



City & County of Swansea

Draft

Corporate Risk Management Framework

Purpose

This framework describes the specific risk management activities that will be undertaken within the City & County of Swansea. The aim is to help managers at all levels apply the principles consistently across their area of responsibility.

CIPFA state that *“Risk management is important to the successful delivery of public services. An effective risk management system identifies and assesses risks, decides on appropriate responses and then provides assurance that the chosen responses are effective.”*

The Council recognises that it has a responsibility to manage risks effectively in order to reduce uncertainty in achieving its priorities and objectives and to benefit from opportunities. This framework applies to all Council staff and its principles should be applied when working internally or externally with partners and other stakeholders.

Definition of Risk

“Risk is an event, action, or lack of action that could adversely affect the Council’s ability to achieve objectives and to successfully execute its strategies. Risk arises as much from failing to capture opportunities whilst pursuing business objectives as it does from a threat that something bad will happen”

Approval

Title	Date

Reference No.: Version 1.10

Date: 14th February 2017

Author: Performance & Delivery

Website <http://staffnet/riskmanagement>

Contents

No	Title	Page
1	Foreword	3
2	Definition of Risk	4
3	Risk Management	4
4	Corporate Commitment to Risk Management	4
5	Aims of the Risk Management Framework	4
6	Risk Levels	4
	- Corporate Risks	4
	- Directorate Risks	5
	- Service Risks	5
	- Information Risks	5
	- Project and Programme Risks	5
7	Roles and Responsibilities	5
	- Leader / Cabinet and CEO / Corporate Management Team	5
	- Cabinet Members	6
	- Elected Members	6
	- Directors	6
	- Heads of Service	6
	- Council Officers and Managers	6
	- Internal Audit	6
	- Audit Committee	6
	- Responsible Officer	6
	- Updater	6
	- Administrators	7
	- Corporate Director (Resources)	7
	- Senior Information Risk Officer (SIRO)	7
	- Project and Programme Managers	7
8	Risk Management Cycle	7
8.1	- Step 1 Risk Identification	7
8.1.1	- Risk Categorisation	9
	- Strategic Risks	9
	- Operational Risks	9
	- Financial Risks	9
	- Regulatory Risks	9
	- Governance Risks	9
8.2	- Step 2 Risk Evaluation	10
8.3	- Step 3 Risk Response	11
8.4	- Step 4 Risk Monitoring and Control	11
9	Risk Escalation	13
10	Performance Improvement & Risk Management Framework – on a page	14

Document Control

Version No.	Revision Date	Summary of Changes
1.10	2016/17	<i>Foreword</i> – amended
		<i>Definition of Risk</i> - added
		<i>Definition of Risk Management</i> - added
		<i>Corporate Commitment to Risk Management</i> - amended
		<i>Aims of Risk Management</i> – amended
		<i>Benefits of Risk Management</i> - deleted
		<i>Risk Levels</i> – added
		<i>Roles & Responsibilities</i> - amended
		<i>Risk Management Cycle</i> – amended
		<i>Risk Escalation</i> – added
		<i>Glossary of Terms</i> - deleted

DRAFT

1. Foreword

This framework aims to help employees, senior managers and elected Members to apply risk management principles consistently across their area of responsibility.

The intention of the framework is to help ensure that risk management is embedded into the culture of the Council, with members, managers and officers at all levels recognising that risk management is part of their jobs.

Clear identification and assessment of risks will improve corporate governance, corporate and service planning and performance and lead to more effective use of resources and direct improvements to the service to our customers.

The Council is increasingly involved in dealing with uncertainty and managing major change. We are under increasing pressure to deliver better services, increasingly in partnership with others, in new and innovative ways and within reducing budgets. All of this attracts risk which needs to be managed and controlled effectively if we are to achieve the desired outcomes.

