APPENDIX 2(A)

Caerphilly County Borough Council

Information Risk Management Policy

Version:	Version 0.1
Date:	April 2013
Author/s:	Corporate Information Governance Unit (ICT Services – Corporate Services)
Consultee/s:	Information Governance Project Team
Approved by:	
Review frequency:	Every 2 years
Next review date:	

1 Introduction

1.1 Reliable and accurate information management is critical to proper decision making across the Caerphilly County Borough Council. Information can take many forms – from data sets containing personal information through to records of sensitive meetings, policy recommendations, social services and education records, case files, correspondence and historical records.

- Information is the lifeblood of our organisation, it is a critical business asset that the Council needs to protect and get the most value from to benefit the business

- The management of information risks should be incorporated into all day-to-day operations. If effectively used it can be a tool for managing information proactively rather than reactively. It will enable the Council to get the right information to the right people at the right time, and help avoid incidents where data is lost or improperly disclosed.

1.2 This policy sets out the Council's commitment to the management of information risk. In doing so, this policy supports the Council's strategic aims and objectives and should enable staff and third party suppliers throughout the organisation to identify an acceptable level of risk and, when required, use the correct risk escalation process. Disciplinary action will be considered for any officer (including contractors, consultants, and suppliers) that does not follow the mandatory actions set out in this policy, unless prior agreement to do so has been secured from the Council's SIRO.

1.3 Senior Information Risk Owner (SIRO) and Heads of Service/Information Asset Owners (IAO) must ensure that Senior Management Teams review and are aware of this policy and that it is available to all staff and Members.

All Service Areas must have an Information Risk Register in place. The Information Asset Owner must initially review and finalise the template Risk Register, plus review the Register quarterly and submit a quarterly IAO Risk Return.

2. Information Risk Management

2.1 Information is a vital business asset that we need to protect. Information risk management provides this protection by managing risks to the confidentiality, integrity and availability of information to assist our services to function effectively.

- Confidentiality means ensuring that only authorised people can get to our information
- Integrity means ensuring that it is authentic, accurate and complete
- Availability means that authorised people can access it when they need to, at the right times in the right ways

2.2 Keeping the right information for the right period of time is also very important and can help ensure we comply with a range of statutory responsibilities (e.g. Freedom of Information 2000 and Data Protection Act 1998), locate information when it is required to provide effective services and provide supporting

evidence in the event of litigation against the Council. For guidance refer to the Council's Retention and Disposal Guidance.

Senior Information Risk Owner (SIRO)

2.3 The SIRO role is held by the Head of Information, Communications and Technology Services, who is also Council's Corporate Data Protection Officer.

2.4 The SIRO is responsible for:

- Owning the risk policy and assessment process for the Council, ensuring that the organisation takes a responsible attitude to information and can implement data handling standards.
- Developing a management statement on risk appetite, which can vary according to current circumstances.
- Writing an annual Information Risk Return informed by quarterly IAO Risk Returns covering the Council and main delivery partners which ensures that the Council can monitor and assess compliance. The annual return gives a structure to improvement and will include:
  a) Details of any changes to key individuals responsible for security matters.
  b) Significant risks and mitigations that have implications for protective security.
  c) All significant security incidents
  d) Declaration of meeting all data handling standards
  e) Confirmation that any significant control weaknesses have been reflected in the Annual Governance Statement.

Information Asset Owner (IAO)

2.5 IAOs (Heads of Service) are responsible for the day to day use of information, which includes who has access to the information and risk management of their information. IAOs are responsible for making sure their Service Areas and external partners with whom they work have in place the arrangements needed to implement and maintain this policy, supported by Directorate Information Governance Stewards. The IAO may wish to appoint Information Governance Service Area Liaison Officers to work on their behalf, taking day to day oversight of assets and reporting back to the IAO on the changes to risks. The IAO must report quarterly on information risk, and submit quarterly IAO Risk Returns to the SIRO. Further information about the role of the IAO can be found in Annex A of this document.

