Risk Management for Managers - Guidance on Risk Assessment

June 2009

Draft 2

Contents

Version No	Revision No	Revision Date	Process Holder
2	1	11.03.09	R. Homewood
	2	30.04.09	R. Homewood
	3	04.06.08	R. Homewood

1. Introduction

1 This simple guide is designed to assist Managers in working through the process of identifying, evaluating and managing risk.

2 Further guidance on Risk and Risk Management can be found in the Institute of Risk Managements publication “A Risk Management Standard”. It defines risk and risk management as:

> “The combination of the probability of an event and its consequences (ISO/IEC Guide 73)”.

3 The advice goes on to state “in all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside). Risk management is increasing recognised as being concerned with both positive and negative aspects of risk. Therefore this standard considers risk from both perspectives. In the safety field, it is generally recognised that consequences are only negative and therefore the management of safety risk is focused on prevention and mitigation of harm.

4 Risk management is a central part of any organisation’s strategic management. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. The focus of good risk management is the identification and treatment of these risks. Its objective is to add maximum sustainable value to all the activities of the organisation. It marshals the understanding of the potential upside and downside of all those factors which can affect the organisation. It increases the probability of success, and reduces both the probability of failure and the uncertainty of achieving the organisations overall objectives. Risk management should be a continuous and developing process which runs throughout the organisations strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organisations activities past, present and in particular, future.

5 Risk management must be integrated into the culture of the organisation with an effective policy and a programme led by senior management. It must translate the strategy into tactical and operational objectives, assigning responsibility throughout the organisation with each manager and employee responsible for the management of risk as part of their job description. It supports accountability, performance measurement and reward, thus promoting operational efficiency at all levels.

6 Risk can only be managed effectively if they have been clearly identified and their nature is properly understood. In stating risks, care should be taken to avoid stating impacts which may arise as being the risks themselves, and to avoid stating risks which do not impact on objectives; equally care should be taken to avoid defining risks with statements which are simply the converse of the objectives (table 1). A statement of risk should encompass the cause of the impact, and the impact on the objective (cause and consequence) that might arise.

Table 1

Risk	"Leads to" Exposure	"Results in" Consequence
Fire	Death/Injury Building/property/asset destroyed	Compensation claim Unable to provide service Displaced staff Press (negative) Fire investigation Corporate manslaughter charge

For a simplistic example HM Treasury has produced a detailed guide to risk management (table 2), which includes a useful table to illustrate the need for accuracy in risk identification, and is reproduced below:

Table 2

Objective – to travel by train from A to B for a meeting at a certain time		
Failure to get from A to B on time for the meeting	ß	This is simply the converse of the objective.
Being late and missing the meeting.	ß	This is a statement of the impact of the risk, and not the risk itself.
There is no buffet on the train so I get hungry	ß	This does not impact on the achievement of the objective.
Missing the train causes me to be late and miss the meeting		This is a risk that can be controlled by making sure I allow plenty of time to get to the station.
Severe weather prevents the train from running and me from getting to the meeting		This is a risk which I cannot control, but against which I can make a contingency plan.

2. Detailed Risk Management Arrangements

The Council's Risk Management Approach is described in detail in the following section.

STEP 1 – Define Objectives

Organisations are primarily concerned with the achievement of objectives. You need to know what you are trying to achieve before you can start to think about the risks that could have an impact on your success. Put simply, there is no value in identifying the risk that a train may be late, if you are not travelling by train that day.

The more clearly objectives are defined, the more it will help you to consider those risks that could actually impact on your objectives.

At Corporate level, the Council has an overarching vision for Hastings "to create an inclusive, successful and sustainable economy which brings a decent standard of living and quality of life to all our residents". This vision is underpinned by a number of Council Objectives that can be found in the Corporate Plan.

At Service Division level, Divisional Performance Plans show how each Division is helping the Council as a whole achieve its overall objectives. The Plans detail the objectives and priorities for service areas over the next twelve months.

