Appendix 1

Caerphilly County Borough Council

Information Risk Management Policy

Version:	Version ~~1~~2
Date:	Oct 2013 Revised September 2017
Author/s:	Corporate Information Governance Unit (ICT Services – Corporate Services)
Consultee/s:	Information Governance Project Team
Approved by:	Cabinet, 16 Oct 2017
Review frequency:	Every 2 years
Next review date:	~~Oct 2015~~October 2019

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~~service delivery.

- The management of information risks should be incorporated into all day-to-day operations~~. If effectively used it can be a tool for~~ to demonstrate accountability in managing information proactively rather than reactively. ~~It~~

- Proactive information risk reviews 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, and ensure compliance with data protection laws.

1.2 This policy sets out the Council's commitment to the management of information risk~~. In doing so, this~~ and should be read together with information risks identified in the Corporate Risk Register. 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.

1.3 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.~~Senior Information Risk Owner (SIRO).

1.~~3 Senior Information Risk Owner (4 The~~ SIRO~~)~~ and Heads of Service~~/~~ as Information Asset Owners (IAO) for their service must ensure that ~~Senior Management Teams~~senior management teams review and are aware of this policy and that it is available to all staff and Elected Members.

~~All~~In addition, all Service Areas must have an Information Risk Register in place~~.~~ developed from the template in Annex C. The Information Asset Owner must ~~initially review and finalise the template Risk Register, plus~~ review the Register ~~quarterly~~every six months and submit a ~~quarterly~~six monthly IAO Risk Return to the SIRO.

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~~, but risks to the confidentiality, integrity and availability of information ~~to assist our~~must be managed in order for services to function effectively.

- Confidentiality means ensuring that only authorised people can ~~get to our~~access information;
- Integrity means ensuring that ~~it~~information is authentic, accurate and complete;
- Availability means that authorised people can access ~~it~~information when they need to, at the right times and 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~~ensures compliance with a range of statutory responsibilities (e.g. Freedom of Information ~~2000~~ and Data Protection ~~Act 1998), locate~~ laws), enables location of information when ~~it is~~ required to provide effective services, assists decision-making, and ~~provide supporting~~provides evidence ~~in the event of litigation against the Council. For guidance refer to~~of the Council's activities. The Council's Retention and Disposal ~~Guidance~~Policy gives guidance on retention of records.

Senior Information Risk Owner (SIRO)

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

~~2.4~~2.3 ~~The SIRO~~ and is responsible for:

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

Information Asset Owner (IAO)

2.~~5~~4 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~~every six months on information risk, and submit ~~quarterly~~six monthly IAO Risk Returns to the SIRO. Further information about the role of the IAO can be found in Annex A of this document.

Information Asset Register

2.5 High level Information Asset Registers have been developed for each Council function, identifying the records held to support the functions, activities and transactions of the Council. The register also includes details of:

- who can access the record,
- where it is located and in what format,
- whether it is a vital record,
- whether it contains personal or otherwise sensitive data, and if personal, how data protection requirements are satisfied, e.g.:
  i. the legal basis for processing the data, including arrangements for consent where applicable
  ii. whether privacy notices are available, and
  iii. whether there is any automated decision-making or profiling.

2.6 The IAO is responsible for making sure Information Asset Registers are updated on a regular basis, including updating those areas that fall within the main control of a different Head of Service (e.g. HR, finance, etc). Information Asset Registers are stored on a shared network drive to facilitate access and update by officers from any Service Area. The records identified in the Information

Asset Register must be reviewed to identify risks that apply to them, which will be documented by the IAO in the Service Area's Information Risk Register.

Information Risk Register

2.62.7 To provide evidence that ~~the~~ risks in ~~their~~ Service ~~Area have been~~ Areas are identified and ~~that there are plans in place for managing them~~managed 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~~an asset would have to the Council. IAOs must review information risks on a ~~quarterly~~six monthly 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~~.~~, and verify that Privacy Impact Assessments will be undertaken at an early stage. Guidance on reviewing the Risk Register can be found in Annex B.

