MEDWAY COUNCIL
RISK STRATEGY 2026/27

Contents

Introduction

Phil Watts
Chief Operating Officer

Risk management is an integral part of good governance.

The council recognises that it has a responsibility to identify and manage risk to achieve its strategic objectives and to identify opportunities to improve the services it provides to the community.

Managing risk is the responsibility of everyone; it is at the heart of the council's culture and values and is reflected in the behaviours of elected members and officers. The council's risk culture balances an acceptance that risks need to be taken to achieve our plans. The council is fully committed to developing a culture where risk is appropriately, effectively, and proportionately managed. This culture flows throughout the whole organisation from elected members to officers who understand and comply with the council's Risk Strategy and processes and are aware of their own roles and responsibilities.

As a risk aware organisation, we are not risk averse. We recognise that risk is unavoidable. We also recognise that there are risks outside our control. However, successfully managing risk, by having appropriate controls/mitigations in place to reduce the likelihood and impact of unexpected events, will enable the council to meet its aspirations for Medway.

The Principles of Risk Management

The following principles shall be applied:

1. Risk management shall be an essential part of governance and leadership, and fundamental to how the council is directed, managed, and controlled at all levels.

2. Risk management shall be an integral part of all organisational activities to support informed decision making in achieving objectives.

3. Risk management shall be collaborative and informed by the best available information and expertise.

4. Risk management processes shall include:

    a. risk identification and assessment to determine and prioritise how the risks should be managed,
    b. the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level,
    c. the design and operation of integrated, insightful, and informative risk monitoring; and
    d. timely, accurate and useful risk reporting to enhance the quality of decision making and to support management and oversight bodies in meeting their responsibilities.

5. Risk management is imperative and our approach to managing risk shall be continually improved through learning and experience.

6. Risk management supports a culture of well-measured risk-taking throughout the council's business, including strategic, programme, partnership, project, and operational risks. This includes setting risk ownership and accountabilities and responding to risks in a balanced way, considering the level of risk, reward, impact, and cost of controls/mitigations.

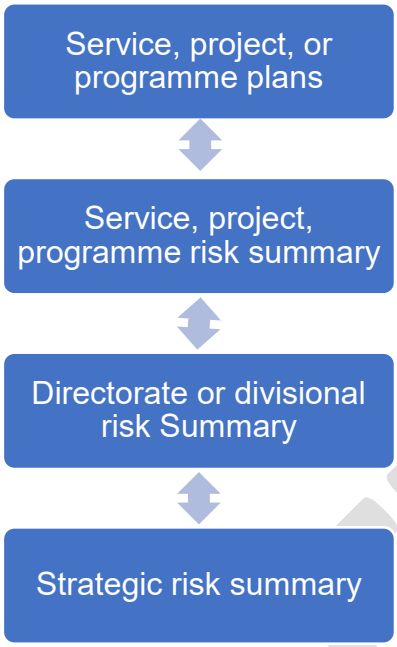
7. Even with good risk management and our best endeavours, things can go wrong. Where this happens, we will use the lessons learnt to try to prevent it from happening again.

Embedding Risk Management

For risk management to be effective, it needs to be an integral part of key business and management processes. Risk management shall be included in the following processes:

- Corporate Decision Making – risks, which are associated with policy or action to be taken when making key decisions, are included in appropriate committee reports.
- Service and Budget Planning – this process includes updating the individual service risk summaries to reflect aims and outcomes.
- Corporate Risk Management Group - supports a culture of objective risk management throughout the Council's business by providing oversight of all risk registers along with the coordination and assurance of risk management activities.
- Project/Programme Management – all projects should consider the risks to delivering the project/programme outcomes before and throughout the project. This includes risks that could have an effect on service delivery, benefits realisation and engagement with key stakeholders.
- Partnership Working – partnerships should establish procedures to record and monitor risks and opportunities that may impact the council and/or the partnership's aims and objectives.
- Procurement and Contract Management – all risks associated with all stages of procurement and contract should be identified and kept under review.

The Risk Management Framework



The risk management framework supports the consistent and robust identification and management of opportunities and risks across the council, supporting openness, challenge, innovation, and excellence in the achievement of objectives.

The risk management framework assists the council in integrating risk management into all levels of the council and ensures that risk is managed in every part of the council.