At Project level, the relevant project brief or project initiation document details the aims and objections of the project.

At Partnership level, the partnership agreement or other formally agreed arrangements will detail the aims and objectives of the partnership.

STEP 2 – Identify Risks

Risk identification attempts to identify the Council's exposure to uncertainty. This is a key process, as we can only attempt to manage risks we have identified.

To ensure completeness and a degree of confidence that risk identification is systematic and consistently applied across the Council, Hastings has adopted a process for risk identification, which should be applied.

Our approach uses a framework of risk types. As risk management is part of our performance management culture, the types are currently built around the word PERFORMANCE as follows:

Political

E Government

Regulatory

Financial

Objectives and/or Opportunities

Reputation

Management

Assets

New Projects/Partnerships

Customers/Citizens

Environment

For further details, including examples of risk from each type, see Appendix A.

Having identified the significant risks, these are recorded in a Risk Register, which is created and maintained on the GRACE risk management system.

At Corporate level, Senior Management and Members will identify strategic and cross cutting risks through facilitated risk identification and assessment workshops. The risks identified are:

- Those that could significantly impact on the achievement of the Council's overall objectives and priorities.
- Recorded in the Strategic Risk Register.
- Used to inform Division risk identification.

At Divisional level, Operational Managers will identify those operational risks that could significantly impact on the achievement of the service objectives and priorities; using GRACE risk management system as well as any measures and actions to manage these risks.

At Project level, Project Managers will identify the risks that could impact on the successful delivery of the project. The risks identified are:

- Those that could significantly impact on the achievement of the project;
- Recorded in the Project Risk Register;
- Used to inform both Corporate and Operational risk identification.

At Partnership level, the key stakeholders will identify the risks that could impact on the successful delivery of the partnership. The risks identified are:

- Those that could significantly impact on the achievement of the partnership's aims and objectives;
- Recorded in the Partnership Risk Register;
- Used to inform both Corporate and Operational risk identification.

STEP 3 – Assess Risks

We don't have the resources to manage every risk all of the time, so we need to consider which risks are most likely to happen (likelihood) and what the impact would be.

Impact and likelihood of risks occurring are used to assess risk and are normally categorised as High, Medium or Low. Often these are first assessed assuming that there are no control measures in place to minimise the risk (frequently referred to as mitigating controls). This is known as Gross Risk assessment. However, for many of the Council's activities there will probably already be measures in place to minimise the risks identified and these Risk Control Measures should already be helping to minimise the likelihood or impact of the identified risks if the risk materialised. This is known as the "Net" Risk. Net Risk Impact and Likelihood are recorded in the Risk Register and the GRACE system automatically calculates the Net Risk Level depending on the Impact and Likelihood scores of high/medium/low attributed. Guidance on assessing the levels of Likelihood and Impact are attached at Appendix B.

Each Risk Control Measure must be allocated an Owner who is responsible for confirming the existence and effectiveness of the current control measure(s) and ensuring that any proposed measure(s) are implemented. Such accountability helps to ensure "ownership" of the control measure action.

The title and/or name of the Action Owner are recorded in the Risk Register.

If you need help assessing the likelihood or impact of a particular risk please contact the Audit Team on 01424 45(1508) who will be able to offer advice and support.

STEP 4 – Prioritise Risks

Hastings Borough Council Risk Management Approach aims to focus on those risks that, because of their likelihood and impact, make them priorities.

The net risk level (likelihood and impact) of each risk are plotted and prioritised using a simple 3x3 matrix.

The matrix uses a "traffic light" approach to show high (red), medium (amber) and low (green) risks.

Likelihood and Impact Matrix

IMPACT	**High**	**Medium 3**	**High 1**	**High 2**
	Medium	**Low 3**	**Medium 2**	**High 3**
	Low	**Low 1**	**Low 2**	**Medium 3**
		Low	**Medium**	**High**
	LIKELIHOOD			

Where Likelihood and Impact cross determines the risk level. For example, a risk assessed as High Likelihood and High Impact gives a Net Risk Level of High 3. A risk assessed as Medium Likelihood and Low Impact gives a Net Risk Level of Low 2.