2.72.8 A partially completed risk register template that ~~you~~ can ~~amend~~be amended to ~~fit your own~~suit each 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*~~*IAO's* *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~~six monthly IAO Information Risk Return is made up of the Information ~~and Assurance Compliance Statement~~Risk Return 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~~end of Aug each year.

3. Privacy Impact Assessments

3.1 A key tool in the Council's armoury for reducing information risk is the Privacy Impact Assessment (PIA) for using personal information. PIAs have been expected by the Information Commissioner for many years, and are an essential component of evidencing 'Privacy by Design' elements of the General Data Protection Regulations, in force in the UK from 25 May 2018. PIAs can be brief, simply listing pros and cons of an activity and concluding whether privacy risk is justified and/or can be mitigated, or they can be more detailed exercises for higher risk schemes. Guidance and a template for a full scale PIA are available on the Information Governance intranet.

4. Business Continuity Planning

~~3~~4.1 The purpose of business continuity planning 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. Service Areas must have in place a plan for the loss of information assets, usually incorporated within their Service Area Business Continuity Plan. The IAO is responsible for Business Continuity Plans within their Service Area and must ensure that all staff are aware of the plans and have enough knowledge to implement them.

~~3~~4.2 ~~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' within their Information Asset Registers and reference these in their business continuity plans. 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~~

~~5~~. Physical and Personnel Security

~~4~~5.1 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~~5.2 Personnel security - All staff, volunteers, and any other party with access to the Council's records 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~~mishandles information ~~without authority.~~. All staff must also undertake and pass mandatory information risk training on an annual basis.

~~5~~6. Delivery Partners and Third Party Suppliers

~~5.1~~6.1 Before entering into a relationship with a third party that involves sharing information, a PIA needs to be undertaken as soon as possible, and appropriate contracts/agreements established to protect each Data Controller.

6.2 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~~6.3 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 and the SIRO if necessary, as outlined in this policy.

~~6~~7. Equalities and Welsh Language ~~Issues~~

~~6~~7.1 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,~~but it can be ~~provided~~supplied from~~,~~ or requested by~~,~~ the public in any language or format.

~~6~~7.2 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~~undertaken without proper controls and safeguards ~~in place~~. The Council's 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.~~..