Information Risk Register

2.7 To provide evidence that the risks in their Service Area have been identified and that there are plans in place for managing them the IAO must compile and maintain an Information Risk Register. The register will enable the IAO to be able to identify and explain the risk that a loss / compromise or lack of availability of that asset would have to the Council. IAOs must review information risks on a quarterly basis to inform the SIRO's annual reports and, where appropriate, the IAO must escalate any risks to the SIRO via the Corporate Information Governance Unit. As well as existing risks that have already been identified, the review must also consider forthcoming potential

changes in services, technology and threats. Guidance on reviewing the Risk Register can be found in Annex B.

2.8 A partially completed risk register template that you can amend to fit your own Service Area can be found in Annex C. The draft has been provided to assist you but you will need to look at the information in each of the columns and consider the extent to which it is valid for your Service Area. *You must include any additional risk descriptions and possible causes with Service Area specific risks and causes where necessary.* The register includes two ratings relating to likelihood of risk being realised and business impact associated with the threat being realised, resulting in a score.

2.9 If a risk is given a collective impact/likelihood score of 9 or above, or an existing risk being managed at Service Area level whose collective score for impact and likelihood is/becomes 9 or above, it must be escalated to the Council SIRO via the Corporate Information Governance Unit immediately. Further guidance on escalating risks to the appropriate level can be found in Annex B

2.10 The quarterly IAO Risk Return is made up of the Information and Assurance Compliance Statement that can be found at the start of the template Information Risk Register. This must be completed and sent electronically to the Corporate Information Governance Unit by the end of Feb, May, Aug, and Nov each year.

3. Business Continuity Planning

3.1 The purpose of business continuity is to create the conditions that ensure a business can continue to operate even after an event that denies it access to its assets and information: this could be a server failure, a power cut, a fire or any other catastrophic event.

3.2 To ensure business continuity is maintained across the Council all Service Areas must have in place a Contingency Plan for the loss of information assets. The IAO is responsible for contingency plans within their Service Area and must ensure that all staff are aware of the contingency plans and have enough knowledge to implement them.

3.3 It is important that IAOs identify their local 'vital records'. These are information assets that have been identified as essential for the continuation of the Council operations if, for example, IT systems and / or paper records cannot be accessed.

3.4 The plan must identify proposals for the recovery of business critical activities promptly and efficiently and include proposals for the protection of ‘vital records’ and the Council’s information assets.

4. Physical and Personnel Security

4.1 Physical Security - Facilities Managers will assess any physical security risks that affect the sites in which ICT-based and paper-based information systems reside. They must ensure that IAOs are made aware of any assessed risks that affect them.

4.2 Personnel security - All staff must have the appropriate level of checking needed to assure the reliability of each employee (including contractors)

according to the sensitivity of the information that the member of staff has regular access to and the business impact that might arise if that employee discloses this information without authority. All staff must also undertake and pass mandatory information risk training.

5. Delivery Partners and Third Party Suppliers

5.1 Council partners and third party suppliers must identify and manage risks to all the Council information assets that they have access to and/or control of, including escalating them via the necessary channels as outlined in this policy.

5.2 Any significant risks relating to Council information must be raised with the partner/third party supplier's usual point of contact within the Council, who will raise this with the relevant IAO, as outlined in this policy.

6. Equalities and Welsh Language Issues

6.1 In general, most information held by the Council is provided in both English and Welsh (as per the guidance in the Editorial Policy) but specifically in terms of Information Risk, it can be provided from, or requested by, the public in any language or format.

