



# **RISK MANAGEMENT POLICY, STRATEGY AND FRAMEWORK**

**October 2012**

## Document Version Control

1.	September 2004	Original Policy, Strategy and Framework set up
2.	September 2005	Altered to include risk management performance indicators
3.	April 2007	Altered to reflect changes in responsibilities
4.	August 2010	Altered to reflect changes in responsibilities
5.	May 2011	Altered to shorten the document
6.	October 2012	Altered the presentation of risk management performance indicators

### Ownership:

- Policy developed by the officer risk management group, approved by corporate management team and cabinet and promoted and scrutinised by the audit committee.

## INDEX

1. Policy Statement
  2. Statutory background to Local Authority Risk Management;
  3. Risk Management Framework;
  4. Midlothian's Code of Corporate Governance;
  5. Responsibility for Risk Management;
  6. Specialist Risk Management Adviser;
  7. Adoption of Risk Management Standards;
  8. Annual Risk Control Programme;
  9. Corporate Management Team and Corporate Risks;
  10. Heads of Service and Service/Operational Risks;
  11. Project Managers and Project Risks;
  12. Community Planning Risks;
  13. Risk Registers;
  14. Risk Management Group of divisional representatives;
  15. Contingency Planning Group;
  16. Risk Appetite and Residual Risk;
  17. Risk Transfer;
  18. Risk Management Training and Awareness;
  19. Risk Management Statements in Reports;
  20. Risk Management included in Major Strategies and Plans;
  21. Risk Management in Business Transformation;
  22. Risk Assessment of Vulnerable Clients;
  23. Strategic Environmental Assessment
  24. Health and Safety;
  25. Risk Analysis in Option Appraisal;
  26. Preparation for External Inspections;
  27. Preparation for New Legislation;
  28. Risk Management in Partnership Working;
  29. Internal Audit and Risk Management;
  30. Risk Performance and Scrutiny;
  31. Risk Management and the Audit Committee;
- Appendix 1 - Risk Management - Risk Assessments Techniques
- Appendix 2 - Risk Management Performance Indicators

## **1. POLICY STATEMENT**

Midlothian Council is wholly committed to the management of risk exposures within its control in order to safeguard its employees, protect its assets, preserve and enhance service delivery to its population, maintain effective stewardship of public funds, ensure good Corporate Governance and promote a favourable corporate image free of reputation damage.

The Council will promote an inclusive approach to Risk Management through the establishment of a Risk Management Framework representing all areas of the Council. This framework forms the Council's strategy and will act as a focal point for promoting Risk Management within the Council and raising awareness of managers and employees of their obligation to take responsibility for good risk management, to take ownership of risks and to share best practice in addressing these.

It is the Council's duty to embed Risk Management throughout the Council and to encourage it to be part of the culture of the Council. Standards and procedures will be promoted Council-wide to help identify and analyse risks in all areas, allowing for appropriate controls to be put in place. This will be supported by a structured, open approach on both Corporate and Operational levels.

The Council will continue to develop its Risk Management Strategy, which will be supported by Corporate, Operational and Project Risk Registers to record risks in a systematic way and review these regularly to ensure exposures are managed within agreed and acceptable levels.

Through adoption of this policy, Midlothian Council will continue to promote Risk Management throughout the Council, ensuring close links with the decision-making processes, corporate aims and objectives, service plans, project management, performance, change management, new legislative and regularity requirements, business continuity, insurance and health and safety. This in turn will allow the Council to build on its successes and seize opportunities with greater confidence.

## **2. STATUTORY BACKGROUND TO RISK MANAGEMENT IN LOCAL AUTHORITIES**

This is contained within the Local Government in Scotland Act 2003, commonly referred to as the 'Best Value and Community Planning Act'. This Act brought new risk management responsibilities to Councils to assess risk at all levels and mitigate it in so far as it doesn't impact heavily on corporate aims and objectives. Best Value Guidance supplied by the Government and others builds on this and indicates that a Council that does not control, or take, risk is unlikely to be a Best Value Council. In reality the Council is looking towards avoiding serious:-

- Financial loss (in fact it may wish to take controlled risk to achieve robust financial stewardship);
- Disruption to services (in fact it may wish to take controlled risk to enhance services further);
- Damage to the area/environment (in fact it may wish to take controlled risk to enhance the area/environment);
- Reputation Damage; and

- Missing opportunities (in fact it may wish to take controlled risk to improve the area and meet need).