The Council like all public bodies, as well as considering short and medium risks, will also have to understand and address the longer-term risks and challenges facing the Council and the community. We need to prevent risks from occurring and to mitigate their impact should they occur. We may need to work with others to prevent risks from occurring or to control and manage them. We need to be mindful that dealing with risks does not create risks and issues for other public bodies. Involving clients, customers and citizens in helping to prevent and to control and manage risks will help too.

Risk management is the process of identifying significant risks, evaluating the potential consequences and implementing the most effective way of responding to, controlling and monitoring them.

By being more risk aware, the Council will be better placed to avoid threats and take advantage of opportunities when they arise.

Risk Management is everyone's business but it will be championed and strongly led by the Corporate Management Team, Cabinet and Leadership Team of the Council

Signed

Phil Roberts
Chief Executive

2. Definition of 'Risk'

Risk is the threat that an event or action will adversely affect an organisation's ability to achieve its objectives and to successfully execute its strategies (CIPFA).

3. Risk Management

Risk Management is the process by which risks are identified, evaluated and controlled and is a key element of the framework of corporate governance (CIPFA).

4. Corporate Commitment to Risk Management

The Council views the management of risk as an essential part of strong corporate governance. The approach is one of managing risk proactively and positively. Effective risk management helps improve services and outcomes, enhances accountability and ensures compliance with formal policies and procedures. Proactive and effective risk management is everyone's business.

5. Aims of the Risk Management Framework

Through this framework, the Council aims to:

- ensure an effective risk management system is in place;
- Improve the ability of the Council to achieve its priorities and objectives.
- help employees, senior managers and elected Members to apply risk management principles consistently across their area of responsibility;
- ensure that the risk management system identifies and assesses risks, decides on appropriate responses and then provides assurance that the chosen responses are effective;
- ensure that risk management is embedded into the culture of the Council, with employees, Members and managers at all levels recognising that risk management is part of their jobs;
- place greater emphasis on prevention rather than detection and correction;
- improve the identification, evaluation and control of strategic and long-term risks, operational risks and community risks;
- protect and enhance the assets and image of the Council;
- embed the Sustainability Principle (Well-being of Future Generations Act) and improve the Council's governance and decision making processes and outcomes.

6. Risk Levels

There are different levels within the risk register: Corporate, Directorate, Service, Information and Project / Programme Risks.

Risks Levels

Corporate Risks are those that could have a detrimental impact on the whole Council or community or could prevent the Council from achieving its priorities and objectives. Corporate Risks are recorded in the Corporate Risk Register.

A **Directorate Risk** is a risk that:

- Could have a detrimental impact on a single directorate and interfere with it achieving its priorities and objectives.
- Needs cross-service mitigation and control within the directorate.
- Is beyond the capacity of a single service to control and mitigate.

Directorate Risks are recorded in the Directorate Risk Register.

A **Service Risk** is a risk that:

- Does not have a detrimental impact beyond a single Service Unit and interfere with it achieving its priorities and objectives.
- Can be mitigated and controlled within the Service Unit.

Service Risks are recorded in the Service Risk Register.

An **Information Risk** is a risk that:

- Involves the fraudulent, unauthorised or negligent access, use, misuse or misplacing of information, records and data held by the Council that is confidential, commercial or otherwise sensitive.

Information Risks are recorded in the Information Risk Register

A **Project and Programme Risk** is:

- An uncertain event or condition that, if it occurs, has a positive or negative effect on a project's or programme's objectives.

Project or programme risks are identified and recorded onto a Risk Tracker, which Project or Programme Managers are expected to control and manage.

There may be 'uniform' risks identified, e.g. safeguarding, Health & Safety, financial control, etc. that should appear at all levels of the risk register. Risks may appear in more one level within the risk register but mitigation and controls would be relevant and specific to each level of risk.

7. Roles and Responsibilities

To implement this framework, specific roles and responsibilities for key stakeholders have been identified as outlined below:

Roles & Responsibilities

Leader and Cabinet

- Set the Council's Risk Management Policy and agree the Risk Management Framework.
- Have ownership of Corporate Risks where Cabinet can help control the risk.
- Assess / challenge the current and long-term risks associated with Cabinet reports.

