Information Risk Management (Policy and Procedure)

OFFICIAL

Publication Scheme Y/N	Can be published on Force Website
Department of Origin	CSD
Policy Holder	Head CSD
Author	Head of Strategy & Business Development
Related Information	APP Information Management APP Management of Information MoPI UK General Data Protection Regulations Data Protection Act 2018
Date First Approved at SMB	30/01/2019
This Version	V1.1 01/04/2022
Date of next Review	01/04/2025

April 2022

Policy

Contents

Version History

Version Number	*Date*	*Rational behind amending/updating policy or procedure.*	*Policy Owner details*
V.1	31/01/2019	New Policy	Head of CSD (Head of Strategy & Business Development)
V.1.1	05/04/2022	Amendments to include ICO Audit recommendations	Head of CSD (Head of Strategy & Business Development)

Policy

Statement

Merseyside Police is committed to ensuring good information management and recognises that the effective management of police information to a high standard is core to efficient policing. Information is the lifeblood of the force and as a critical business asset it needs adequate protection and management, commensurate with its degree of reliance and sensitivity.

Merseyside Police is committed to adhering to information related legislation and standards with particular emphasis on maximising the benefits effective information management brings to operational policing.

Aims

This aim of this policy is to set out the arrangements that are in place to manage **information risks**, to facilitate effective, clear direction and to support achievement of compliance with legislation, statutory obligations, and good practice standards.

Objectives

a) To ensure that the force's information is processed in compliance with legislation and force risk appetite.

b) To provide a risk management framework to ensure consistency of approach around the management of information risk.
c) To encourage a proactive rather than reactive approach to information risk management.
d) To promote a well-managed and informed information risk management process and improve the quality of decision making
e) To ensure the force's assets are safeguarded (people, information, property, finance and reputation)
f) To define the forces risk appetite and ensure risks are managed in line with this appetite.
g) To define the key and accountable roles within the force that can accept information risk and the level of risk they can accept

Application and Scope

This policy applies to all information and assets held and used by Merseyside Police, including that used for policing duties, e.g., crime and incident reports and for administrative purposes e.g., employment records, payroll.

The policy applies to all Merseyside personnel including police officers, police staff, special constabulary, and volunteers, who use the force's information as necessary to carry out their 'policing duties'. It equally applies to contractors, partner agencies and other individuals who may have access to the force's information for the purpose of carrying out their 'policing duties,' or general processing.

In particular this policy applies to Information Asset Owners, Project Managers and ICT staff that are most likely to make changes to the manner in which information and assets are managed and which could present risks to the force and wider public sector partners.

For the purposes of this policy, policing duties assumes the same definition as the Code of Practice for the Management Police Information, which highlights:

- Protecting life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty of responsibility of the policy arising from common or statue law.

This policy document sets out principles to help guide decision making and is in some parts quite prescriptive. However, it is vital that officers and staff have the freedom to innovate, exercise discretion and take risk-based decisions centred on the needs in the circumstances and the merits of each case. There may be occasions when a member of staff is considered to have acted outside of policy but if they have done so with honesty, integrity and professionalism, to make the best decision for the community we serve, they will be trusted and supported. On occasions when this is the case, the rationale for it must be properly recorded

Outcome Evaluation

The SIRO (Senior Information Risk Owner) Governance Board will evaluate outcomes resulting from of regular monitoring taking into consideration the following:

a) Compliance with legislation and national information management standards.

b) Reduction in data protection breaches/ICO (Information Commissioner's Office) referrals which may be attributable to gaps in information risk management.

c) Improve data quality and consistency in decisions to process.

d) Improved understanding of information risk from accountable roles.

The information will be made available to Chief Officers and the SIRO upon request.

Procedure

1. Overview

1.1 Authorised Professional Practice (APP) is produced by the College of Policing as the official source of professional practice on policing. All officers and staff are expected to have regard to APP in discharging their responsibilities. Essentially, our "policy" is to comply with APP as it develops to cover all areas of policing.

Where content exists within APP we should not be reproducing it locally but instead signposting the on-line version. Similarly, we should not retain or develop any local policy documents if the subject matter is covered by APP. We may have some relatively low volume procedural documents but only if they are deemed necessary to supplement the content of APP. This is one such document.

1.2 Merseyside Police recognises that the effective management of police information to a high standard is core to efficient policing. Information is the lifeblood of the force and as a critical business asset it needs adequate protection and management, commensurate with its degree of reliance and sensitivity.