It is amplified to elected members, managers, partners, independent members on the Audit Committee and other stakeholders that risk management in local government is a **Statutory Duty**.

### **3. RISK MANAGEMENT FRAMEWORK**

The Council's policy on risk management acts in a dual way. Below, it not only articulates the policy but the reader gains an impression of the governance of risk management, its organisation, the roles and responsibilities, the routines, the 'joining-up' of risk management activity and the review of risk management performance. This is called the Council's **Risk Management Framework**.

### **4. MIDLOTHIAN'S CODE OF CORPORATE GOVERNANCE**

The Council's overarching Code of Corporate Governance indicates that the authority has a risk management policy and other structures listed elsewhere in this document. The Code is approved by Council and is reviewed and updated every two years. It is regularly audited by external and internal audits.

### **5. RESPONSIBILITY FOR RISK MANAGEMENT**

As a corporate body, Midlothian Council is responsible for the management and control of risk within the authority.

Not only should officials be managing risk automatically through their management duties, it should also be systematic and demonstrable, and the main risk exposures reported regularly to elected members.

Cabinet is responsible for the Risk Management Policy, and receives mid-year and end-of-year monitoring reports.

The Corporate Management Team, led by the Chief Executive, is responsible for managing the policy dictates, the strategy, framework and for the annual Risk Control Programme.

The Audit Committee of elected and independent members is responsible for promoting robust risk management.

The Performance Review and Scrutiny Committee of elected members is responsible for reviewing and scrutinising performance, including headline risk management performance indicators.

The Head of Finance and Human Resources is responsible for facilitating and coordinating risk management across the Council, principally through the Risk and Audit Manager and the Risk Management Group.

Other Directors and Heads of Service are responsible for the management of risk within their services and projects.

Internal Audit has the responsibility of adopting a risk-based approach to the Internal Audit Strategy and Planning and to periodically examine the risk management policy, strategy and framework.

The role of the Risk Management Group is described later.

## **6. SPECIALIST RISK MANAGEMENT ADVISER**

This is the Risk and Audit Manager, through Risk and Audit Services. This risk management service facilitates and coordinates all the risk management work within the Council and ensures that this policy (and strategy and framework) is operating effectively.

As well as using internal resource and expertise, the risk management service uses the free risk management consultancy supplied by the Council's insurers. On the prompt of the Risk Management Group, around four times a year, the insurer can carry out surveys and provide reports for the Risk Management Group, senior and middle management and the Audit Committee. As examples, some previous surveys have covered school trips, legionella management compliance, asbestos management compliance, driving standards, motor accumulation at depots, fire prevention compliance, violent incidents control and the categorising and scoring of risks.

## **7. ADOPTION OF RISK MANAGEMENT STANDARDS**

The Council adopts the concept of Enterprise Risk Management (ERM) which monitors and controls threats in relation to risks and opportunities that could impede or achieve Council aims and objectives. This is 'downside' as well as 'upside' risk management. ERM is also sometimes referred to as 'Organisation-Wide Risk Management'.

ERM involves the Council making every attempt to avoid the pitfalls described in item 2 above. In so doing, it attempts to protect the following Council assets: People, Finances, Property, Integrity of Services, Integrity of Major Projects, Vehicles and Plant and Reputation.

The Council has adopted the Institute of Risk Management/Association of International Risk Management and Insurance Companies/Association of Local Authority Risk Managers (IRM/AIRMIC/ALARM) joint standards for risk management which are nationally recognised as best practice. These can be referred to in the IRM/AIRMIC/ALARM booklet.

Standard practice is adopted in terms of risk assessment where the two variables of likelihood and impact are applied to identifiable hazards.

The risk assessment techniques adopted are described in Appendix A.

## **7. ANNUAL RISK CONTROL PROGRAMME**

The Annual Risk Control Programme is normally developed through consultation between the Risk and Audit Manager, the Risk Management Group and the council's insurers and endorsed by the Audit Committee. The programme spots emerging risks on the horizon and existing risks that are troublesome and recommends headline actions to match residual risk to an agreed risk appetite.