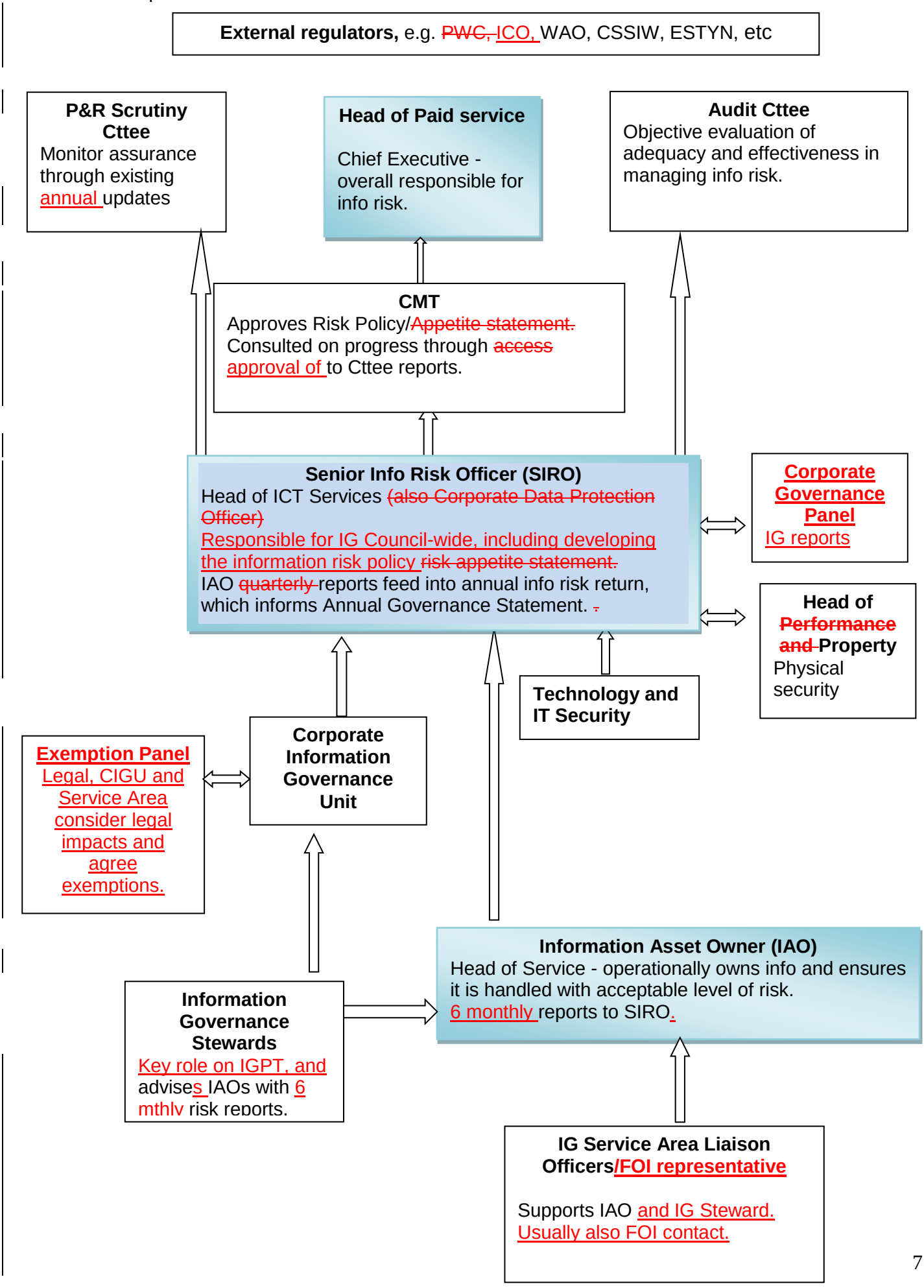
~~7~~8. Supporting documents

- 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 together with the Council Leader.

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~~year.

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~~Has a role in monitoring information management via ~~PWC~~external 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, including Privacy Impact Assessments when necessary.
- ~~understand~~maintain an information asset register to enable understanding of 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~~information assets.

The IAO may wish to appoint Information Asset Custodians/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. 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.

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 overall 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~~1.3 For new initiatives that involve personal data, or for higher risk ongoing initiatives, a Privacy Impact Assessment will supplement the overall Service Area Information Risk Register. The learning acquired by following the procedure described below can be applied to the process of completing a PIA.

1.4 In order to complete the Information Risk Register template 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~~5 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~~6 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~~7 The Service ~~Area has an~~Area's Information Asset Register ~~in place, this can be used to~~will 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~~8 Once you have considered the information assets that might be at risk you need to identify the ~~'risk description' which~~ key risks posed to this information. If personal data is contained in the ~~form~~information asset, a Privacy Impact Assessment is a useful tool to identify risks that cannot be avoided. In the ~~compromise / loss might take. The following suggestions~~template in Annex C, seven key risks are ~~some of the factors that you might want to consider as 'risk descriptions' - this list is only for guidance and~~identified, but 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~~9 Once you have identified the ~~'risk description'~~key risks, the next step is to identify the organisations, people or events that ~~pose~~can cause 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~~10 Assessing a risk involves evaluating two factors, these are:

- The Impact to the Council ~~where~~were the compromise/loss to occur, and
- The Likelihood of the risk being realised, taking into account the working environment ~~and past experience~~.

1.~~10~~11 The assessment of these factors helps you to decide on the overall severity of each risk, ~~this~~which means that they can be prioritised and resources focused on the most serious.

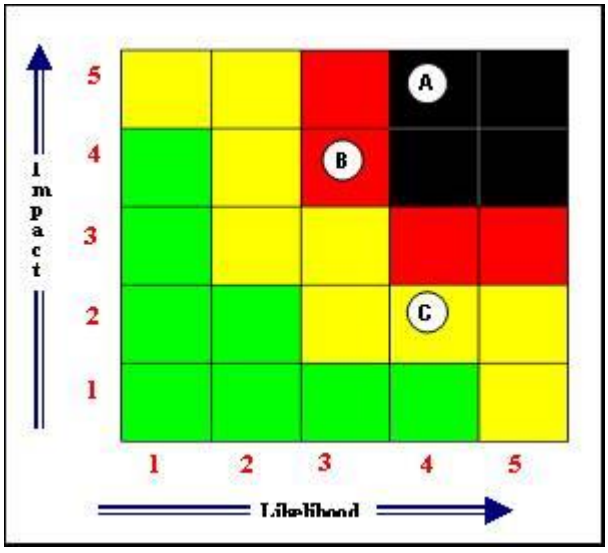
1.~~11~~12 The table below illustrates ~~what score is~~the scores attached to each level for both impact and likelihood. Once you have decided on the scores they are multiplied together to give the overall risk score.