Chief Executive and Corporate Management Team:

- Ensure that an effective Risk Management Policy, Framework and arrangements are in place within the Council.
- Have ownership of Corporate Risks where CMT can help control the risk.
- Review and monitor 'RED' risks at the different risk levels.
- Consider the current and long-term risks associated with decisions.

Cabinet and CMT

- Have joint-ownership of the Risk Management Policy and Framework and champion risk management throughout the Council.
- Identify and evaluate current and longer-term Corporate Risks during corporate planning and as they emerge.
- Review, monitor and ensure control of Corporate Risks.
- Have joint-ownership of Corporate Risks where CMT and Cabinet can help control the risk.

Cabinet Members:

- Have joint-ownership / ownership for Corporate, Directorate and Service Risks where they can help control the risk.

Elected Members:

- Gain an understanding of risk management and its benefits;
- Be aware of how risks are being managed through the Risk Management Policy and Framework; and
- Maintain an awareness of the risk management implications of policy decisions.

Directors:

- Champion and make arrangements for embedding risk management throughout their Directorate.
- Identify and evaluate current and longer-term Directorate Risks during directorate planning and as they emerge.
- Review, monitor and ensure control of Directorate Risks.
- Ensure Directorate level risks are escalated when necessary.

Heads of Service:

- Champion and make arrangements for embedding risk management throughout their Service Unit.
- Identify and evaluate current and longer-term Service Risks during service planning and as they emerge.
- Review, monitor and ensure control of Service Risks.
- Ensure Service level risks are escalated when necessary.

Council Officers and Managers:

- Identify opportunities and manage risks effectively in their jobs, reporting any risk management concerns, incidents and 'near misses' to their line managers.
- Identify, evaluate and control operational risks and ensuring they are documented on relevant risk registers/trackers/reporting templates.
- Escalate risks when necessary.

Internal Audit:

- Provide an independent and objective opinion to the Council on the control environment (which comprises of risk management, control and governance) by evaluating its effectiveness in achieving the Council's objectives.

The Audit Committee:

- Challenge and provide independent assurance to the Members of the adequacy of the risk management framework.
- Challenge and monitor the effective development and operation of risk management in the Council.
- Monitor progress in addressing risk related issues reported to the Committee.

The **Responsible Officer** is responsible for the management, monitoring and control of an identified risk. The responsible officer should be the person who is able to do something to control the risk. The responsible officer will escalate risks for control and mitigation when necessary.

The **Updater** is responsible for updating the risks recorded in the risk register.

The **Administrators** are responsible for oversight of the risk management framework, quality assurance, maintaining policies and procedures and system administration and maintenance.

The **Corporate Director (Resources)** has the authority to escalate risk concerns or issues from PFM to Corporate Management Team on behalf of Corporate Finance, HR and Performance

representatives.

The **Senior Information Risk Owner (SIRO)**:

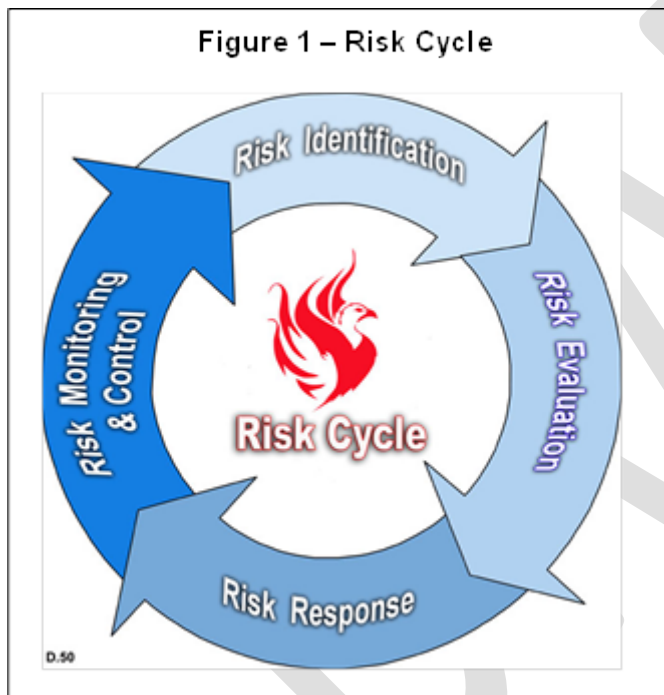
- Ensuring that information risks are treated as a priority for all business outcomes.
- Providing board-level accountability and greater assurance that information risks are being addressed.