This is the means by which the policy and strategy objectives for risk management will be achieved in the ensuing year of account and is normally a series of actions to be progressed by officials. The Policy, Strategy and Risk Control Programme are subject to a mid-year monitoring report to the Corporate Management Team, Cabinet and the Audit Committee a month later.

The Programme picks up any outstanding actions from the previous year. The Programme shows that within this Council, risk management is not 'bolted on' and is part of management thinking and activity.

The annual risk control programme seeks to stabilise or reduce risk exposures as well as insurance premiums.

## **9. CORPORATE MANAGEMENT TEAM (CMT) AND CORPORATE RISKS**

On a quarterly basis, the CMT receives a report on corporate risks. The number of corporate risks is limited to no more than a dozen in number and are risks that impact on all services across the council, hence the term 'corporate'. Major service and project risks are not included in the corporate risk register unless they become so problematic that they are likely to affect the rest of the Council.

Currently there are 12 corporate risks listed:-

- Employees
- Governance and Standards in Public Life
- Finance and Efficiencies
- Corporate Change and Transition
- Emergency Planning and Business Continuity Management
- Internal Control Environment
- Customers and Performance
- Legal and Regulatory Compliance
- Condition of Assets
- Corporate Policies and Strategies
- Procurement; and
- Welfare Reform

These are considered to be where serious risk exposures could lie, requiring close review and robust controls.

The CMT can 'relegate' risks from the list and 'promote' others, if it so wishes. This is generally carried out after detailed analysis/discussion and comparison with other risks on the list.

The corporate risk register is reviewed by the Audit Committee twice-yearly.

## **10. HEADS OF SERVICE AND SERVICE/OPERATIONAL RISKS**

Heads of Service are responsible for service/operational risks. There are currently 10 risk registers of this nature and each Head of Service is instructed to list a handful of generic risks across their services and service-specific risks. At any stage, if a Head of Service identifies a risk exposure that could become a corporate threat, he/she has, in liaison with

the Risk and Audit Manager, permission to invite CMT to elevate it to the Corporate Risk Register.

Service risks are reviewed quarterly as part of quarterly performance reporting.

## **11. PROJECT MANAGERS AND PROJECT RISKS**

In accordance with PRINCE2 principles, project managers are obliged to identify, evaluate and mitigate project risks. There is a requirement to report risk exposures to each Project Board every month. The main focus is in avoiding project delays, cost creep and not achieving project objectives.

## **12. COMMUNITY PLANNING RISKS**

The Community Planning Steering Committee maintains a high-level risk register which manages the headline community planning risks. Each strategic group manages a governance risk register in terms of their remits and services. The Steering Committee ensures that the strategic groups are managing risk properly.

## **13. RISK REGISTERS**

Risk Registers are crucial to the management and reporting of risk, are currently held in the covalent computer system and are the depositaries for risk registration. Principles of risk assessment are strictly applied and risk registers, whether hosting corporate, service/operational, project, community planning or new legislation risks must be updated at least quarterly. However, project risk registers are expected to be reviewed and updated monthly. All new and emerging risks of a threatening nature must be registered in a risk register immediately, and notified to the Risk Management Group for discussion.

Risks that are scored high or critical are automatically included in quarterly performance reporting to senior management, the Cabinet of elected members and the Performance Review and Scrutiny Committee of elected members.

## **14. RISK MANAGEMENT GROUP OF DIVISIONAL REPRESENTATIVES**

The Risk Management Group works to a remit, meets every six weeks, is chaired by the Risk and Audit Manager and is attended by divisional representatives. All 'risk' disciplines attend i.e. Risk Management, Internal Audit, Health and Safety, Insurance, Emergency Planning and Information Security, as well as Service Management in charge of potentially high risk scenarios.

The Risk Management Group monitors risk performance targets, provides facilitation/coordination/guidance to all levels of management, discusses risk exposures, promotes risk management and internal control across divisions and suggests mitigating measures for risk hotspots. The Group minutes are issued to Divisional Management Teams and the members of the Audit Committee. Any important recommendations are presented to CMT.

Every quarter, the Group assesses its own effectiveness in terms of promoting robust risk management.



## **15. CONTINGENCY PLANNING GROUP (CPG)**

The CPG meets every six weeks, is chaired by the Director, Corporate Resources and focuses on compliance with the Civil Contingencies Act and potential loss of accommodation, computer systems, staffing and other resources as well as planning for any disasters in the community. There are Emergency Plans, Divisional and Generic (e.g. IT) Business Continuity Plans as well as Incident Response and Bomb Threat Plans.