Allocating a numeric helps to indicate the degree of Net Risk rather than simply Low/Medium/High.

The result of this prioritisation is recorded in the Risk Register.

STEP 5 – Respond to Risks

Most risks cannot be eliminated altogether and risk management involves making judgements about what level of risk is acceptable. Hastings Borough Council Risk Management Approach details four categories of response – transfer, treat, terminate and tolerate – known as the Four T's.

Response Categories

Response	Description
Treat	Some risks will need additional *treatment* to reduce their likelihood or impact. This response is most likely where the likelihood or impact is such that a risk has been identified as a high/red risk.
Tolerate	This response will be appropriate where you judge that the control measures in place are sufficient to reduce the likelihood and impact of a risk to a *tolerable* level and there is no added value in doing more.
Transfer	Some risks can be *transferred* to an insurer, eg legal liability, property and vehicles etc. Some service delivery risks can be transferred to a partner or contractor by way of a formal contract or written agreement. However, some risks cannot be transferred, eg reputation risks.
Terminate	In some instances, a risk could be so serious that there is no other option but to *terminate* the activity that is generating the risk.

High Risks generally any "net" red risks (ie those risks that appear in the High 1, High 2 or High 3 box of the matrix after taking any mitigating actions into account) are viewed as unacceptable in the first instance and should be "treated" by a separate management action plan wherever possible. At this stage some form of cost benefit analysis may be needed to ensure that the cost of further risk mitigation action does not outweigh the cost of tolerating the risk. It is possible that treatment for some risks may not be wholly possible and the final decision is that the risk must be tolerated,. In these circumstances it is essential that the details of consideration and conclusions are clearly documented and cross referred to the risk using the hyperlink facilities within the GRACE system.

The Corporate Management Team (for strategic risks), appropriate Divisional Management Team) for operational risks) or Project/Partnership Boards (for project or partnership risks) are responsible for considering additional management action plans and any cost benefit analysis. CMT, DMT or Project Board (as appropriate) will make the decision as to whether or not these risks will be treated further.

Amber Risks are acceptable, but the risk should be reduced as low as reasonably practicable. Contingency plans must be developed.

Green Risks are broadly acceptable.

The acceptance of a risk represents an informed decision to accept the impact and likelihood of that risk and is recorded as a "tolerated" risk in the Risk Register.

A Risk Owner must be allocated to each identified risk. Such accountability helps to ensure "ownership" of the risk is recognised and appropriate resources are allocated. The title and/or name of the Risk Owner must be recorded in the Risk Register.

These Risk Owners are responsible for:

- Ensuring that appropriate resources and importance are allocated to the process;
- Confirming the existence and effectiveness of the current mitigating actions and ensuring that any proposed mitigating actions are implemented;
- Providing assurance that the risks for which they are the Risk Owner are being effectively managed.

STEP 6 – Monitor Risks

Hastings Borough Council's approach is one where monitoring:

- Is part of existing performance monitoring timetables;
- Focuses on those risks that, because of their likelihood and impact, make them priorities; and
- Is delegated to one responsible body.

To achieve this, the following monitoring frequency must be followed:

Red	High risk, prompt action, monitor at least monthly.
Amber	Medium risk, contingency plan, monitor at least quarterly
Green	Low risk, monitor at least yearly

At Corporate level monitoring is undertaken by the Corporate Management Group supported by the Chief Auditor.

At Divisional level monitoring is undertaken by individual Divisional Management Teams supported by the Divisional Risk Champion.

At Project level monitoring is undertaken by the Project Review Board supported by the relevant Head of Projects and individual Project Managers.

At Partnership level monitoring is undertaken by individual Partnership Boards and with Contracts by the relevant Client Monitoring Officer.