1.~~12~~13 For example:

- A risk ~~is~~ determined to have a 'significant detrimental effect in the long term' would have a score of High (4).
- ~~It~~If it is ~~then~~ judged that the likelihood of this occurring is unlikely ~~giving~~, a score of Low (2~~).~~) could be given.
- This is multiplied to give a total risk score of 8~~.~~
- ~~This score~~, which 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~~are illustrated by this 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~~14 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~~15 *There are generally four options that the IAO must consider when deciding how to manage the identified risk.*

1.~~15~~16 The first one is 'treating the risk' which is done by applying one or more ~~Information Assurance~~information assurance controls, for example training, to reduce the likelihood of the risk

being realised or lessen the impact if the risk is realised. Examples of these controls ~~could be:~~are given in the template in Annex C.

- ~~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~~17 The second option is 'removing the risk', ~~this~~which is done by finding another way to achieve a Service Area objective.

1.~~17~~18 Another possible option to consider is 'transferring the risk,' for example by outsourcing services. ~~It is important to recognise that~~However even if it is possible to transfer responsibility for managing a risk ~~to an organisation other than the Council~~elsewhere, 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*~~*Therefore if services are outsourced, the legal basis for sharing information and appropriate contractual arrangements must be in place.*

~~1.18~~1.19 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.

Stage 4 – Monitor and Escalate:

1.~~19~~20 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~~21 An annual Information Assurance Compliance Statement is compiled by the SIRO, giving assurance that Information Risk Registers are in place.

1.~~21~~ 22 In addition to this the IAO must carry out a ~~quarterly~~six monthly 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~~1.23 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~~24 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~~25 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~~for *[insert either 1 March – 30 Aug or 1 Sept - 31 Feb]* [i1]

IAO name		**Signature**	
Service Area		**Date**	
Directorate			
I have reviewed the information risk register for my service area.		Yes/No	
I can confirm that the risks are:		The same as the last period/have changed since the last period. (If changed, please modify Info Risk Register, and submit to SIRO.)	
I can confirm that the impact/level of the risks are:		The same as the last period/have changed since the last period	
If the impact/level of the risks have changed, please describe.			
I can confirm that the active controls are:		The same/have changed	
If the active controls have changed, please describe.			
I can confirm that the proposed controls:		Have/have not been implemented	
If the proposed controls have been implemented, the impact/level of risk has changed to:			

If the proposed controls have not been implemented, please describe why not, and outline plans for actioning the proposed control.	
I can confirm that any new work programmes have been assessed for information risk and reflected in this return.	Yes/No

Notes on reviewing the information Risk Register

1.1 IAOs must review information risks on a regular basis and, where appropriate, escalate any risks to the SIRO. At each review consider if existing risks are still relevant, achieve the same score and if new risks have emerged. Even where risks remain the same, it is likely that controls and contingency plans will require updating

1.2 Where an operationally significant risk has been identified the IAO will need to describe the mitigating actions that will be put in place and then assess the residual risk rating, taking into account the additional measures that are being proposed. When the review of the Risk Register is carried out the IAO must take into account when the mitigating actions have been carried out so they can be entered onto the register as control measures.

1.3 As well as existing risks that have already been identified, the review must also consider forthcoming potential changes in services, technology and threats that may give rise to new risks.

1.4 Please complete and submit the information risk return together with the updated Service Area Risk Register to the Senior Information Risk Owner (SIRO) by emailing both documents to Corporate Information Governance Unit at 'Information Unit' address.