The Contingency Planning Officer facilitates and coordinates all emergency planning, incident response planning and business continuity management matters including the testing of plans and dry-run exercises.

The CPG also monitors Emergency Planning and has input to the Lothian and Borders Strategic Coordinating Group Community Risk Register. The Group reports to CMT and occasionally the Audit Committee.

## **16. RISK APPETITE AND RESIDUAL RISK**

It is vital that every operational service, the corporate body and project managers effectively assess where the risk appetite lies. Any red (high) and yellow (medium) risks are likely to be in excess of a designated risk appetite.

Managers are obliged to identify (within set timescales) extra control measures to bring the residual risk into line with an agreed risk appetite.

The residual risk and the risk appetite are hosted in the covalent computer system and are agreed and set by senior management.

Risk appetite is a regular focus for managers and the Risk Management Group.

## **17. RISK TRANSFER**

Wherever feasible and cost effective, the Council will transfer the risk to another party. An example is insurable risk where the risk is carried by the insurer in lieu of insurance premiums and the Council bearing any deductibles and excesses.

Another example is the PPP contracts for Secondary and Primary Schools where an external contractor accepts some of the risk for a monthly payment.

Insurance provides vital cover for the Council but insurance premiums and excesses are challenged and the Council's engages an experienced broker to introduce, and relate, the Council to the insurance market.

Insurance claims experience is monitored through the Risk Management Group which reviews trends, spots potential problems and recommends risk mitigation actions.

## **18. RISK MANAGEMENT TRAINING AND AWARENESS**

Training on effective risk management is carried out by the Risk and Audit Services, principally the Risk and Audit Manager. Occasionally, an external party, such as the

Insurer, may be called upon to assist. Training is seen as vital to maintain buy-in and consistency of risk management.

Training is installed so that risk managers can effectively contribute to the management of significant risk exposures and work problems. Training is also aimed at Elected Members of the Council, especially if they are new to the role. Overall training includes:-

- A dedicated Risk Management website (Finance intranet > FAQs > Risk Management) where there are guidance documents of various kinds;
- Risk workshops;
- Bespoke training for any changes to the posts of Chief Executive, Director, Head of Service and Third Tier Manager;
- A dedicated training guide for Elected Members;
- A step-by-step guide to the Covalent/Risk software;
- Regular meetings with Heads of Service and Project Managers; and
- Proactive guidance provided on an 'as required' basis.

## **19. RISK MANAGEMENT STATEMENTS IN REPORTS**

All levels of Management have guidance on how these statements should be compiled and presented in official reports to elected member committees, the CMT and Business Transformation Groups, with the aim of having proper and meaningful risk data supporting policy/practice decisions. Periodically, the Risk and Audit Manager reviews a sample of the statements to ensure that they are robust.

No policy changes can be accepted unless the risk implications are fully expressed. There is a particularly important requirement to assess financial risks when committing significant sums of expenditure.

## **20. RISK MANAGEMENT INCLUDED IN MAJOR STRATEGIES AND PLANS**

Risk assessment supports many of the Council's main strategies and plans i.e. the Strategy or Plan may highlight what the risks are and provide risk management solutions to help achieve the strategy or plan.

## **21. RISK MANAGEMENT IN BUSINESS TRANSFORMATION**

The Council's Business Transformation Programme (BTP) is bringing major changes to the way the Council operates, in response to the economic climate.

This is considered to be a high-risk area for the Council and therefore the BTP has its own risk management strategy but operates risk registers and risk reporting through the covalent computer system and project boards, and overall through the Business Transformation Board. .

## **22. RISK ASSESSMENT OF VULNERABLE CLIENTS**

Throughout personal services provided by the Council, where vulnerable clients are involved, the principles of risk assessment are applied rigorously, using recognised methods.

## **23 STRATEGIC ENVIRONMENTAL ASSESSMENT**

Strategic Environmental Assessment (SEA) is a legal requirement under the Environmental Assessment (Scotland) Act 2005 that applies to all qualifying plans, strategies, programmes and policies.

The risk of non-compliance is managed through a risk register within the Planning and Development Service.

