nd January 2015. The Learning and Development Business Partner advised that all service managers, with the exception of two, had attended the training. The training session was also attended by all members of the Corporate Management Team (CMT). In addition, the Business Planning Officer was able to confirm that 80% of the Scrutiny – Resource and Performance Panel had attended training which had included a session on risk and opportunity management on 4th June 2015.

Risk appetite can be defined as the amount of risk that an organisation is willing to seek or accept in the pursuit of its long term objectives. The Council's management have decided not to specifically define the organisation's risk appetite on the basis that this may vary depending on the decision that needs to be made. The Risk and Opportunity Management Framework communicates the need to anticipate, identify and proactively manage risk and opportunity in order to maximise resources, make effective decisions and ensure efficiency and customer focus. In addition, the Council uses a matrix approach based upon impact and likelihood to assess and score each risk and opportunity identified. A status of red, amber or green is provided according to the overall scoring of risk or opportunity following the evaluation process.

The Council's attitude to risk is reflected by the way in which risks are prioritised with energy and resources focused on 'red' risks requiring immediate action to manage the risk. Risk appetite is therefore considered on this basis.

Specific roles and responsibilities are summarised in the Risk and Opportunity Management Framework. All officers and Members have a role to play in delivering the Council's Framework, by making themselves aware of risks and opportunities within their day to day duties and ensuring that any issues are escalated as appropriate. It is part of 'mainstream line management' and therefore a duty of all managers to identify risks and opportunities within their area of responsibility and to follow the procedures set out in the Framework.

Project risks are reported to the Programme Board via monthly project highlight reports, however, it was noted that the role and responsibilities of the Programme Board were not detailed within the Risk and Opportunity Management Framework. **Recommendation 1** addresses this finding**.**

Based upon these findings, the assurance rating for the controls in respect of this risk is ***Substantial Assurance.***

Risk 2: Risks facing the Council are not identified and / or effectively managed or controlled

The risk identification process is detailed in the Risk and Opportunity Management Framework. Further information is provided in the Risk and Opportunity Management Toolkit, which includes matters in relation to the following:

- Identifying risk and opportunity at the planning stage to help inform decision making;
- Horizon scanning:
  - Internal factors – Strengths, Weaknesses, Opportunities and Threats (SWOT);
  - External factors – Political, Economic, Social, Technological, Legal and Environmental (PESTLE); and
- Understanding objectives and defining risk or opportunity using the *Cause, Event and Effect* method.

Corporate risks are in relation to the medium to long term aims and objectives of the Council and are identified by the Risk Strategy Board, which is made up of all members of CMT, the Business Development and Programme Manager and the Business Planning Officer. Corporate risks are monitored by the Risk Strategy Board through quarterly risk monitoring meetings. In addition, quarterly risk reports are produced for submission to the Executive and Scrutiny - Resource and Performance Panel.

Business risks are in relation to the Council's critical or key activities and are identified through the Council's Corporate Delivery Plan. Business risks are reviewed and updated on a quarterly basis by the relevant members of the Corporate and Senior Management Team. Any risks which are red after residual scoring are reported to the Performance Improvement Board and escalated to the Risk Strategy Board if necessary.

Operational risks are encountered by managers and staff during their day to day operational activities. They are reviewed and updated on a quarterly basis by the Senior Management Team. As with business risks, any risks which are red after residual scoring are reported to the Performance Improvement Board and escalated to the Risk Strategy Board if necessary.

Project risks are identified by the relevant Project Manager and are reported to the Programme Board via monthly project highlight reports. With the exception of project risks, all risks are recorded on the TEN Performance Management System which is available to all staff via the intranet. The Auditor was advised that project risks would also be recorded on the TEN Performance Management System by the end of quarter two.

The Risk and Opportunity Management Toolkit communicates the need to 'keep horizon scanning constantly' in order to continuously identify risks and opportunities.

The Council's Corporate Delivery Plan for 2016/17 sets out the Council's Critical Outcomes and how it will deliver these over the forthcoming year in order to achieve the Council's vision and priorities. Auditor review of the corporate risk register on 2nd June 2016 confirmed that all 18 risks were linked to the Council's Critical Outcomes.