Project and Programme Managers are responsible for controlling, reporting and escalating programme / project risks above their agreed tolerance levels to senior management.

Risk awareness raising and training sessions will be provided for the workforce and for elected Members on identifying and reporting risks, including what to do if they identify a risk.

8. Risk Management Cycle

The Council implements a 'Four Step' Risk Management Cycle across the Council to provide a consistent approach to managing risk.



Step 1 – Risk Identification

Step 2 – Risk Evaluation

Step 3 – Risk Response

Step 4 – Risk Monitoring & Control

8.1 Step 1 - Risk identification

Risk identification is about considering the hazards that could happen and, if they did, would have an adverse or other impact.

Risks are formally identified and reviewed during annual corporate and service planning as part of the consideration of the threats to achieving our priorities and objectives. This is illustrated in fig 2 on the next page.

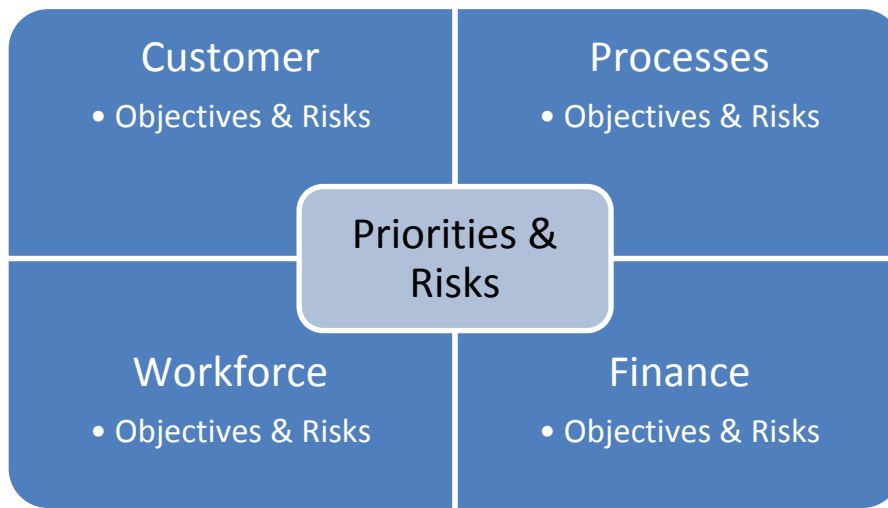


Fig 2 – Identifying risks to achieving our priorities and objectives during corporate and service planning.

The SWOT (Strengths, Weaknesses, Opportunities and Threats) tool and the PESTLE tool are useful to help scan the **current** and **future (long-term) organisational** and **external environment** in order to help **identify potential risks**:

- **P**olitical forces
- **E**conomic factors (including financial)
- **S**ocial factors (including demographic / well-being)
- **T**echnological factors (including systems, information and data)
- **L**egal factors (including legislative)
- **E**nvironmental factors

Note that any **Health & Safety threats or hazards** should be reviewed and identified during corporate and service planning as part of the risk identification process. More information on Health & Safety Risk Assessments can be found at <http://www.swansea.gov.uk/staffnet/riskassessments>