## **24. HEALTH AND SAFETY**

In accordance with the law and regulation, the Council adopts a robust means of risk assessment to ensure the health and safety of employees.

Health and safety policies are updated regularly and a programme of training and audits is carried out.

Health and safety initiatives are progressed in line with best practice.

## **25. RISK ANALYSIS IN OPTION APPRAISAL**

The Council has a corporate option appraisal system which supports the Capital Investment Strategy and any other major transformation decisions. Whenever options are identified, the risk management service assists in risk analysis; the threats and opportunities of each option.

## **26. PREPARATION FOR EXTERNAL INSPECTIONS**

Generally, external inspectors seek details of the Council's Risk Management policy and framework and we attempt to demonstrate effective and ongoing risk management through this framework.

## **27. PREPARATION FOR NEW LEGISLATION**

All major pieces of legislation are risk assessed and reported to the relevant Divisional Management Team and occasionally the Corporate Management Team and Elected Members e.g. Welfare Reform Act. If there are considerable resource issues, Cabinet may receive a report.

## **28. RISK MANAGEMENT IN PARTNERSHIP WORKING**

If any of the Council services enter into a partnership agreement, management normally risk assesses this first.

## **29. INTERNAL AUDIT AND RISK MANAGEMENT**

The three-year Internal Audit Strategy and Annual Internal Audit Plan is risk-based and concentrates on high risk activities like the main Financial and IT systems, Corporate Risks and Fraud Prevention. Internal Auditors are trained to examine management perceptions and control of risk. Each internal audit normally strengthens the Council's management of risk.

### **30. RISK PERFORMANCE AND SCRUTINY**

To support quarterly divisional and 'whole-council' performance reporting, managers are expected to review the risks under their management and flag any problem risks to their Head of Service and Director/Cabinet spokesperson. If a risk is very urgent, it should be elevated immediately.

While the ultimate test of the Council's Risk Management arrangements is through the Best Value reports of Audit Scotland, and also the demonstrable avoidance of problems, the Council has a number of ways of testing the efficiency and effectiveness of its management of risk viz:-

- Comparing Midlothian's Best Value report on risk management with the other 31 Scottish Councils;
- Benchmarking the Council's Corporate Risk Register with a handful of similar-sized Scottish Councils;
- Reviewing and applying best practice from the professional risk management bodies;
- Scrutiny of a risk management PI (high risks) by the Performance Review and Scrutiny Committee of elected members;
- Scrutiny by the Audit Committee in promoting quality risk management;
- Occasionally completing survey questionnaires and interpreting the results;
- An internal audit by the Internal Audit Team;
- An annual review of compliance with this policy;
- Twice yearly review of the success of the Council's Risk Management Group; and
- Review of around 20 PIs which are then reported to the Risk Management Group, CMT, Audit Committee and Cabinet. These PIs are in appendix 2.

### **31. RISK MANAGEMENT AND THE AUDIT COMMITTEE**

Midlothian's Audit committee principles, in accordance with the CIPFA Guidance of 2004 and the CIPFA Audit Committee Toolkit, are managed through the Audit Committee. The committee scrutinises the Risk Management Policy and Risk Control Programme, the Corporate Risk Register and this Framework and generally promotes the sound management of risk.

## **RISK ASSESSMENT: TECHNIQUES**

**(Available to all employees involved in risk management)**

### **PURPOSE OF THIS GUIDE**

- Give Managers an insight into the basics of risk management;
- Provide guidance on how to assess risk;
- Provide guidance on how to manage a risk register; and
- For managers to be compliant with risk management standards and Cabinet policy.

### **THE PROCESS**

Six simple steps to being a 'Risk Manager', in your role as a Midlothian Manager

- Identify risk;
- Evaluate risk;
- Set a risk target and appetite;
- Control, Transfer or Tolerate risk;
- Monitor risk on an ongoing basis; and
- Report risk regularly

### **WHAT IS RISK?**

The threat that an event or action will adversely affect the Council's ability to achieve its objectives and execute its strategies

Be especially aware of:-

- Financial Loss;
- Reputation Damage;
- Disruption to Services;
- Harm to the Environment;
- Harm to Employees or Midlothian citizens; and
- Missing genuine opportunities

### **TWO IMPORTANT VARIABLES**

Found in covalent:-

**Likelihood** – extent to which an event is likely to happen

**Impact** – the consequences of an event, the outcome

These are multiplied to arrive at the risk rating.