Although risks are not categorised within the corporate risk register, Auditor review confirmed that external, operational and change related risks had been considered and documented. The Council recognises that all risks should be clearly defined to ensure that the potential effects of each risk are clearly understood. The Risk and Opportunity Management Framework refers to the *Cause, Event and Effect* method in order to achieve this. Auditor review of the corporate risk register on 2nd June 2016 confirmed that of the 18 risks recorded:

- 56% of risks described the cause and effect;
- 33% of risks described the effect only; and
- 11% of risks described the cause only. **Recommendation 2** addresses these findings**.**

A standard methodology for considering the impact and likelihood of risks is detailed in the Risk and Opportunity Management Framework. An assessment of the impact (the effect a risk would have, should it occur) and likelihood (the probability that it will occur) is carried out for each risk and scored accordingly. The criteria for scoring impact and likelihood are as follows:

Impact	**Major**	**Significant**	**Moderate**	**Minor**
Score	4	3	2	1
Likelihood	**Very Likely**	**Likely**	**Unlikely**	**Very Unlikely**
Score	4	3	2	1

The two scores are multiplied to establish the overall risk score (inherent score) after which a risk response is identified using the 5T method (treat, transfer, tolerate, terminate or take the opportunity). The risk is then scored again to establish the residual score. Auditor review of the corporate risk register confirmed that the impact and likelihood had been considered for each of the 18 risks detailed. Furthermore, all risks had been scored accordingly and a risk response had been identified using the 5T method. It was noted that the residual score of the following risk was greater than the inherent score detailed:

CR 11 *Constitution is limited in its delegations and flexibility and leads to delayed decision making.*

Although actions had been taken to mitigate this risk, a delay in completion had increased the impact from an inherent score of 6 (amber) to a residual score of 9 (red). The Business Planning Officer advised that a new version of the Constitution would be in place during 2016/17 in order to manage this risk to an acceptable level.

The Business Planning Officer is responsible for the development of the Risk and Opportunity Management Framework and the processes and systems to manage opportunity and risk. This includes the co-ordination of the corporate risk register. Auditor review confirmed that all 18 corporate risks had a named risk owner(s) as at 14th June 2016. Furthermore, sample testing of five corporate risks confirmed that appropriate action plans and timescales were in place; in addition, all five risks had been reported at the appropriate level.

Auditor review of the Business and Operational risk registers as at 12th May 2016 confirmed the following:

Business risks:
All 60 risks recorded in the business risk register had a named risk owner(s) and were linked to key activities; however, the following issues were identified:

- 8% of the risks recorded did not include a risk mitigation;
- 7% of the risks recorded did not include a residual score; and
- 3% of the risks recorded did not include an accurate residual score.

Operational risks:

- All 66 risks recorded in the operational risk register had a named risk owner(s) and with the exception of one risk, all risks did include a risk mitigation. **Recommendation 3** addresses these findings**.**

Based upon the audit findings, the assurance rating for the design of controls in respect of this risk is ***Substantial Assurance*** and the rating for compliance with these controls is ***Sufficient Assurance****.*

Risk 3: Lack of / no assurance that risk management is effective
A full review of risks and opportunities is undertaken annually as part of the Business Planning Process. Operational risks and opportunities are identified in line with the production of the Corporate Delivery Plan and Team Plans.

The Council has a number of monitoring and review mechanisms in place to ensure that there is clear accountability for managing risks. All risks should be monitored and reviewed on a quarterly basis at a minimum, in line with governance arrangements set out in the Risk and Opportunity Management Framework. Staff are advised to consider the following when reviewing risks:

- Is the risk still relevant?
- Have there been any changes or movement to the risk and its mitigations?
- Has anything occurred which might change the impact and / or likelihood and the risk score?

- Are the mitigations effective and what has the progress been?
- If the risk is increasing, are any further mitigations needed to prevent its occurrence?
- If the risk is decreasing, can any of the mitigations be relaxed?
- Are there any new or emerging risks?

Risk management forms a key part of the decision making process within the Council. All Committee reports and business cases contain a section to record the risk implications associated with the content of the report or project. The Scrutiny – Resource and Performance Panel receive quarterly reports in relation to the Council's corporate risk register, however, it was noted that the role and responsibilities of the Panel with regards to risk had not been detailed within the Council's Constitution. The Business Planning Officer advised that a new version of the Constitution would be in place during 2016/17. **Recommendation 4** addresses this finding.

Based upon the audit findings, the assurance rating for the design of controls in respect of this risk is ***Sufficient Assurance*** and the rating for compliance with these controls is ***Substantial Assurance****.*

3. LIMITATIONS TO THE SCOPE OF THE AUDIT

This is an assurance piece of work and an opinion is provided on the effectiveness of arrangements for managing only the risks specified in the Audit Planning Record.

The Auditor's work does not provide any guarantee against material errors, loss or fraud. It does not provide absolute assurance that material error, loss or fraud does not exist.

4. ACTION PLAN

The following Action Plan provides a number of recommendations to address the findings identified by the audit. If accepted and implemented, these should positively improve the control environment and aid the Council in effectively managing its risks.