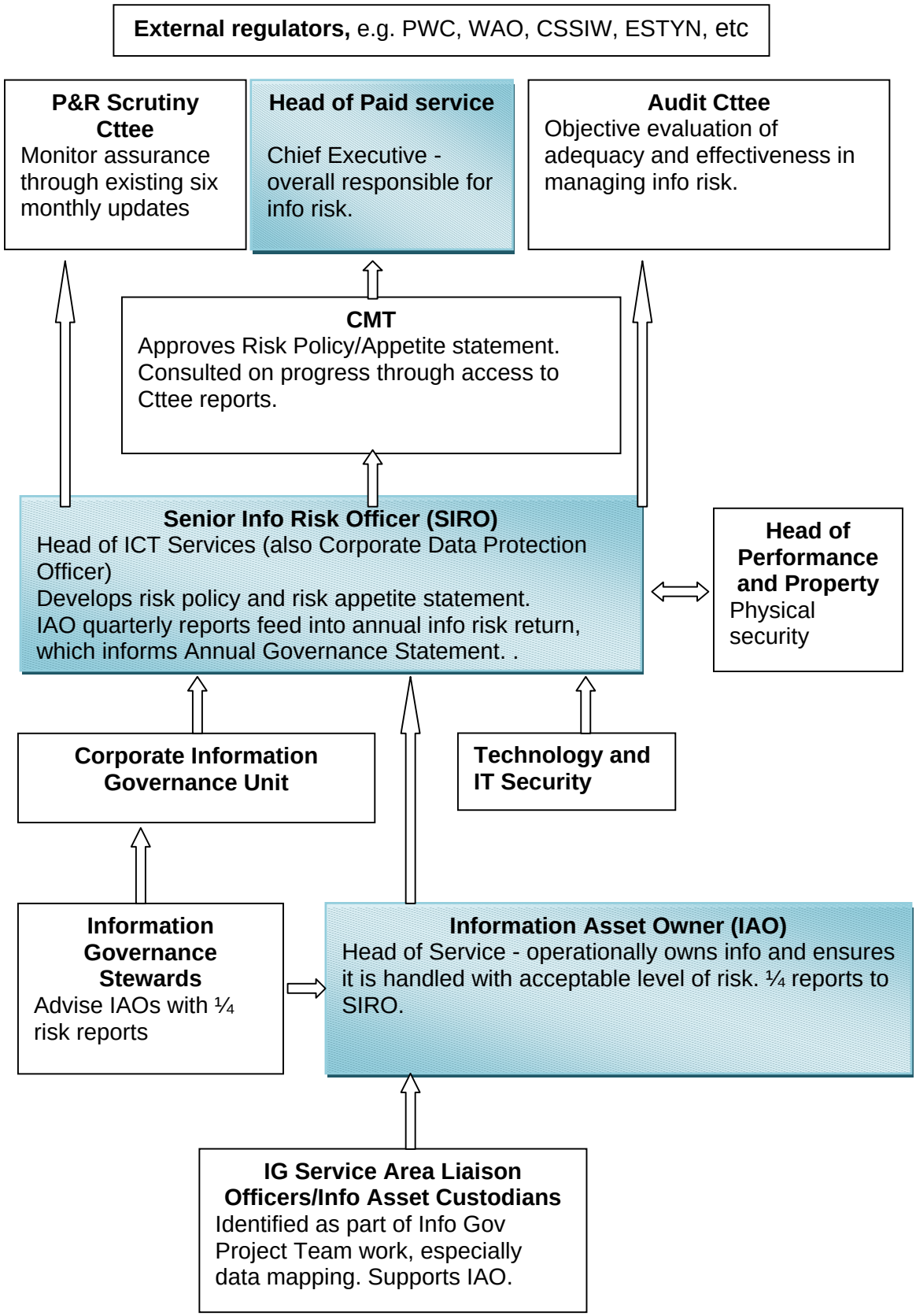
6.2 When dealing with correspondence, information or data of a sensitive nature, the issue of translation or interpreting can thus potentially add a significant risk to the Council if done without proper controls and safeguards in place. The Equalities and Welsh Language team in Legal and Governance provide advice, Welsh translation in house in the strictest of confidence where necessary, and can provide advice and guidance on secure translation and interpreting for British Sign Language, Braille and any other spoken language where necessary.