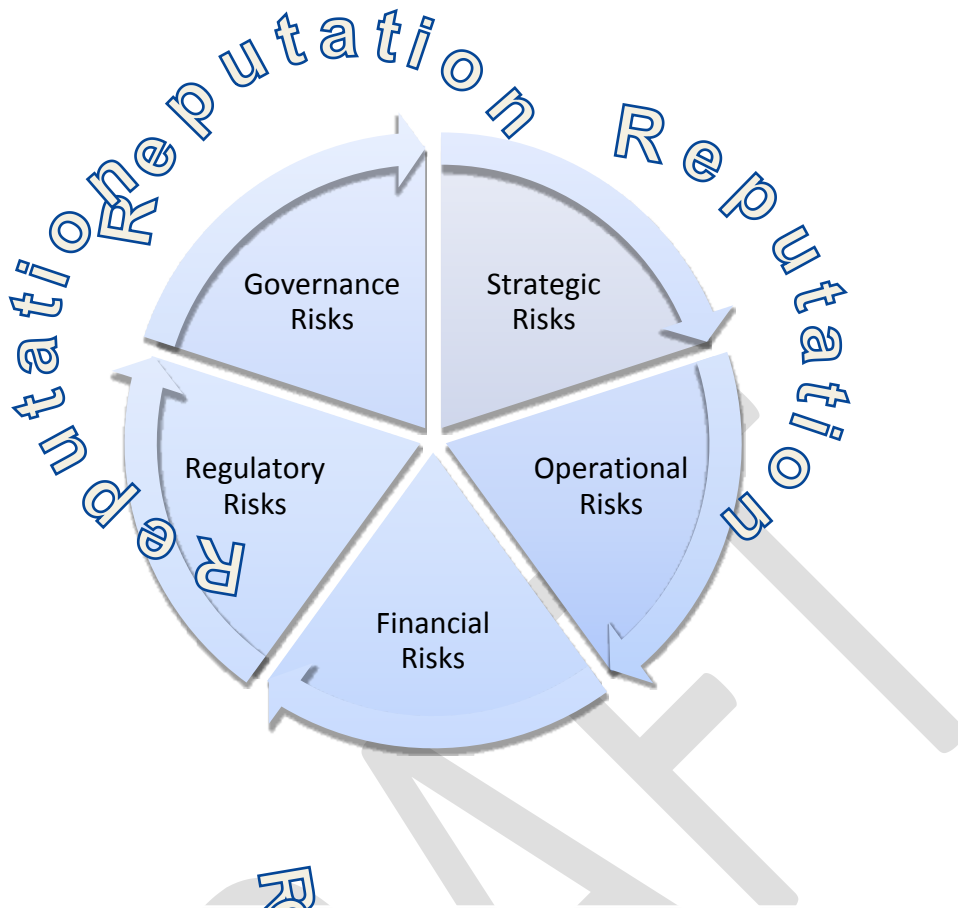
Risks are described using the “**If and then**” statement. The “**If**” being the risk and the “**then**” being the impact if it’s not dealt with.

The risk description must be clear and precise and appropriate to the public domain. Here is an example of wording a risk:

“If the Council does not meet WAG targets to achieve diversions from landfill **then** the Council will be subject to penalties and payments”

Note that new and emerging risks will also need to be identified, recorded, evaluated and controlled as they become known.

8.1.1 Risk Categorisation



Risk Categories

Strategic Risks are long-term or external threats or events that adversely affect the Council's ability to achieve its priorities and objectives.

Operational Risks are threats or events that arise from the services the Council delivers or the activities that it carries out.

Financial Risks are threats or events that may have an adverse impact on or result from the Council's financial budgeting, planning, control and resilience.

Regulatory Risks are threats or events resulting from the legislative framework within which the Council operates.

Governance Risks are threats or events that result from the leadership, management, decision making and control of the Council.

All risks have the potential to damage the reputation of the Council.