1.3 Merseyside Police is committed to adhering to information related legislation and standards, with particular emphasis on maximising the benefits effective information risk management brings to operational policing. It details the responsibilities of those concerned with information risks including, but not exclusive to:

- Information Asset Owners
- ICT
- Project Managers
- Information Management Specialists/Board members; and
- Senior Information Risk Owners.

1.4 Information risks are defined as threats to:

- **Confidentiality** – ensuring only authorised persons can access or be provided with information
- **Integrity** – ensuring the information is authentic, accurate and complete, not excessive; and
- **Availability** – ensuring authorised persons can access it when they need to at the right time and in the right way.

1.1. The policy also details the processes to be followed to identify information risks, determine who can accept information risks on behalf of the force and the process for the escalation of information risks.

2. Information Management – Accountable Roles

2.1 Most of the accountable and other key roles mentioned below will need to complete or refer to existing relevant Data Protection Impact Assessments (DPIA) while assessing risk against proposed or current processing practices. Having a DPIA is an integral part of the Information Governance & Compliance Cycle along with the Record of Processing Activity (ROPA). The ROPA assesses the necessity, proportionality, and lawfulness of specified processing whilst the DPIA assesses the impact that such processing has on the data subjects involved in the processing. Both documents assist in determining and, when completed, demonstrating compliance with the legislation (S64. DPA 2018) and accountability to data subjects, the Information Commissioner and ourselves as members of the police family and as individuals. Further information about DPIAs and ROPAs are available. Policies are available on the iForce policy pages iForce policy pages and the DPIA and ROPA templates are available useful document list on the Information Assurance & Data-Protection. iForce page.

2.2 **Appendix 1** sets out the structure for information risk management within Merseyside Police.

2.3 The Data Controller is the Chief Constable who is ultimately accountable for information and the risks taken.

2.4 The Senior Information Risk Owner (SIRO) is the Deputy Chief Constable of Merseyside Police, who holds the delegated responsibility for oversight of this policy through the SIRO Governance Board, setting the Local Force Risk Appetite Statement (**Appendix 2**) and leading the management of information risks for policing within the force. This includes:

- Leading and fostering a culture that values, protects, and uses information for the public good.
- Owning the information risk management policy and information risk assessment process; and
- Being accountable to the Chief Constable, advising them on information risks and taking and/or accepting or rejecting risk-based decisions in respect of the manner in which information is to be managed within their force.

2.5 Information Asset Owners (IAO) are accountable to the SIRO and for reporting information risk as necessary. An IAO is responsible for knowing what assets they own, who has access to the asset(s), its use (including information added/removed), keeping it up to date, keeping it secure and identifying risks to the information and its effective management. IAOs are supported in their role by the Data Protection Officer (DPO), Information Assurance Coordinator (IAC) and IT Security Officer.

3. Information Risk Management – Other Key Roles

3.1 It is important that consultation on new projects takes place with information specialists at the outset to enable a proactive approach in identifying and managing information risks. The key roles to support this within Merseyside Police are:

- The Data Protection Officer (DPO) – the force expert, providing professional advice and guidance to the organisation on compliance with the Data Protection Act 2018

(DPA) and GDPR; informing and advising the data controller and SIRO of the force's obligations under the DPA.

- The Information Assurance Coordinator (IAC) – coordinates, develops and implements information assurance initiatives to meet the force's statutory responsibilities and ensure compliance with the police Community Security Policy, current legislation and all national/local, Home Office, College of Policing and NPCC policy objectives.

- The Force Records Manager – ensures availability, integrity and confidentiality of personal data and other records and its' timely review, retention, or deletion.

- IT Security Officer (ITSO) – responsible for providing technical advice and ensuring information risks are brought to the attention of the IAO and/or specialists within the Information Management business area during any new system design, development or configuration that might affect the confidentiality, integrity, or availability of force information.

- Force Risk Manager – To provide the force with the underpinning risk management, corporate governance, and business development structures necessary to drive effective and efficient strategic decision making. Coordinate, maintain and promote risk management arrangements within the Force in line with the principles of risk management. Develop, manage, and maintain risk registers at various levels throughout the organisation that clearly identify the risks facing the Force, together with the relevant mitigating actions aimed at reducing those risks. Report to Chief Officers on the risk profile at regular intervals via the corporate meeting structures.

- Information Compliance Officers will monitor compliance with this, and other Data Protection Policies and Procedures will by assurance mapping and scrutiny/analysis of Security Breach reports to identify risks. The results will be used to inform Information Risk Management procedures and be notified where relevant as Key Performance Indicators to the Senior Information Risk Owner (SIRO) Board.

  Where appropriate, this may also prompt further internal audit in addition to existing planned audit processes.