Risk summaries will be in operation at service, project, or programme level, at directorate or divisional level, and strategic level. Risks can be escalated up and managed down. Directors are responsible for identifying risks that should be escalated up to the strategic risk summary. The strategic risk summary will be reported to Corporate Management Team, Cabinet and Overview and Scrutiny Committees.

Risk will be captured in a single, consolidated platform. This removes version control issues, allows for centralised risk management, update, and score changes, and reduces administrative overhead by removing the need for multiple document exchanges. To enable the council to better understand its overall risk profile.

Risk types

Strategic risks are those risks which may stop the council achieving its objectives. The impact may affect all, or a large part, of the council. These risks cannot be managed solely at service level because higher level support is needed. These are managed by Corporate Management Team.

Operational risks are risks which may affect the day-to-day running of a service, division, or directorate. The impact may affect the service, division, or directorate only. The impact of these risks may be critical in the context of the service level but lower in the context of the strategic risk level. These are managed within the service, division, or directorate.

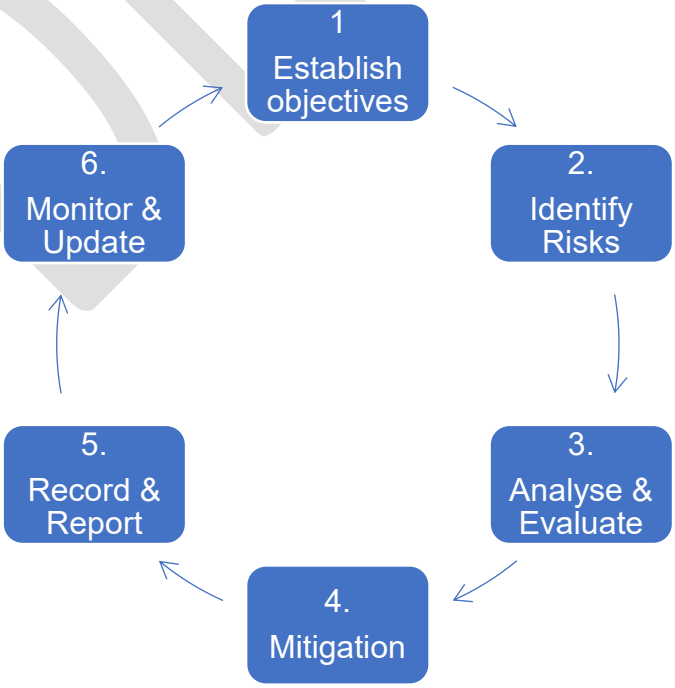
Project or programme risks are those which may impact the successful outcome of a project or programme. These are managed within the project or programme by the leads or sponsors but may be escalated depending on their size and purpose.

Reporting Framework

The reporting framework for risks is outlined in the following table:

Report or Review	Review Body	Purpose
Annual risk strategy review and report	Corporate Management Team, Audit Committee, Business Support and Digital Overview and Scrutiny Committee, Cabinet	Assurance of the effectiveness of the council's risk management process
Quarterly strategic risk review and report	Corporate Management Team, Cabinet, All Overview and Scrutiny Committees	Updates on most significant risks and assurance on how they are being managed
Quarterly strategic review of risk registers	Corporate Risk Management Group	Formal review of risk registers to discuss and agree escalation and de-escalation of risks to and from the Strategic Risk register
Quarterly directorate or divisional risk review	Directorate or Divisional Management Teams	Updates on risks that may impact on the objectives of the directorate or division
Quarterly service, project, or programme review	Service Managers, Project Managers, Programme Managers	Updates on risks that may impact on the objectives of the service, project or programme

The Risk Management Process



Risk management is an iterative process which aims to help the council understand, evaluate, and act on all risks. It supports effective decision making, identification of priorities and objectives and increases the probability of success by making the most of opportunities and reducing the likelihood of failure.

Risk management helps us deliver performance improvement and is at the core of our governance. It helps us manage business planning, change management, innovation, budget setting, project and programme management, equality and access, and contract management.

Risk management is applied at all levels of management and service delivery. This enables the effective use of resources and helps secure the assets of the organisation and continued financial and organisational well-being.

Stage 1: Establish Objectives

Before we can identify risks, we need to establish what we are trying to achieve and what our proposed outcomes are. Once objectives have been established, the risks that may impact successful completion of the objective can be identified.

Stage 2: Identify Risks

The purpose of risk identification is to find, recognise and describe risks that might prevent the council achieving its objectives.