7. Supporting documents

- Records Management Policy
- Corporate Record Retention and Disposal Policy
- Environment Directorate Retention Schedule
- Social Services Directorate Retention Guidance
- Data Protection Policy
- IT Security Policy
- Policy on Requests for and Access to Unpublished Information
- Publication Scheme
- Wales Accord on Sharing of Personal Information (WASPI)
- Information Sharing Protocols (WASPI and non-WASPI)
- Strategic Equality Plan
- Welsh Language Scheme (specifically the Editorial Policy supplementary guidance document)

Annex A - Roles and Responsibilities

See below for specific details of each role.



Head of Paid Service - Chief Executive who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level, and signs Annual Governance Statement.

Corporate Management Team - approves Information Risk Policy and Corporate Risk Appetite Statement, and monitors progress via reports to Policy and Resources Scrutiny Committee.

Policy and Resources Scrutiny Committee - considers information assurance and overall management of information every six months.

Audit Committee - objectively evaluates the adequacy and effectiveness of the Council's management of information risk as a key component of its wider assurance responsibilities for risk management. Already has a role in monitoring information management via PWC audit follow-ups.

Senior Information Risk Owner (SIRO) - overall responsibility for information assets, understands and manages information risk, and provides assurance that all IAOs in the Council are following their responsibilities. Has a key role in maximising the effectiveness of information usage, both internally and with delivery partners. Corporate Information Governance Unit, IT Security and ICT fall within the SIRO's Service Area. Head of Performance and Property works closely with SIRO to ensure buildings security is appropriate to protect assets, and to coordinate responses to security related matters.

Information Asset Owners (IAOs) – Heads of Service responsible for the day to day use as well as the risk management of their information asset, and help the SIRO to foster a responsible attitude towards the use and protection of information. In particular, IAOs:

- identify and manage information risks associated with the particular Council information assets that they are responsible for.
- understand what information is held, what is added and removed, how it is used, how transferred, and who has access and why
- ensuring that information is fully used within the law for the public good, and
- ensuring that appropriate business continuity plans are in place for their Service Area.
- implementing and regularly reviewing this information risk policy and ensuring their business areas, and the delivery partners and third party suppliers with whom they work, have in place the arrangements needed to implement and maintain an effective information risk management policy.
- providing written input annually to the SIRO on the security and use of their asset.

The IAO may wish to appoint Information Asset Custodians to work on their behalf, taking day to day oversight of assets and reporting back to the IAO on the changes to risks. Directorate Information Governance Stewards will also provide support to the IAO, but the IAO will retain the overall responsibility.

Corporate Information Governance Unit - based in the ICT Services Section of Corporate Services Directorate, the team aims to advise on information management to deliver service benefits and efficiency savings, reduce information risk and facilitate compliance with information legislation.

Directorate Information Governance Stewards – the Stewards, along with their service area networks, support their directorate in all aspects of information governance, including advice and communication, training, information security, records management, data quality, and information systems (IT and hard copy). The Stewards contribute to the work of the Information Governance Project Team.

Annex B

Information Assurance Risk Management Process

1.1 Risk management encompasses the following stages: Risk Identification, Risk Assessment, Risk Monitoring and Escalation.

1.2 A Risk Register that provides enough information to explain risk management decisions will enable the IAO to monitor and manage the risks within their Service Area. A partially completed risk register template that you can amend to fit your Service Area can be found in Annex C.

1.3 In order to complete it you will need to look at the information in each column and consider the extent to which it is true in your location and provide an appropriate risk rating. *You must include any additional risk descriptions with Service Area specific risks, causes and mitigating actions and also include the possible consequences of the risk being compromised where necessary.*

Stage 1 - Risk Identification:

1.4 Situations where risks must be identified may take many forms, for example:

- Preparation to develop a new Information Communication Technology (ICT) based or paper-based information system, or
- Work to address a change of requirement, etc

1.5 The starting point in these examples is risk analysis: being clear on what information assets fall within scope of the assessment and the importance of those assets to the Council (or the impact of loss of confidentiality, integrity or availability).