STEP 7 – Review and Report

Effective risk management requires a reviewing and reporting structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place.

Regular internal reports will enable senior managers and Members to be more fully aware of the extent of the risks and the changes occurring to them.

These arrangements will enable:

- Regular monitoring of the risk identification and prioritisation process as an integral part of the existing service and corporate planning process;
- Regular monitoring and updating of the key risks facing service divisions;
- Assurance that mitigating actions are operating effectively;
- Quarterly reports to Lead Members through Performance Review meetings on the key risks facing the Council and its management;
- An annual review of the risk management strategy.

STEP 8 – Communicate and Consult

Continuing to raise awareness and provide training is vital. Risk management information is available on the Audit and Investigations intranet site, as well as through regular updates and guidance and awareness sessions. The level and nature of this will vary according to individual needs and external influences.

The Council's Risk Management Strategy is circulated to key stakeholders in partner organisations. The Policy and Strategy will be reviewed annually by the Corporate Risk Management Group to take account of changing legislation, government initiatives, best practice and experience gained within the Council. Any changes to the Policy and Strategy will be submitted to Audit Committee for comments before submission to Cabinet for approval.

This Guidance will be reviewed annually by the Corporate risk Management Group and updated as necessary to support managers in managing risk.

3. Risk Management Responsibilities

Cabinet

The Lead Member for Risk Management will be the Cabinet Member with responsibility for Resources.

All Cabinet Members are responsible for:

- Understanding the nature of risk.
- The strategic risks that the authority is faced with.
- The effective management of these risk by officers.
- Ensuring that the Strategic Risk Register is being effectively maintained and reviewed when changes occur that could affect the achievement of Corporate Objectives.
- Agreeing, where necessary, action to be taken on Key Strategic Risks.
- Approving the Risk Management Strategy.
- Receiving an annual report on the adequacy and effectiveness of Risk Management and Internal Control from the Chief Auditor.

The Chief Executive is responsible for:

- Ensuring good Corporate Governance of which Risk Management is a part.
- Signing off the Annual Assurance Statement and the Annual Governance Statement along with the Leader of the Council.
- Ensures that risks are fully considered in the strategic decision making process and that the Risk Management Strategy assists the Council in achieving its objectives and protecting its assets.

The Chief Executive's Nominee is responsible for:

- Leading on all risk management issues and acting as the Officer Risk Champion.

The Audit Committee is responsible for:

- Monitoring the effectiveness of the authority's risk management arrangements, receiving quarterly reports and reviewing the Risk Management Annual Report to Council.
- Seeking assurance that appropriate action is being taken on risks identified by Internal Audit and other inspectors.
- Reviewing the Annual Inspection Letter and Statement on Internal Control (SIC) to ensure that they properly reflect the risk environment and that action is being taken upon any improvement recommendations contained therein.

The Corporate Risk Management Group is responsible for:

- Implementing this strategy and reporting upon progress to Council via Corporate Management Group and Audit Committee.
- Annual review of the strategy and reporting results to Corporate Risk Management Group.
- Risk assessment of Corporate Objectives (in conjunction with Corporate Directors).
- Providing recommendations to Corporate Management Group on the Council's Risk Management Policy and framework and ensure that both are reviewed at least annually.
- Ensuring that Risk Management procedures and developments are regularly maintained and disseminated to officers.
- Receiving quarterly updates from each Division on their key risks to maintain and report on the corporate risk profile to Cabinet and Audit Committee via Corporate Management Group.
- Focusing and co-ordinating risk management activities throughout the Council to facilitate the identification, evaluation and management of all key business risks in accordance with an agreed Terms of Reference.
- Development, implementation and maintenance of the Risk Management Strategy.
- Making available to Corporate Management Group and Leadership Group a Risk Register in which Service, project and partnership risks and controls will be recorded.
- Annual review of the Strategy for adequacy and compliance with statute/best practice.
- Managing a Risk Management Fund to be used for risk management training, resource requirements and improvement.