The aim is to generate a comprehensive, up-to-date, easy to understand summary of risks that are relevant to the council, directorate, division and service plan or project and programme delivery.

To identify risks, managers should:

- Undertake a risk assessment exercise.
- Horizon scan: Research and consider the risks or adverse incidents that have affected others including keeping up to date with new local, national, and international policies, legislation, and events.
- Measure current performance and identify weaknesses.
- Recognise the risks that can be managed by the council and those that cannot.

Risks may fall under the following categories:

Political	Outcomes	Projects/Programmes
Economic	Reputation	Customers
Regulatory	Management	Environment
Financial	Assets	

When a new risk is identified it will be allocated a unique reference code which will remain with the risk throughout its lifespan including the escalation and de-escalation between different risk summaries. Each directorate and division should maintain a list of existing and expired risks from which to determine new risk codes.

Stage 3: Analyse and Evaluate

The purpose of risk analysis and evaluation is to understand the nature of the risk, including the level of risk and to prioritise treatment. Risks are assessed as ‘reasonable-worst-case scenarios’ representing the worst plausible manifestation of that risk to undertake proportionate planning.

Risk evaluation may lead to the decision to:

- **Do nothing**: It may not be cost effective to manage all risks. In these circumstances the council will tolerate the risk or reconsider the original objective.
- **Avoid:** Where the risk outweighs the benefit, avoid the risk by doing things differently.
- **Accept:** Accept the risk without implementing further controls/mitigations. The risk owner makes an informed decision to accept that existing actions sufficiently reduce the likelihood and impact and there is no added value in doing more.
- **Transfer:** Transfer all or part of the risk to a third party or through insurance. Although responsibility can be transferred, in most cases accountability remains with the council, so this still needs to be monitored.
- **Reduce:** Implement controls/mitigations to reduce the impact or likelihood of the risk occurring. Further actions are recorded in the risk summary and regularly monitored, and the current risk score re-assessed.
- **Exploit:** Whilst taking action to mitigate risks, a decision is made to exploit a resulting opportunity.

During this process risks will be rated to determine the:

- **Inherent risk score**: This is assigned at the commencement of the risk before controls/mitigations have been put in place. It is a useful indication of the total exposure that the council may have to a particular risk if no controls/mitigations are applied, or if controls/mitigations are ineffective.
- **Current risk score**: This is the current risk level that remains after some controls/mitigations have been considered.
- **Target risk score**: This is the level of risk the council is willing to accept once all controls and mitigations have been considered.

Risks are rated through a combined assessment of:

<u>Likelihood: how likely the risk is to occur</u>

Risk should be assessed using a consistent assessment horizon, that defines the period over which the likelihood and impact of a risk are evaluated. Doing so ensures consistency in scoring and comparability across risks.

Unless otherwise stated, the standard horizon risks should be assessed on is based on their probability of occurring within the next 12 months. This aligns with the council's annual planning and reporting cycle.

In some cases, varying horizons can be applied:

- Long-term risks: an extended horizon of up to 3 years may be applied for example for infrastructure delivery, climate change, etc.
- Project and programme risks: The horizon should reflect the full duration of the project or programme, including major milestones.

<u>Impact: the potential impact before and after mitigation</u>

It is important to note that impact ratings can vary depending on the perspective applied. For example:

A service manager may view a potential income loss of £200,000 as major or critical because it

significantly affects their service budget. However, when assessed at a corporate level, the same loss may be considered minor, as it represents a small proportion of the council's overall income.

This variation does not change the horizon but highlights the need to apply the appropriate lens when scoring impact:

- Strategic lens: Impact relative to the council's overall financial and strategic position.
- Operational level lens: Impact relative to the service, division or directorate's objectives and resources.
- Project or programme lens: Impact is assessed relative to the project's objectives, budget, and timeline.

When assessing the impact, it is always important to confirm which lens is being applied before scoring impact. For reporting purposes, risks escalated to the corporate register should reflect the strategic perspective.

Risk Matrix

The risk matrix is the visual tool to illustrate and compare risks.

	Minor impact 4	**Moderate impact 3**	**Major impact 2**	**Critical impact 1**
Likelihood - Very Likely A	**A4**	**A3**	**A2**	**A1**
Likelihood -Likely B	**B4**	**B3**	**B2**	**B1**
Likelihood - Unlikely C	**C4**	**C3**	**C2**	**C1**
Likelihood -Rare D	**D4**	**D3**	**D2**	**D1**

Key

Risks that fall into the grey shaded squares should be considered for the Strategic Risk Summary as outlined in stage 6 on page 10.