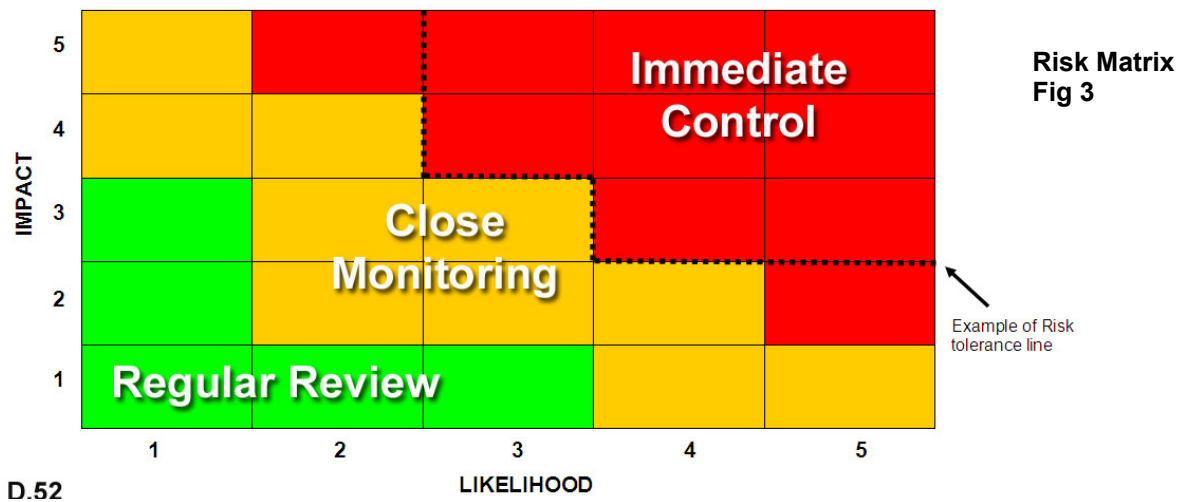
Risk categorisation helps clarify the nature of risks, although in reality risks may be put into more than one category; attempts should be made to identify the main category that any risk should fall into.

The different categories of risk should help identify whether a particular risk is a corporate, directorate or service level risk. For example, a care provider going out of business may be an operational risk but it may also lead to a reputational risk to the whole Council. For this reason, because there is a potential impact on the whole Council, it may be deemed that the risk is a Corporate level risk instead of a Service level risk.




8.2 Step 2 - Risk Evaluation

There are two factors that determine how important a risk is. These are:

- The chances of it happening (**likelihood**);
 - The cost or consequences if it does (**impact**).
- **Risk Matrix**
 - When evaluating the likelihood and impact of risks, the risk matrix (as shown in figure 3 below) can be used to help plot the risks. This is a simple mechanism to increase visibility of risks and assist management decision making.



Within the Council, a RAG (Red, Amber, and Green) status will be used to evaluate these factors and it's important to recognise that each RAG colour represents a particular meaning as follows:

-  **Red – Immediate Control** - There are significant problems which will have a significant impact on the Council if it is not managed;
-  **Amber – Close Monitoring** - will affect the Council if it is not properly monitored and controlled;
-  **Green – Regular Review** - Going to plan but needs to be monitored on a regular basis.

- **Assessing Likelihood and Impact**
 - Once the risks have been identified the **likelihood** of risk occurring and the **impact** they will have if they occur must be assessed. It is important to note that the likelihood and impact of the risks identified need to be considered and ranked using the risk matrix according to the worst case scenario that could happen with the existing controls in place.
- **Risk Proximity**
 - When considering a risk's likelihood, another aspect is when the risk might occur. Some risk will be predicted to be further away than others and so attention should be focused on the more immediate ones first. This prediction is called the risk's **proximity**. Under the Sustainable Development Principle, the Council should look to identify **longer-term risks** – See Section 8.3 Risk Response.
- **Control Measures/Countermeasures**

- When evaluating risk, there is a need to identify existing control measures that are currently in place to manage the risks and any new countermeasures that need to be put in place to manage the risk. See Section 8.3 Risk Response.
- **Risk Tolerance**
 - When identifying risk tolerance, a **risk tolerance line** could be plotted on the matrix to show that any risks above this line needs to be referred upwards for decisions. An example is plotted on fig 3 above. See Section 9 Risk Escalation.