4. Information Risk Register

4.1 The Information Management Risk Register is overseen by CSD and is used to support decision making and activity in respect of the SIRO Governance Board, chaired by the DCC. It is consistent with the force's other risk registers/dashboards.

4.2 Significant risks identified within the Information Management Risk Register will be escalated, where appropriate, for consideration onto the Strategic Risk Register on a quarterly basis following each SIRO Governance Board meeting.

4.3 The IAC will work with those directly involved in information management, including the ITSO, DPO, Records Manager as well as information access and compliance and audit teams to review the information risks and agree mitigating actions / controls to be taken.

4.4 Depending on the degree of risk, the IAC will decide whether it is appropriate to escalate any information risks to the SIRO in the form of a separate SIRO report. **(Appendix 4).** If the risk involves personal data, the IAC may refer to the DPO who may provide advice or refer up to the SIRO

.

4.5 Information risks will also be recorded following work undertaken to comply with:

- Statutory Codes of Practice
- National Policy
- Codes of Connections
- Risk Management & Accreditation Document Sets (RMADS); and
- IT Health Checks.

1.4 Information risks arising from such work will be escalated to the Information Management Risk Register and/or SIRO reporting process, as necessary.

1.5 Information risks may be discovered following:

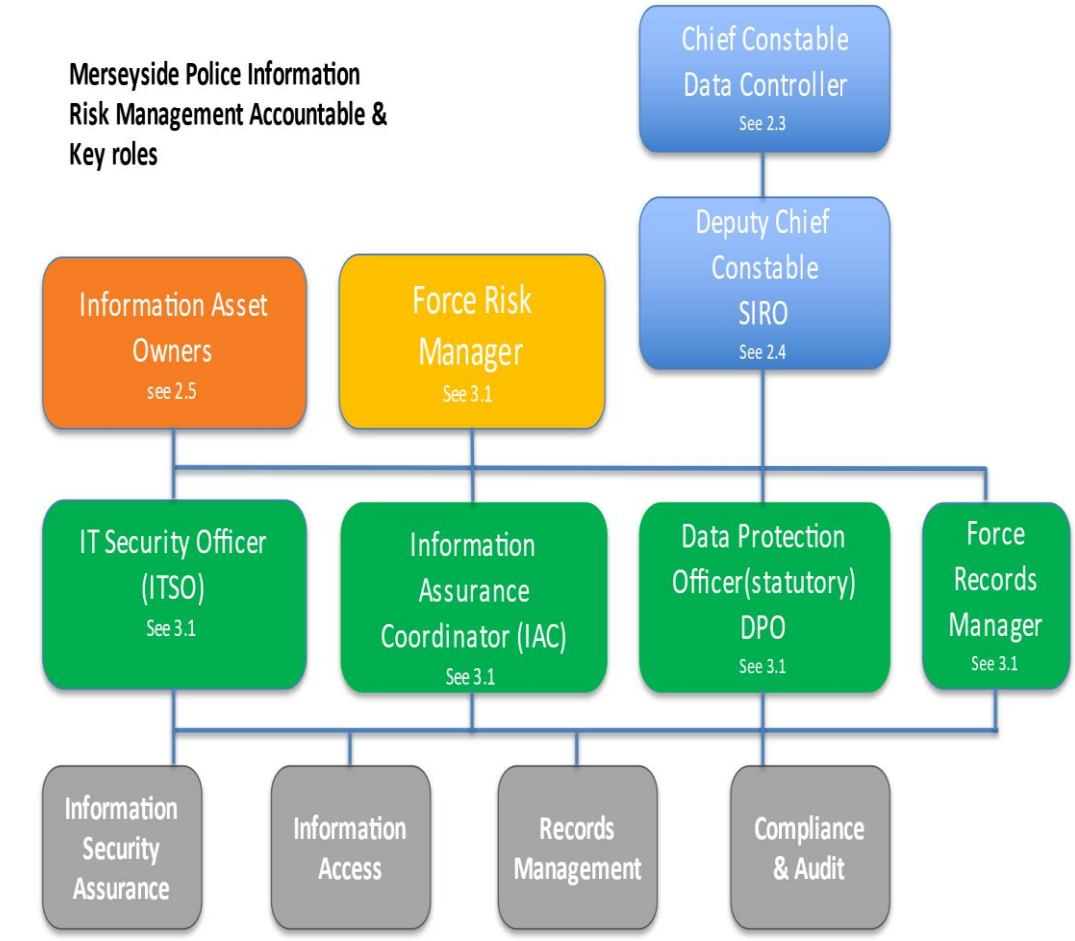
- audits,
- assurance mapping,
- personal data breaches or other security breaches,
- IAO assurance reporting.