The Corporate Management Group is responsible for:

- Identifying and (where appropriate) accepting, risks to Corporate Objectives and ensuring this data is recorded in the Strategic Risk Register in accordance with corporate guidance.

The Project Review Board is responsible for:

- Ensuring that all projects valued in excess of £50k are progressed in accordance with the Hastings Borough Council Project Management methodology.
- Scrutinising and challenging the Project Risk Assessment and where appropriate recommending approval to proceed to Risk Management Group.

- Overseeing risk management in major capital projects and reporting quarterly to Cabinet.

Corporate Directors are responsible for:

- Ensuring Heads of Service are familiar with this Strategy and the Risk Assessment Methodology.
- Ensuring the Divisional Risk Champions and Heads of Service receive timely risk training.
- Ensuring that Heads of Service maintain a current risk assessment for their areas of responsibility in the Risk Register in accordance with guidance provided by the Audit Team. Risk assessments will be maintained in accordance with these instructions for core services, projects and partnerships.
- Maintenance of the Strategic Risk Register (in conjunction with the Chief Auditor).
- Regularly monitoring risks to service delivery, project implementation, opportunities and partnership arrangements. A checklist is attached at Appendix C to evidence that significant issues have been considered, a copy of this should be forwarded to the Audit Team for any GRACE amendments required and for audit purposes.

Divisional Risk Champions are appointed by Heads of Service and are responsible for:

- Ensuring effective and consistent maintenance of Risk Registers within their Division.
- Identification of risk training requirements.
- Regular review of risk movements.
- Ensuring that where appropriate Operational Risk Registers inform the Strategic Risk Register to ensure consistency.
- Ensuring that reports to Corporate Management Group and Cabinet etc are informed of risk implications and methods by which risks will be managed.

The Head of Financial Services is additionally responsible for:

- Reporting to Risk Management group on the adequacy of external insurance arrangements, level of cover and internal provision.
- Management of the insurance function, including claims etc.
- Monitoring claims and suggesting ways in which risks can be minimised.

The Head of Environmental Health is responsible for:

- Overseeing the management of Health and Safety, reporting quarterly on policy development and compliance to the Corporate Risk Management Group.

Heads of Service are responsible for:

- Maintaining current risk arrangements for their areas of responsibilities in the Operational Risk Register in accordance with guidance from the Audit Team.

- Appointing Divisional Risk Champions.

- Regular maintenance of the relevant area of the Operational Risk Register. Risks relating to core service delivery are likely to remain stable, however those relating to new project undertakings and new or existing partnerships are frequently subject to external factors and risk may change as a consequence.

- Regular review of all high risks identified within their Divisions, ensuring that action is taken to either reduce these to an acceptable or refer them to Corporate Risk Management Group if the risk cannot be accepted and/or needs additional resources/input from other Heads of Service/Officers.

- Ensuring reports to formal committees and Cabinet include a statement by the report originator that the risk assessment methodology has been applied where appropriate. Where the level of risk has been assessed as "high", reports must include a short statement on the implications and show how the risk will be managed.

Service Managers are responsible for:

- Ensuring that risk is continuously re-assessed and risk register details changed accordingly. (The Chief Auditor will monitor changes and where necessary take follow up/reporting action.)

Officers are responsible for:

- Recognising, managing and reporting to the Head of Service upon the risks they encounter on a daily basis.

The Directorate Performance Review Groups are responsible for:

- Ensuring that Service Delivery Plans, priorities and budgets reflect consideration of risks when constructing the relevant work programmes for that year, and that risk management processes are activated where necessary to maintain performance.

- Ensuring that Operational Risk Registers are reviewed on a quarterly basis.

The Chief Internal Auditor is responsible for:

- Reviewing the Annual Governance Statement with specific reference to risk management prior to approval by Audit Committee.