Risk Ratings

The following criteria is to be used as a guideline to aid evaluation.

Likelihood

Likelihood of the risk occurring during the risk assessment horizon:

Very Likely **A**	Almost certain. Expected to occur in most circumstances. History of very frequent occurrence at the council or similar organisations. More than 75% chance of circumstances arising.
Likely **B**	Strong possibility. History of frequent occurrence at the council or similar organisations. 41% to 75% chance of circumstances arising.
Unlikely **C**	Not expected. Moderate possibility it may occur. 10% to 40% chance of circumstances arising.
Rare **D**	It could happen but is very unlikely. Less than 10% chance of circumstances arising.

Impact

The Council assesses impact across 6 broad dimensions as all risks in the register have a wide range of impacts:

	Critical impact 1	**Major impact 2**	**Moderate impact 3**	**Minor impact 4**
People / Duty of Care	Death or life threatening	Severe injury, lost time, short term sick absence	Minor injury, no loss of time	Incident, no loss of time
Financial	Financial impact not manageable within existing funds and requiring Council approval for virement or additional funds. More than £1,000,000.	Financial impact not manageable within existing funds and requiring Member approval for virement or additional funds. More than £500,000 or more than 15% of budget	Financial impact manageable within existing Directorate/Divisional budget but requiring Director and Chief Operating Officer approval for virement or additional funds. Between £250,000 and £500,000 or more than 5% and less than 15% of budget	Financial impact manageable within existing service budget but requiring service manager approval for virement or additional funds. Up to £250,000 or more than 2% and less than 5% of budget
Legal	Legal action, Section 114 or government intervention or criminal charges	Major civil litigation and/or national public enquiry	Legal action unlikely / Minor breach of duty resulting in disciplinary action	Legal action unlikely / Localised service level deviation from duties

	almost certain and difficult to defend			
Service/Project Delivery	Loss of service for more than 5 days / Impacts on vulnerable groups / Affects the whole council	Loss of service 2 to 3 days / Impacts on non-vulnerable groups / Affects a single directorate/division	Loss of Service 1 to 2 days / Impacts on non-vulnerable groups / Affects 1 or a few services of the council	Brief disruption, less than 1 day / Impacts on non-vulnerable groups / Affects a project
Reputation	Sustained negative national publicity, resignation or removal of Chief Executive Officer, Director, or elected member	Sustained negative local publicity / High proportion of negative customer complaints	Significant negative local publicity	Minor, short term negative local publicity
Environment	Major impact, long term contamination to local area	Moderate impact, short term contamination to local area	Minor impact, short term contamination to local area	Local incident would be dealt with immediately with minimal impact

Live risks and managed risks

Strategic risks are distinguished as follows:

- **Live (acute) risks** require continued management and further mitigating action because they change rapidly and require frequent attention These risks may change each quarter. Measures put in place to mitigate such risks will be tested regularly to make sure they remain effective.
- **Managed (chronic) risks** are risks where all reasonable mitigation has been applied and embedded into business-as-usual work. Due to their nature or sensitivity, these risks may still require a corporate overview but would not typically change each quarter.

Stage 4: Mitigation

The purpose of mitigation is to manage the risk to minimise the likelihood of the risk occurring, reduce the frequency of it occurring or limit the severity of the event should it occur.
This stage involves:

- Identifying the existing controls/mitigations in place.
- Identifying what further controls/mitigations are required.
- Accepting that it is not possible to eliminate all risk and there may not be reasonable controls/mitigations available.

The Risk Owner, the person who is responsible and accountable for the risk, must be assigned. This should be the person with the knowledge of the risk area and have sufficient seniority to enable them to allocate resources to manage the risk and to ensure that actions required to treat it are completed. For strategic risks this is usually the Assistant Director or equivalent.

Each control/mitigation should be allocated a unique reference code which aligns with the reference code for the risk. Current control/mitigation codes will be assigned by the risk owner.

Stage 5: Record and Report

Risks should be recorded and reported; this occurs through the Strategic, Directorate/Divisional and Service/Project/Programme Risk Summaries.

Risk summaries are live assessments that record the key details of the risks such as:

- title,
- risk owner,
- inherent, current and target risk scores,
- the current controls/mitigations in place to manage the risk,
- a summary of the actions and their progress, and comments providing further information and updates on the management of the risk.