## STAGES OF RISK RATING

- Original Rating – the very first attempt at risk assessment, the starting-point and inherent risk, which never changes;
- Current Rating – where the risk is now; and
- Target Rating – where we want the risk appetite to be (and the date expected).

## WHAT IS RISKY? WHERE IS RISK?

- Corporate Objectives.....it's vital in terms of best value and the Government and Council aims, that these are achieved
- Corporate Matters like Legalities, Compliance, Standards.....there are pitfalls in terms of fines, censure, reputation damage and corruption if risk is uncontrolled.
- Services.....any services impeded are likely to impact on Midlothian citizens
- Themes like health and safety, internal control and data protection.....which can lead to fines, censure and reputation damage
- New legislation.....are we ready for it, sufficient resource to enact it?
- Projects – change, computer, construction.....there could be serious cost creep, serious delays and the end-result may not meet objectives
- In external inspections.....possibility of criticism and reputation damage

## RISK ASSESSMENT

- Combining the two variables of likelihood and impact to arrive at a risk rating;
- Leaves an impression of very low, low, medium, high or critical risk; and
- This can be at original, current or target ratings

## RISK RATING SYSTEM

### Likelihood

- Low;
- Medium; or
- High

### Impact

- Insignificant;
- Minor;
- Moderate;
- Major; or
- Critical

So the rating system is a 3 x 5.

## RISK RATING RESULTS

Covalent works out the risk rating for you and you will find that any rating:-

- Between 1 and 5 is very low risk – green
- Between 6 and 10 is low risk – green
- Between 11 and 16 is medium risk – yellow
- Between 17 and 22 is high risk – red
- Between 23 and 25 is critical risk – red

The grid below gives a brief indication. Red ratings should be controlled immediately or through a staged process.

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Critical
High					
Medium					
Low					

Likelihood

## RISK REGISTERS METHOD FOR SCORING RISKS

Remembering from above that risk assessment is made up of 2 variables

### VARIABLE 1 - LIKELIHOOD

### 3 – High

- Certain to happen
- Not absolutely certain to happen but very strong likelihood

### 2 – Medium

- Has happened before, but intermittently
- Mixed opinion on whether it could happen

### 1 – Low

- Has never happened before
- Highly unlikely to happen

## VARIABLE 2 - IMPACT

Each risk exposure should choose one or more of the boxes

Impact/ Problem	Financial Loss/Leakage – in terms of affecting the Council's overall financial position	Reputation (this includes serious ultra vires/reputati on episodes)	Harm to People – Employees or the Public	Disruption to Services/Obj ectives/Major Projects	Harm to Environment	Missing Opportuniti es
Insignificant	Box 1  None	Box 2  Overnight but transient news which will fade away and leave no permanent damage	Box 3  No injury/harm to any person	Box 4  Hardly any impact at all  Previous ground easily recovered	Box 5  No harm	Box 6  Very marginal had opportunity been taken
Minor	Box 7  Less than £100k and likely to be a one-off	Box 8  Short-term reputation at stake but will pass shortly	Box 9  First aid treatment, Non permanent harm up to 1 month	Box 10  Minor impact on service, project, legislative and corporate objectives  Will take a month to recover previous ground	Box 11  Little harm and can be easily cleaned up	Box 12  Would have helped but only marginal
Moderate	Box 13  Between £100k and	Box 14  Some mid- term	Box 15  Medical treatment	Box 16  Services can operate but at	Box 17  Some harm which can be	Box 18  Opportunity grasped