- Ensuring the Hastings Borough Council risk management system complies with best practice.

- .

- Developing risk related learning software.

- Promoting risk management awareness throughout the authority through publicity material, guidance and update notes and maintenance of a Risk Management Intranet site.

- Acting as facilitators, enabling and guiding managers and staff through the risk management process, usually as part of a self assessment exercise, without themselves necessarily becoming directly involved in the process.

- Acting as risk and control analysts providing managers with expert advice on the identification and assessment of business risks and the design of control and mitigation strategies.

- Making available to management tools and techniques used by internal audit to analyse risk and controls.

- Providing a centre of expertise for managing risk.

- Monitoring the risk register for significant changes recorded by Service Managers and if appropriate report via the Audit Committee on these changes and the adequacy/effectiveness of controls established to mitigate risks.

- Reporting to the Chair of Corporate Risk Management Group and the Audit Committee upon the existence of any unaddressed high risks over the period agreed in the policy statement.

- Ensuring the confidentiality, integrity and availability of the Strategic Risk Register.

- Reporting annually to the Audit Committee via Corporate Management Group on the adequacy and effectiveness of risk management arrangements, highlighting the areas of greatest risk.

- Advising the Corporate Risk Management Group on the actions necessary to maintain this Strategy to ensure compliance with statutory requirements and best practice.

- Maintaining a risk based strategic audit programme that is informed by the Strategic Risk Register.

Head of People and Organisational Development is responsible for:

- Provision of risk training to officers

Audit Programme

Internal audit will maintain a strategic 3 year plan. It is driven by the risks identified by management and recorded in the Corporate Strategic Risk and Service Risk Registers and by the need to review all major systems within the 3 year period as identified by an Audit Need Analysis. The Audit Needs Analysis considers a number of factors which may influence the regularity and scope of internal audits, eg financial/operational materiality, strength and stability of system, previous internal and external audit findings.

Appendix A - Risk Types

The following are examples only and are not exhaustive. Officers undertaking risk assessments should be aware that other risks may be present depending upon the nature of the activity being assessed and external influences.	
Risk Type	*Example*
Political	Political personalities Member support / approval Electorate dissatisfaction Impact of election changes and new political arrangements
E-Government	Use of new technology Lack of / failure of existing technology Lack of / failure of disaster recovery arrangements Hacking or corruption of data, breach of security
Regulatory	Central Government policy Legislation Internal policies and regulations Grant Funding conditions etc Data Protection Freedom of information Race Equality and diversity Disability Discrimination Human Rights Employment law TUPE Health and Safety Potential for legal change Judicial Review
Financial	Budgetary Pressures Loss of or reduction of income Interest rates Inflation Financial management arrangements Investment Decisions Non compliance with Prudential Code Inadequate insurance cover External funding issues e.g. loss or reduction of funding and sustainability once funding ceases Weaknesses in systems and / or procedures that could lead to fraud or other loss Failure to obtain best value
Objectives and / or **O**pportunities	Failure to achieve financial or outcome objectives on core service delivery Failure to achieve financial or outcome objectives on projects Opportunities to add value or improve services to customers Opportunities to reduce waste and / or inefficiency Missed business, service or funding opportunities
Reputation	Negative publicity (local or national) arsing from service or project failure, theft or loss. Potential for legal challenges e.g. tribunal
Management	Key personalities Loss of key staff Recruitment and retention issues Internal management arrangements and protocols