Risk reporting is an iterative process that takes place quarterly. Risk reporting should:

- Provide relevant, concise but sufficient risk information in a timely manner that facilitates decision making and action.
- Ensure that the views of the leadership team, management teams, and committee(s) receiving the risk report are passed to the relevant risk owners.
- Focus on the most significant risks, ensuring adequate responses are put in place.

Stage 6: Monitor and Update

Iteration and controls/mitigations

The council's approach to risk management is iterative with reviews taking place quarterly. Controls/mitigations are put in place to reduce the likelihood of the risk occurring or the impact should the risk manifest.

Escalation and tolerance

The council has agreed the risk tolerance be drawn at B1 (likely and critical). Risks that are B1 or above should be considered for the strategic risk summary and where appropriate added to the strategic risk summary. These are the risks that fall into the grey shaded squares on the risk matrix. Directorate, Divisional, Service, Programme or Project risks will generally be below B1.

All risks may escalate to higher levels of risk summaries when further action to mitigate a risk cannot be taken by the current owner. Service, project, or programme managers should submit their risks to Directorate or Divisional Management Teams for consideration of inclusion in the Directorate or Divisional Risk Summary. Directorate or Divisional Management Teams should submit their risks to Corporate Management Team for consideration of inclusion in the Strategic Risk Summary.

All risks may be de-escalated to lower levels of risk summaries when mitigation has reduced the severity of the impact should the risk occur or the likelihood of it occurring. When Corporate

Management Team feel that a strategic risk is sufficiently controlled to warrant its removal from the Strategic Risk Summary, they will return it to the Directorate or Divisional Management Team who will decide whether it remains on their risk summary or is returned to the service, project, or programme risk summary.

Roles and responsibilities

All Members, officers and partner organisations have a role to play in ensuring that business risk is effectively managed across the council.

The council expects risk management to be part of all roles in the council and applicable objectives built into individual performance objective plans.

Elected Members

Members will:

- Ensure that they understand the council's risk management arrangements and the strategic risks facing the council.
- Take reasonable steps to properly consider all the risk implications during the decision making and policy approval taken by them.
- Understand the risks facing the council and Medway.
- Review strategic risks through the quarterly reports and information contained in the Council Plan, Cabinet reports and Overview and Scrutiny reports.

Portfolio Holders

Portfolio Holders will:

- Review risks and mitigations and escalation with Assistant Directors on a quarterly basis.

Cabinet

Cabinet will:

- Agree the Risk Strategy and review strategic risks through the quarterly reports.
- Ensure the effective operation of the council's approach to risk management.

Audit Committee

Audit Committee will:

- Provide independent assurance on the adequacy of the risk management framework and the associated control environment, including consideration of the Council's approach to risk management.
- Review the Risk Strategy prior to final approval.

Overview and Scrutiny Committees

The Council's Overview and Scrutiny Committees will:

- Scrutinise and review the operation of risk management in the Council, including reviewing strategic risks through the quarterly reports (all Overview and Scrutiny Committees) and reviewing the Risk Strategy prior to final approval (Business Support and Digital Overview and Scrutiny Committee only).

Leader of the Council

The Leader of the Council will:

- Ensure the work of the Cabinet, Audit Committee, Overview and Scrutiny Committees, and Council is conducted in accordance with council policy and procedures for management of risk and with due regard for any statutory provisions set out in legislation.

The Chief Executive

The Chief Executive will:

- Take overall responsibility for the council's risk management performance.
- Ensure the council has effective and efficient risk management arrangements in place.
- Ensure all decision-making is in line with council policy and procedures for management of risk and any statutory provisions set out in legislation.
- Ensure adequate resources are made available for the management of risk.
- Ensure management of risk performance is continually reviewed.
- Ensure the risks facing the council and Medway are understood.

Corporate Management Team

Corporate Management Team will:

- Promote and oversee the implementation of the Risk Strategy.
- Take a lead in identifying and analysing significant corporate and crosscutting risks and opportunities facing the authority in the achievement of its key objectives.
- Determine the council's approach to each risk and set priorities for action ensuring they are effectively managed, reviewed and updated on a quarterly basis.
- Identify, develop, manage, and update the Strategic Risk Summary on a quarterly basis.
- Understand the risks facing the council and Medway.
- Review and challenge the Directorate/Divisional Risk Summaries as appropriate.
- Support and promote a risk management culture throughout the council.
- Provide leadership and support to promote a culture in which risks are managed with confidence at the lowest appropriate level.
- Agree the risk management framework for the council.