Action Plan

Rec No.	ISSUE	RECOMMENDATION	Management Comments	Priority	Officer Responsible	Due date
1	Project risks are reported to the Programme Board via monthly project highlight reports, however, it was noted that the role and responsibilities of the Programme Board were not detailed within the Risk and Opportunity Management Framework. There is a risk that decisions may not be made at the appropriate level if all roles and responsibilities are not clearly defined and communicated. This could lead to inefficiencies in the risk management process.	All roles and responsibilities in relation to risk management should be clearly defined and communicated. In particular, the Risk and Opportunity Management Framework should include the role and responsibilities of the Programme Board to reflect the current structure that is in place within the Council.	Agreed: Projects are monitored through either the programme board or Performance Improvement Board. An addendum will be appended to the risk and opportunity management framework detailing the roles and responsibilities and will be formally incorporated at the next bi-annual adoption by Council	Low	Head of Finance and Corporate Services and S151 Officer	30th September 2016
2	Auditor review of the Corporate risk register on 2nd June 2016 confirmed that of the 18 risks recorded: • 33% of risks described the effect only; and • 11% of risks described the cause only. A lack of clarity in defining risks could lead to a poorly formulated risk response which could result in the risk materialising.	All risks should be clearly defined in accordance with the Risk and Opportunity Management Framework. In addition, the specific risks which have been identified as describing only the cause or effect should be updated by the relevant risk owner(s).	Management is confident that the inherent and residual risks are correctly scored on line with the framework. The business planning officer will undertake a rolling programme of reviews to ensure that all risks record the cause, event and effect	Medium	Head of Finance and Corporate Services and S151 Officer	Ongoing – 1st review by end of Sept 16

Rec No.	ISSUE	RECOMMENDATION	Management Comments	Priority	Officer Responsible	Due date
3	Auditor review of the Business and Operational risk registers as at 12th May 2016 confirmed the following: **Business risks:** All 60 risks recorded in the Business risk register had a named risk owner(s) and were linked to key activities; however, the following issues were identified: • 8% of the risks recorded did not include a risk mitigation; • 7% of risks recorded did not include a residual score; and • 3% of risks recorded did not include an accurate residual score. **Operational risks:** All 66 risks recorded in the Operational risk register had a named risk owner(s) and with the exception of one risk, all risks did include a risk mitigation.	Appropriate controls should be in place to ensure that the Business and Operational risk registers are accurate and up to date. In addition, the issues identified should be reported to the relevant risk owners and they should be advised to update the risk registers accordingly.	Review of 25% of business and operational risks will be undertaken each quarter to ensure all fields are complete. Accountability for risks remains the responsibility of the risk owner	Low	Head of Finance and Corporate Services and S151 Officer	30th September 2016

Rec No.	ISSUE	RECOMMENDATION	Management Comments	Priority	Officer Responsible	Due date
4	The Scrutiny – Resource and Performance Panel receive quarterly reports in relation to the Council's Corporate risk register. It was noted, however, that the role and responsibilities of the Panel with regards to risk had not been detailed within the Council's Constitution. The Business Planning Officer advised that a new version of the Constitution was due to be in place during 2016/17. There is a risk that decisions may not be made at the appropriate level if all roles and responsibilities are not clearly defined and communicated. This could lead to inefficiencies in the risk management process.	The Scrutiny – Resource and Performance Panel's role and responsibilities in relation to risk should be clearly defined in the Council's Constitution to ensure that appropriate governance arrangements are in place.	The Council will receive a report of possible changes to the constitution in July 2016 following consideration by the constitutional review committee. This role is not in the current changes that have been consulted on and will be considered as part of the next review stage, Management consider the scrutiny of risks by the performance scrutiny panel adequate discharges member oversight and challenge of the corporate risks of the Council	Medium	Head of Finance and Corporate Services and S151 Officer	31st March 2017

Glossary

The Auditor's Opinion

The Auditor's Opinion for the assignment is based on the fieldwork carried out to evaluate the design of the controls upon which management relay and to establish the extent to which controls are being complied with. The table below explains what the opinions mean.

Level	Design of Control Framework	Compliance with Controls
SUBSTANTIAL	There is a robust framework of controls making it likely that service objectives will be delivered.	Controls are applied continuously and consistently with only infrequent minor lapses.
SUFFICIENT	The control framework includes key controls that promote the delivery of service objectives.	Controls are applied but there are lapses and/or inconsistencies.
LIMITED	There is a risk that objectives will not be achieved due to the absence of key internal controls.	There have been significant and extensive breakdowns in the application of key controls.
NO	There is an absence of basic controls which results in inability to deliver service objectives.	The fundamental controls are not being operated or complied with.

Category of Recommendations

The Auditor prioritises recommendations to give management an indication of their importance and how urgent it is that they be implemented. By implementing recommendations made managers can mitigate risks to the achievement of service objectives for the area(s) covered by the assignment.

Priority	Impact & Timescale
HIGH	Management action is imperative to ensure that the objectives for the area under review are met.
MEDIUM	Management action is required to avoid significant risks to the achievement of objectives.
LOW	Management action will enhance controls or improve operational efficiency.