Information Risk Return dates *[1 March – 30 Aug or 1 Sept - 31 Feb]*[i2]

Service Area:……

Risk Owner – Head of Service (IAO)

Risk 1: Inappropriate disclosure of personal data		**Active Controls**				**Proposed controls**	
Cause	**Effect**	**Last Period**		**Current**		**Target**	
		I	**L**	**I**	**L**	**I**	**L**
Lack of identification of those information assets containing personal data and sensitive personal data. Lack of awareness training. Absence of Information Sharing Protocols (ISPs) or other agreement (e.g. memo of agreement). Failure to double-check contents proposed for disclosure (including data sitting behind Excel or Word docs). Advice on disclosure of information is not sought from line manager and/or Corporate Information Governance Unit.	Serious and unwarranted damage and distress to individuals Breach of DPA and infringement of privacy Regulatory, court action or financial penalties Damage to reputation and integrity Cost and resources required to investigate						

Risk 2: Theft, loss or unauthorised access to information (electronic and system related)		**Active Controls**		**Proposed controls**
Cause	**Effect**	**Last Period**	**Current**	**Target**

		I	L	I	L	I	L
Inadequate access and permissions management Password sharing Poor information asset management - network drive and e-mail Dishonesty Emails sent to wrong address or lost / compromised during transmission Inadequate business continuity planning	Serious and unwarranted damage and distress to individuals Breach of DPA and infringement of privacy Regulatory, court action or financial penalties Damage to reputation and integrity Cost and resources required to investigate Cost of recreating / retrieving information						

Risk 3: Theft, loss or unauthorised access to information (paper based)		Active Controls				Proposed controls	
Cause	**Effect**	Last Period		Current		Target	
		I	L	I	L	I	L
Documents stored in damp conditions, not rat-proof and damaged beyond repair Documents not filed correctly and not available to be retrieved Dishonesty / sabotage Carelessness Tidy work area not enforced Documents posted / faxed to wrong address or lost / compromised during transmission Incorrect shredders (ribbon) used for document destruction Records being transferred to new location as a result of rationalisation of Council buildings	Serious and unwarranted damage and distress to individuals Breach of DPA and infringement of privacy Regulatory, court action or financial penalties Damage to reputation and integrity Cost and resources required to investigate Cost of recreating / retrieving information						

Risk 4: Ineffective or Insecure Information Sharing internally and externally							
Cause	**Effect**	**Last Period**		**Current**		**Target**	
		I	**L**	**I**	**L**	**I**	**L**
ISPs / agreements not in place or not comprehensive enough Failure to share the right information with the right people at the right time Failure to meet the FOI Compliance rate Lack of awareness of what information is held and therefore when/where it could be beneficially shared Shared information is not stored securely (paper or electronic)	Information used for purposes other than those agreed Serious & unwarranted damage and distress to individuals Breach of DPA and infringement of privacy Damage to reputation and integrity Information not shared prior to the departure of staff - knowledge not retained Loss of business continuity						

Risk 5: Records retained for the wrong length of time		**Active Controls**				**Proposed controls**	
Cause	**Effect**	**Last Period**		**Current**		**Target**	
		I	**L**	**I**	**L**	**I**	**L**
Information not covered by retention policy; particular attention to be paid to European funded programmes, which need to be retained for 13+ years after the end of programme. Lack of awareness	Breach of DPA, FOI & Public Records Act Breach of other requirements for the retention of records Unnecessary cost of storage of physical and						

Lack of motivation to file records appropriately and regularly Dishonesty / sabotage Records retained 'just in case'. Lack of awareness of what information is held and therefore when it should be disposed of. Reduction in staff / staff not replaced results in increased workload – could impact on ability to archive / destroy records	electronic information Inability to protect Council's best interests in cases of litigation because relevant records have been destroyed or can't be found Premature destruction seen as an attempt to prevent disclosure Regulatory, court or financial penalties Damage to reputation and integrity						