Corporate Risk Management Group

- Review and maintain the Risk Registers, ensuring they are comprehensive and up-to-date.
- Evaluate control measures and ensure they are effective.
- Escalate and de-escalate risks from Strategic, Directorate, and Operation risk registers.
- Review risks on the National Risk Register for potential inclusion in Medway's risk registers.
- Identify and discuss emerging risks and themes.
- Review insurance risks and claims history and implement learning from this to reduce the opportunity and/or impact of these events reoccurring.
- Oversee the delivery of risk management training for council Officers and Members as a means of maintaining the council's risk management arrangements.
- Develop assurance mapping across the organisation to identify strengths and weaknesses in the 'three lines of defence' model.

Directorate and Divisional Management Teams

Directorate/Divisional Management Teams will:

- Develop a Directorate or Divisional Risk Summary and review and update it on a quarterly basis.

- Monitor the Directorate or Divisional Risk Summary and ensure that controls/mitigations are allocated to nominated officers and completed.
- Ensure that the risk management process is an explicit part of all major projects, partnerships and change management initiatives within their Directorates or Divisions.
- Ensure that risk management roles and responsibilities and performance management targets are included within appropriate job descriptions.
- Understand the risks facing their Directorate, Division, the council, and Medway.
- Be accountable for escalating and de-escalating risks between the different risk summaries.

Assistant or Deputy Directors

Assistant or Deputy Directors will:

- Take primary responsibility for identifying and managing significant strategic and operational directorate or divisional risks arising from their service activities. These will be recorded, monitored, and reviewed via the Directorate/Divisional Risk Summary on a quarterly basis.
- Ensure that current controls and mitigations are nominated to specific personnel and are completed.
- Ensure that reports for decision making include comprehensive risk management information to allow effective decisions to be made.
- Promote Risk Management and ensure that the Risk Strategy is implemented effectively across their service and that they and their officers undertake training as required.
- Ensure that their teams carry out risk assessments where appropriate as a routine part of service planning and management activities.
- Ensure that all officers are aware of the risk assessments appropriate to their activity.

Strategic Managers, Service Managers, Programme and Project Managers

Strategic Managers, Service Managers, Programme Managers or Project Managers will:

- Manage operational risks in their service areas by identifying risks for their service areas, assessing them for likelihood and impact, then propose actions to treat them, and allocate responsibility for the controls and mitigations treating the risk within the service risk summary.
- Maintain a service, project, or programme risk summary arising from service/project/programme plans. This will be held as local files unless they are escalated to a higher risk summary. A template is provided in Appendix 1 to the risk strategy.
- Clearly define what the risk is, and the steps being taken to reduce the level of risk.
- Agree risks and current controls and mitigations with Assistant Directors and report progress through the service managers' quarterly update.
- Alert their Assistant Director if the impact or likelihood of the risk increases.
- Escalate risks appropriately.

Council Officers

All officers will:

- Comply with the Risk Strategy for their operational activities and processes.
- Comply with current controls and mitigations identified to reduce risk.
- Report potential hazards and risks they cannot manage to line managers.
- Work in a safe manner not putting themselves, others, or the organisation at risk.
- Alert their line manager if the impact or likelihood of a risk changes.

Internal Audit

Internal Audit will:

- Provide assurance, advice, and guidance on the implementation of the Risk Strategy.
- Ensure that internal audits consider the risks identified within the Strategic and Directorate or Divisional Risk Summaries.
- Provide assurance on the robustness of the council's management of risks.
- Undertake deep dives into high level risks.

Security & Information Governance Group (SIGG)

The Security & Information Governance Group (SIGG) (which includes Assistant Directors) will:

- Comply with the Risk Strategy and escalate information related risks to Corporate Management Team and Directorate and Divisional Management teams.
- Comply with current controls and mitigations identified to reduce risk.
- Agree risks and current controls and mitigations with Assistant Directors and report progress through minutes of their quarterly meetings.
- Restrict processing of information or new initiatives which is likely to result in risks to the rights and freedoms of individuals.
- Record and seek approval from the Senior Information Risk Owner (SIRO) prior to acceptance of information related risks.
- Consult the Information Commissioner's Office (ICO) if residual high risk cannot be fully mitigated.