Also, identified risks may be examined by the deployment of assurance mapping or internal audit to identify inherent risk and therefore accept or mitigate the risk.

Documenting Risks

Guidance on methodology to Assess and identify residual risk and thereby risk appetite is at Appendix 2.

Appendix 1


Merseyside Police Information Risk Management Accountable & Key roles
Chief Constable Data Controller
See 2.3
Deputy Chief Constable SIRO
See 2.4
Information Asset Owners
see 2.5
Force Risk Manager
See 3.1
IT Security Officer (ITSO)
See 3.1
Information Assurance Coordinator (IAC)
See 3.1
Data Protection Officer(statutory) DPO
See 3.1
Force Records Manager
See 3.1
Information Security Assurance
Information Access
Records Management
Compliance & Audit

Appendix 2

Information Risk Management

Local Force Information Risk Appetite

Introduction

This document sets out Merseyside Police's **Information Risk Appetite** for information risk such as theft, loss (both unintended release and loss of access to), corruption, access, or unintended alteration of the information assets for which it has responsibility. It is set by the Force Senior Information Risks Owner (SIRO) governing the information assets under their level of control.

This document is to inform Information Asset Owners (IAOs), Information Security Managers, Accreditors, Information specialists, Project leads, ICT and other interested parties of the force's Information Risk Appetite Statement and its implications. It will enable such persons to make effective decision and **defines the extent to which information risk must be mitigated or escalated**. IAOs and Accreditors can only deviate from the Risk Appetite with the authority of the SIRO, following a Risk Escalation Case (see below).

The risk appetite is defined using the framework of the National Policing Risk Appetite Statement which is subsequently aligned to the Information Risk Directive that is published and maintained by the Office of the Government Senior Information Risk Owner (SIRO).

This risk appetite aims to support IAOs and Accreditors to effectively manage information risks to avoid the development of an overly cautious and risk adverse approach to information management and/or excessive risks being taken without due care and attention.

Risk Appetite

Risk appetite is defined as:

> ***"The amount of risk that an organisation is prepared to accept or be exposed to at any point in time"***

This document identifies the baseline for managing information risks for Merseyside Police's information systems for example Niche, Storm etc. and their infrastructures and capabilities based on the need to protect information that is shared by both forces with other law enforcement agencies, central and local government bodies, and voluntary bodies.

Insufficient guidance on legitimate, acceptable levels of risk may develop an overly cautious (risk averse) culture which results in a failure to seize important opportunities that maximise performance. Conversely excessive risk may be accepted without regard to the potential impact. It is imperative that the Local Force Information Risk Appetite is set and delegated throughout the force. Effective alignment of risk exposure to risk appetite maximises business performance through taking acceptable risks when developing and delivering services.

When addressing risk, it is important the controls applied are pragmatic, appropriate and cost effective. The Local Information Risk Appetite will assist force Information Asset Owners, Project Managers, Accreditors (Information Security practitioners), ICT staff, Programme Managers, and other interested parties to understand and manage information risks by setting out the risk acceptance and escalation criteria for Local Information Systems and the data they hold regardless of its business impact level or protective marking.

The Local Information Risk Appetite forms part of the overall Information assurance governance for Merseyside Police and is owned by the SIRO and ratified by the SIRO Governance Board.

Scope

This document relates to the Information Assets for which the Chief Constable of Merseyside Police is Data Controller.

It also takes into consideration the requirements of the National Policing Information Risk Appetite statement (which provides a framework for all risk decisions in relation to data held on National Police Information Systems[1].

Method

There follows, 5 tables which will assist you in assessing and categorising risks and risk appetites around the system/project/process you are considering. Tables 1 to 4 provides information to assist you in completing table 5 which will be your assessment.

Risk Ranking and Appetite Definitions and Application (Tables 1 & 2)

Information Assets

Table 1 - provides the suggested risk rankings, largely based upon the impact. These are used by the Office of the Government SIRO.		**Table 2 -** sets out the categories and definitior of risk appetite that will be used for setting the Local Force Risk Appetite.	
In many cases the risk ranking correlates across to the risk appetite category on the same row though this does not have to be so.			
To arrive at a Risk Ranking select which of the below describes the risk(s) involved	**Risk Ranking**	**Risk Appetite Description**	**Risk Appetite category**
This is above the organisation's defined tolerance level. The consequences of the risk materialising would have a disastrous impact on the organisation's reputation and business continuity. Comprehensive action is required immediately to mitigate the risk.	**Very High**	Avoidance of risk and uncertainty is a key organisational objective.	**Averse**
The consequences of this risk materialising would be severe but not disastrous. Some immediate action is required to mitigate the risk, plus the development of a comprehensive action plan.	**High**	Preference for ultra-safe business delivery options that have a low degree of inherent risk.	**Minimalist**
The consequences of this risk materialising would have a moderate impact on day-to-day delivery. Some immediate action might be required to address risk impact, plus the development of an action plan. Status of the risk should be monitored regularly.	**Medium**	Preference for safe delivery options that have a low degree of residual risk.	**Cautious**
The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered. Status of the risk should be monitored periodically.	**Low**	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while	**Open**