1.6 If the Service Area has an Information Asset Register in place, this can be used to help to identify the different types of information assets held and to provide direction on the risk to the organisation that a loss / compromise of that asset would have. Please contact your Directorate Information Governance Steward for further information. Some examples of information assets are:

- Staff and HR Details
- Client records and reports
- Financial information
- Caseworking files

1.7 Once you have considered the information assets that might be at risk you need to identify the 'risk description' which is the form that the compromise / loss might take. The following suggestions are some of the factors that you might want to consider as 'risk descriptions' - this list is only for guidance and you might identify different or additional risks that are more appropriate in your own Service Area:

- Inappropriate disclosure of personal material
- Theft, loss or unauthorised access to information (paper records should be considered as well as electronic and systems)
- Ineffective or insecure information sharing
- Records retained for the wrong length of time

- Failure to create or locate reliable records as evidence of business decisions and activities
- Poor management of information risk

1.8 Once you have identified the 'risk description', the next step is to identify the organisations, people or events that pose a threat to your information assets. The following are just a few of the possible causes of information loss / compromise but you need to consider which of these are true in your Service Area and update the Risk Register to reflect this:

- Lack of awareness and training
- Absence of information sharing agreements
- Password sharing
- Documents sent to incorrect address or lost/compromised during transmission
- Dishonesty
- Inappropriate storage
- Records retained unnecessarily result in large volumes of data to be searched.
- Unavailability of business continuity plans

Stage 2 - Assessing the Scale of Risk:

1.9 Assessing a risk involves evaluating two factors, these are:
The Impact to the Council where the compromise/loss to occur, and
The Likelihood of the risk being realised, taking into account the working environment and past experience.

1.10 The assessment of these factors helps you to decide on the overall severity of each risk, this means that they can be prioritised and resources focused on the most serious.

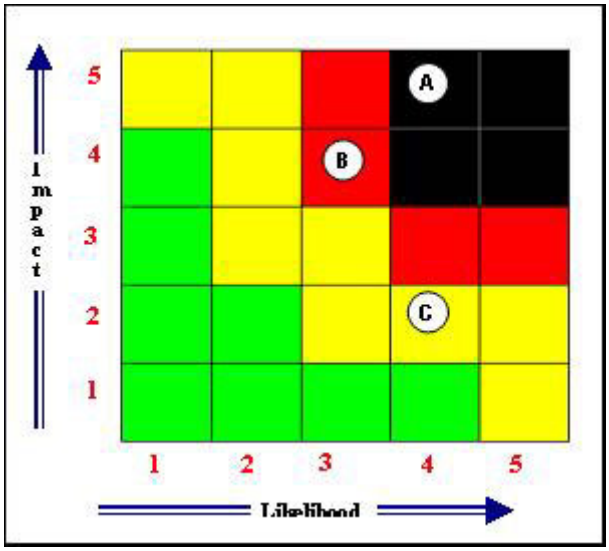
1.11 The table below illustrates what score is attached to each level for both impact and likelihood. Once you have decided on the scores they are multiplied together to give the overall risk score.

1.12 For example:

- A risk is determined to have a 'significant detrimental effect in the long term' would have a score of High (4).
- It is then judged the likelihood of this occurring is unlikely giving a score of Low (2).
- This is multiplied to give a total risk score of 8.
- This score is then used to determine if the risk needs escalating.

Scale	IMPACT	LIKELIHOOD
5 Very High	Prevents achievement of the Council objectives or has highly damaging impact on the Council operational effectiveness or reputation.	> 80 % **Almost Certain**
4 High	Significant detrimental effect on achievement of the Council corporate objectives in the longer term. Media criticism.	51 – 80 % **Probable**
3 Medium	Impacts at Service Area level on elements of efficiency, output and quality which impacts on the outcome of long term the Council corporate objectives. Potential for negative local media coverage	21 – 50 % **Possible**
2 Low	Impact on Service Area short term goals within their objectives without affecting long term achievement of the Council corporate objectives.	6 – 20 % **Unlikely**
1 Very Low	Minor and containable impact on achievement of Service Area objectives.	< 5 % **Very Unlikely**

Risk scores can be shown on a matrix:



Risk **A**: *Very High* Impact (5), and *High* Likelihood (4), giving a score of 20;
Risk **B**: *High* Impact (4), and *Medium* Likelihood (3), giving a score of 12;
Risk **C**: *Low* Impact (2), and *High* Likelihood (4), giving a score of 8.