Impact/ Problem	Financial Loss/Leakage – in terms of affecting the Council’s overall financial position	Reputation (this includes serious ultra vires/reputati on episodes)	Harm to People – Employees or the Public	Disruption to Services/Obj ectives/Major Projects	Harm to Environment	Missing Opportuniti es
	£1m but there could be some delays in stemming the leakage	reputation embarrassment which will pass in time	required.  Semi-permanent harm up to a year.	reduced capacity with some inefficiencies  Statutory and corporate duties barely met  Will take 1 month to 6 months to recover previous ground	rectified over a medium period of time	would have been very useful
Major	Box 19  Major loss of between £1m and £5m with possible ongoing leakage	Box 20  Serious damage for a while which will have some lasting impression of Midlothian	Box 21  Extensive injury, major permanent harm	Box 22  Significant impact on service provision and statutory and corporate duties  Could take between 6 months to a year to recover previous ground	Box 23  Serious harm which will take time to rectify	Box 24  Opportunity that only comes around every now and then and will have to wait
Critical	Box 25  Over £5m with possible ongoing leakage	Box 26  National news Watchdog criticism Government step-in.	Box 27  Immediate death or probable death	Box 28  Unable to function, inability to fulfil obligations, especially statutory and corporate.  Could take over a year to recover previous ground	Box 29  Severe harm and scarring. Censure high. Take a long time to recover	Box 30  Will have a lasting impact on the Council, from which it will take a long time to recover

## Appendix 2

### RISK MANAGEMENT PIs

PI	Measurement method	Desired Outcome
1. % of agreed corporate priorities that have been risk assessed in the year and reported	Review of risk registers; 100% coverage, each quarter.	Clear evidence of control of risk and corporate priorities progressed, or progressing unimpeded.
2. Corporate Risk Registers presented to the CMT at least quarterly during the financial year	Calendar achievement	Evidence of risk control
3. Local Code of Governance reviewed annually and used to produce the Council's Annual Statement of Governance	Calendar achievement and any required improvements identified	Satisfaction of external audit
4. Internal Audit Plan risk-based	External Audit review and achievement of the Plan	Satisfaction of external audit
5. Internal Audit reports focus on risk management	QA system and auditees judged on the control of risk	Clear demonstration that internal audits are assisting in the reduction of risk
6. Heads of Service risk registers reviewed/updated at least quarterly	Calendar achievement	Evidence of risk control
7. Project risk registers reviewed/updated monthly	Calendar achievement	Evidence of risk control
8. Community Planning risk registers updated at least quarterly	Calendar achievement	Evidence of risk control
9. Major new pieces of legislation risk assessed	Head of Service awareness > Risk and Audit Manager > Risk Management Group > Risk Assessment	Evidence at the end of any financial year that effective risk assessments have been carried out and risk is controlled
10. High risks reviewed quarterly by senior management, the Cabinet and Performance Review and Scrutiny Committee	Calendar achievement	Evidence of risk control
11. Business Transformation risk registers reviewed/updated at least quarterly	Calendar achievement	Evidence of risk control
12. Risk Management Statements in official reports to CMT and elected members are of a sufficiently high standard	Approval of reports by senior management	Evidence of risk control
	Sample tests by Risk and Audit Manager	Positive results from sample tests
13. Risk management actions in risk registers are dealt with on time	Head of Service Review and calendar achievement.	Evidence that actions are being raised, are going to add value and timescales have been achieved.
14. Risk management projects and risk management control	Calendar achievement	Risk management group satisfaction

<b>PI</b>	<b>Measurement method</b>	<b>Desired Outcome</b>
programme are monitored by the risk management group at least six times in a financial year		
15. The risk management group assesses its performance in promoting robust risk management at least quarterly	Calendar achievement	Consensus among group members that risk is being controlled
16. Insurance claims experience performance	Claims experience reviewed at each meeting of the Risk Management Group and any adverse experience rectified through various actions	Evidence that any adverse trends are being addressed
17. Deadlines have been met in insurance procurement years	Calendar achievement	Procurement team satisfaction
18. Each risk manager in charge of a risk register has a clear vision of where risk appetite should be and is comparing it at least quarterly to residual risk.	Risk and Audit Manager review Risk Management Group review	Risk appetites are realistic, are achieved or there are robust signs of the gap being closed between current risk and risk appetite.
19. Contingency Planning Work Plan achieved	Calendar achievement	Contingency Planning Group satisfaction
20. Health and Safety Work Plan achieved	Calendar achievement and compliance with Health and Safety Acts	Health and Safety Executive approval, as well as other means of inspection.  Evidence of compliance with health and safety policies
21. Insurance Work Plan achieved	Calendar achievement	Risk and Audit Manager approval
22. Information Security Work Plan achieved	Calendar achievement	Head of Customer Services approval
23. Risk Management website and training schedule assists the risk control programme	Monitoring by the Risk Management Group	Evidence of robust training events