	Lack of or inadequate management support Poor communication (verbal, written or electronic) Capacity issues – sufficiency Resource requirements Training issues Availability Sickness absence Emergency Preparedness and business continuity
Assets	Management and control of resources – land, property, equipment, vehicles, plant and Information Data protection Intellectual property rights
New Projects / Partnerships	Alignment with corporate objectives – vision, direction, aims, objectives Funding Governance Culture Partnership agreements – arrangements / adequacy / effectiveness / compliance New initiative / project Project management arrangements – best practice / adequacy / effectiveness / compliance (PRINCE 2) Project failure to deliver on time, to specification / user requirement Change programmes – new ways of working, organisation, new policies / procedures
Customers / **C**itizens	Demographic change, current and future changing needs and expectations Impact on customers / citizens if service or project fails Consultation and communication with (adequacy, effectiveness, satisfaction) Crime and disorder Customer protection Satisfaction Feedback H & S Physical Risk Mental health Sense of well being
Environment	Environmental impact of activities of the authority and / or it partners Recycling Green issues Energy efficiency & carbon footprint Land use Noise Contamination Pollution Planning implications Transportation Policies Green Procurement \Policy and procedures Sustainability

Appendix B – Assessing Measure of Impact and Likelihood

Impact - When allocating a Risk Score please ensure that this reflects the impact upon the authority, not the service.

Level Description	Example Detail
High Red	Death or life threatening Serious service failure impacts on vulnerable groups Negative national publicity, highly damaging, severe loss of public confidence Serious impact felt across more than one Directorate Legal action almost certain and difficult to defend Financial impact not manageable within existing funds and requiring Member approval for virement or additional funds i.e. in excess of £100,000 Non-compliance with law resulting in imprisonment Loss of, or permanent damage to, 'priority' environmental/historic resources
Medium Amber	Extensive, permanent/long term injury or long term sick Service failure impacts on property or non-vulnerable groups Negative local publicity, some loss of confidence, needs careful public relations Expected impact, but manageable within Directorate contingency plans Legal action expected Financial impact manageable within existing Directorate budget but requiring Director approval for virement or additional funds i.e. £20,000 - £100,000 Non-compliance with law resulting in fines Recoverable damage to 'priority', or loss of 'non-priority', environmental/historic resources
Low Green	Short term sick absence, first aid or medical treatment required Some risk to normal service but manageable within contingency arrangements Little if any scope for impact on vulnerable groups Possible negative customer complaints, unlikely to cause adverse publicity, no damage to reputation Possible impact, but manageable locally by Head of Service Legal action possible but unlikely and defendable Possible financial impact manageable within service budget i.e. less than £20,000 Non-compliance with regulations / standards or local procedures resulting in disciplinary action. Recoverable damage to 'non-priority' environmental/historic resources

Likelihood

Level Description	Example Detail
High Red	Has **happened** in the past **year**; or Is **expected** to happen in the next **year.** More than **50% probability. Controls known to be weak / ineffective in certain situations.**
Medium Amber	Has **happened** in the past **2 – 5 years**; or Is **expected** to happen in the next **2-5 years.** Between **25% to 50% probability. Controls known to have be inadequate / ineffective on occasions or in some situations**
Low Green	Has **not happened** in the past **5 years or more**; or Is **not expected** to happen in the next **5 years or more.** Between **1% to 25% probability. Controls believed to adequate and cost effective.**

Appendix C - Divisional Quarterly Risk Management Assurance - Check List

Review criteria	Y	N	Comments / Guidance
Have any objectives for your Division changed, e.g. new services or projects? If so, have new risks been identified along with corresponding mitigating actions?			
Have Service / Project / Partnership risks been clearly identified and adequately described?			**Risks *not* implications**
Are the risk owners still valid?			Is this person still the most appropriate risk owner?
Are the risks still valid?			Are the risks identified still relevant or has the event passed / circumstance now changed? Can the risk be closed?
Is the assessment of the net risk, i.e. likelihood / impact of risks occurring still valid?			Has this increased / decreased / remained the same?
Is the assessment of each mitigating action in reducing the likelihood of the risk and the impact, should it occur, still relevant?			Has this been correctly interpreted? E.g. the likelihood of major building damage is minimal but the impact, should it occur, would be major
Are mitigating controls still sufficiently effective and adequate?			
Head of Service to sign off to confirm that the above is correct and retain copy for audit inspection.			**Signed:** **Date:**