1.13 The risk scores are used to decide if the level of risk is acceptable, or if further action to mitigate is required, (e.g. controls, escalation and/or contingency plans).

Stage 3 - Managing the risk:

1.14 *There are generally four options that the IAO must consider when deciding how to manage the identified risk.*

1.15 The first one is 'treating the risk' which is done by applying one or more Information Assurance controls to reduce the likelihood of the risk being realised or lessen the impact if the risk is realised. Examples of these controls could be:

- Implementing best practice in the Council's Retention and Disposal Guidance
- Investigation of incidents and lessons learned
- Training and awareness
- Putting in place suitable business contingency plans

1.16 The second option is 'removing the risk', this is done by finding another way to achieve a Service Area objective.

1.17 Another possible option to consider is 'transferring the risk,' for example by outsourcing services. It is important to recognise that even if it is possible to transfer responsibility for managing a risk to an organisation other than the Council, the consequences of a risk will rest wherever the business impact associated with it being realised is felt, and legal responsibility will usually remain with the Council. *The legal basis for sharing information and appropriate contractual arrangements must be in place.*

1.18 Finally the IAO could decide that 'tolerating the risk' is the most appropriate action. This is usually done where:

- the financial cost of mitigation is too great,
- where the likelihood of the risk being realised is low,
- where the impact on the Council if the risk is realised is low or else
- where the business benefit is high.

<u>Stage 4 – Monitor and Escalate:</u>

1.19 An ongoing programme of periodic monitoring, inspection and testing is required which validates and provides evidence that the information assurance controls used to manage risks remain effective.

1.20 An annual Information Assurance Compliance Statement is compiled by the SIRO, giving assurance that Risk Registers are in place.

1.21 In addition to this the IAO must carry out a quarterly review of the information risks. As well as existing risks that have already been identified, the review must also consider forthcoming potential changes in services, technology and threats. Reviews must be discussed at Service Area level and minuted.

1.22 If a risk hits a certain score it must be escalated to a specific management level, following expedited consultation with Divisional/Senior Management Teams. This is set out below;

- **High (I/L20 - 25) Corporate Management Team (CMT) and SIRO**

- **Med (I/L 9 - 19) the Council SIRO through the Corporate Information Governance Unit**
- **Low (I/L 1 - 8) Information Asset Owner**

1.23 How does it work in practice? The description below illustrates the step by step process.

- Step 1 (Risk registration) - *Any new risk which has a collective impact/likelihood score of 9 or above, or an existing risk being managed at Service Area level whose collective score for impact and likelihood is/becomes 9 or above, must be escalated to the Council SIRO via Corporate Information Governance Unit on x4322.*

- Step 2 (Risk acceptance) - The SIRO will review any proposed new risks and make a decision on whether to accept, reject or transfer the risk to a new owner. The SIRO will also agree that the scoring is appropriate, the mitigating actions, target dates and risk owner.

- Step 3 (Escalation to CMT) - Any new/existing risks which are identified as having an impact/likelihood score of 20 or above will be escalated via the SIRO to Corporate Management Team. These risks will require an accompanying action plan (or risk treatment plan) setting out in detail the full risk, the controls in place, the proposed mitigating controls and a detailed timeline to completion. Additionally, IAOs will be required to provide updates on these significant risks.

- Step 4 (Closure) - Risks with a score of 20+ which are tabled for closure will need to go to CMT with an accompanying closure report (which may be an updated action plan, outlining all of the mitigations which are in place, the target score which has been achieved and any residual risk).

1.24 It is worth remembering that when risks are escalated and assessed at the next management level, that the level of impact is likely to be moderated as objectives and responsibilities widen. Therefore, a risk identified at Service Area level may often (although not in all cases) have a lower impact upon the overall Council business objective.

Annex C

Information Risk Return and Risk Register