8.3 Step 3 Risk Response

Once risks have been identified and adequate control measure assessed, decide how to respond to specific risks by taking action to improve the outcome. Possible responses to risk should include the four T's as follows:

- **Treat** - Treating the risk – take action to control it in some way by applying containment or contingent actions. Within this categorisation:
 - **Containment** actions are those which lessen the likelihood of the risk or the consequences, and are applied **before** the risk materialises.
 - **Contingent** actions are those which are put into place **after** the outcome from the risk has happened. Here the focus is on reducing the impact of the risk. These actions can be pre-planned so that people know what to do in advance.
- **Transfer** - Transferring some aspects of risk is a recognised method either by getting a third party to take it on or, if available, an insurance policy.
- **Tolerate** - Perhaps nothing can be done at a reasonable cost to mitigate the risk, although the risk should be monitored to ensure it remains acceptable.
- **Terminate** - By doing things differently and thus removing the risk, where it is either feasible or practical to do so.

When considering how to respond to risks, the Sustainable Development principle should be applied as outlined below:

- **Long-term**...looking at longer-term and emerging risks and looking to see how they may be prevented or their impact reduced, e.g. climate change.
- **Prevention**...looking to see how risks may be prevented from happening or their impact reduced should they occur.
- **Integration**...reviewing how risks, controls or responses may have a detrimental impact on the goals and objectives of other public bodies.
- **Collaboration**...reviewing working in partnership with others to help prevent, control or remove risks.
- **Involvement**...considering how involving stakeholders may help prevent, control or remove risks.

8.4 Step 4 Risk Monitoring and Control

Risks must be **monitored** and **controlled**. Risks should be **monitored on a monthly basis** and more frequently if necessary.

Corporate Risks will also be reported and reviewed in-depth **each quarter** in line with corporate performance monitoring. In addition, RED Risks at the different levels, including

Directorate and Service Risks, should also have visibility and be reviewed **each month** at CMT.

Risks are monitored and controlled at the appropriate forum as follows. Risk must be a standard item on the agenda for each of these meetings.

Risks	Forum
Corporate Risks	Corporate Management Team
Directorate Risks	Performance & Financial Monitoring (PFM) meetings
Service Risks	Directorate Management Team (DMT) / Senior Management Team (SMT) & PFMs.
Information Risks	Information Governance Board
Programme / Project Risks	Programme / Project Board

Risk Control Checklist

The following checks can be useful to help monitor and control the risk:

- ✓ Is the proximity of the risk still correct?
- ✓ Is the likelihood and impact of the risk occurring still correct?
- ✓ Are the controls in place accurate and up-to-date?
- ✓ Are the planned responses (actions) in place the right ones?
- ✓ Have the planned responses (actions) to the risk been implemented?
- ✓ Are the controls and / or planned responses (actions) having the desired effect in controlling and / or mitigating the risk?
- ✓ Do additional risk responses (actions) need to be put in place to help control or mitigate the risk?
- ✓ Does the risk need to be escalated?

9. Risk Escalation

Risks would be escalated from Service level to Directorate level to Corporate level when:

- A decision is required or actions need to be taken to mitigate risk that are beyond the authority or capacity of the Service or Directorate;
- When a broader view is required or the collective knowledge of the Service or Directorate is not enough to mitigate the risk.
- When the impact of a risk coming into effect is broader and goes beyond a single Service or Directorate.
- When the 'tolerance line' plotted onto the risk matrix has been crossed.
- 'Information only escalation', i.e. when it is important that a higher body is aware of issues or risks that they may be required to take action on in the future.

Note – these guidelines must be exercised with some discretion and judgment from Heads of Service and Directors. There may be political, reputational issues etc. that although may not be of the greatest corporate importance might still need to be escalated anyway. There may be occasions when risks are escalated from service level straight to corporate level at Corporate Management Team. See Point 7 Roles and Responsibilities.

Performance Improvement and Risk Management Framework