Risk 6: Failure to create or locate reliable records as evidence of business decisions and activities		**Active Controls**				**Proposed controls**	
Cause	**Effect**	**Last Period**		**Current**		**Target**	
		I	**L**	**I**	**L**	**I**	**L**
Records not created in the first place that documents key decisions and activities **Records retained unnecessarily result in large volumes of data to be searched if information is requested** **Electronic records (network drives and e-mail) not stored / saved correctly.** **Physical records not stored in their correct location** **Electronic and physical filing not carried out regularly.**	Breach of DPA and FOI Records required for evidential purposes (i.e. in court) will not be available Inability to defend the Council in any legal action Critical information can't be found or takes too long to find when needed						

Risk 7: Information assets, including vital records, lost as a result of fire, flood, server failure, a power loss etc.		**Active Controls**				**Proposed controls**	
Cause	**Effect**	**L**	**P**	**C**	**r**	**T**	**r**

		I	L	I	L	I	L
Vital records not identified in local business continuity plan Business continuity plans are not in place	Vital records may be destroyed Unable to access information with potential legal & financial consequences Significant investment required in the case of a major incident or failure Business continuity affected						

Risk controls:

Service Areas need to:

- Review causes and effects of the risks to check whether they need to be adjusted.
- Review the active controls to make sure they are still in place and effective.
- Review the proposed controls to check whether they can be moved across to active.
- Add new active and proposed controls as applicable, bearing in mind any corporate controls suggested at IGPT.
- Finally review scoring to check whether the changes you have made enable you to score lower in likelihood and/or impact.

Suggested active controls

	Date actioned	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
Reminder to staff to comply with Corporate Risk Management Policy and Risk Appetite Statement.								
Reminder to staff to comply with information request policies (FOI, EIR and Subject Access Requests)								
Reminder to staff to comply with IT Security and Data Protection policies.								
Awareness raised of Data Breach Reporting Procedure.								
Awareness raised of need for Privacy Impact Assessments								

Awareness raised of guidance on ensuring Word / Excel do not contain hidden data on IG intranet.								
Awareness raised of File Naming Conventions on IG intranet.								
Awareness raised of Record Retention and Disposal Policy, including use of Council approved confidential waste supplier.								
Seek retention advice from Corporate Information Governance Unit as required.								
Relevant staff aware of the need to retain European funded programme documentation until WEFO authorise disposal.								
Awareness raised of guidance on Email Good Practice and How to Manage Email within Outlook on IG Intranet.								
Information Asset Register completed.								
Vital Records identified as part of the Information Asset Register and included in Business Continuity Plan								
Regular [give frequency] Protecting Information e-learning for all staff completed.								
Protecting Information (paper version) provided to non-pc user staff on a regular [give frequency] basis.								
Data Protection / FOI /CCTV / Records Management training attended.								
Staff who share information to undertake on-line Information Sharing Training on All-Wales Academy website								
Need for Information Sharing Protocols or other agreements considered.								
Only encrypted removable media (e.g. laptops, smartphones and USB sticks) will used.								
Use of secure email systems – GCSx and Egress considered.								
Documents stored in appropriate containers and kept in safe, dry conditions.								
Inventory of archived records and their location being undertaken, and records that have passed retention period disposed of.								
Only cross-cut shredders used – all ribbon-cut shredders replaced.								
Add any additional controls relevant to your Service Area								

Suggested proposed controls

	Target date	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
Review storage of vital records								
Tidy work area to be enforced, leading to regular filing of physical records.								
Raise awareness of importance of keeping records, one of the organisation's most important resources, correctly.								
Raise awareness of staff of the Public Service Ombudsman's new Principles of Good Administration and Records Management, in particular the two new principles on records management (in IGPT W drive folder).								
Allocate time for staff to review records starting with offices and Council Records Centres with a view to disposal, including offering to Glamorgan/Gwent Archives, and make sure the Council's retention schedules are followed and disposal documented in case of future challenge. Once hard copy records are dealt with, follow same process for electronic records, and maintain this house-keeping in future.								
Remind all staff to double-check address details (email and hard copy) – significant number of breaches still being reported in this area.								
Review Information Asset Registers								
CCTV review								
WASPI Facilitator trained for Service Area								
Raise awareness of new 2 min DPA training and new IG intranet								
Raise awareness of Data Controller and Data Processor Agreements								
Identify records requiring long-term retention that are held electronically, so that digital preservation requirements can be considered								
Add any additional proposed controls relevant to your Service Area								