[1] The system must be one which is provided for the Police community as a whole and managed centrally, and it must be used by a number of forces (at least 10), and Police ICT Directorate and/or PNC Services of the Home Office have a contractual relationship with the service provider and/or the service management of the system. N.B. Managed centrally makes the distinction that the system is not distributed (e.g. PNC which is hosted and administered centrally) or a distributed system, hosted and managed at individual force level (e.g. Holmes 2). A system in a cloud environment which is centrally administered is considered a centrally managed system.

		also providing an acceptable level of reward (and value for money etc).	
The organisation accepts this risk / impact of risk would be insignificant. Status of the risk should be reviewed occasionally.	**Very Low**	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater risk.	**Hungry**

Information Assets by category with suggested risk appetite (Table 3)

The level of risk appetite, and therefore the severity of subsequent risk controls, will vary for different information asset types that are relevant to policing to allow Merseyside Police to make improved risk management decisions based on the actual business impact of the loss or compromise of the data.

Table 3 - provides a list of the different information assets that Merseyside Police manage:		
Information Asset	**Description**	**Risk Appetite**
Police Marketing and Communications	Information generated, collected, stored, and used for internal and external marketing and communications.	**Open**
Personal Data	'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person; (GDPR Article 4.1. see also DPA 2018 Part1 section 3 (2) & (3))	**Cautious**
Special categories of personal data	personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (GDPR Article 9.1.)	**Cautious**
Personal data relating to criminal convictions and offences	Processing of personal data relating to criminal convictions and offences, or related security measures based on Article 6(1) (GDPR Article 10)	**Cautious**
Public / Citizen	Personal data, as defined by GDPR and DPA2018, of all citizens collected, stored and utilised by the police. (see below)	**Cautious**
Commercial / Procurement / Supplier	Information collected, stored, and used throughout the procurement process.	**Open**
Police Corporate Information	Information generated, collected, stored, and used by the corporate functions of forces. Includes policy, security metrics et al.	**Cautious**
National Security Commercial / Procurement / Supplier	Information collected, stored, and used throughout the procurement process of systems and services related to national security.	**Cautious**

National Security Corporate Information	Information generated, collected, stored, and used by the corporate functions of forces and directly related to management of national security. Includes policy, security metrics et al.	**Cautious**
Covert Intelligence	Information generated, collected, stored, and used in the course of covert intelligence operational processes.	**Minimalist**
Counter Terrorism	Information generated, collected, stored, and used in the course of counter terrorism operational processes.	**Minimalist**

Information Risk Delegation Matrix (Table 4)

The **Information Risk Delegation Matrix** below indicates to those involved in information related projects the points at which they need to escalate risk to the IAOs, Accreditors (ISM) and SIRO. The Information Risk Delegation Matrix is to be used for determining the level of residual risk ownership and demonstrates how the risk appetites vary between the risk ownership for Residual Risk Levels.Residual risk is an indication of the level of risk remaining **after controls** have been implemented to mitigate the risk. The Force SIRO may delegate the handling of particular risks to the IAO while retaining accountability for it.

Table 4 – Information Risk Delegation Matrix. (Level/Risk Appetite matrix to identify minimum accreditor)

Residual Risk level	**Risk appetite**				
	Averse	**Minimalist**	**Cautious**	**Open**	**Hungry**
Very Low	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)
Low	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)
Medium	IAO	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)
Medium-High	SIRO	IAO	IAO	Accreditor (IAC or ITSO)	Accreditor (IAC or ITSO)
High	SIRO	SIRO	SIRO	IAO	Accreditor (IAC or ITSO)
Very High	SIRO	SIRO	SIRO	SIRO	IAO

Table 5 – The assessment of risk rankings and risk appetite to each question are likely to result in differing individual risks and appetite in the first instance. Some questions may not be relevant to your assessment but are present to assist in considering all potential areas of risk. Complete a separate assessment for each information asset type (table 1) which may be relevant to your project

	Question/consideration	Your Answer/ Comments describing the risks	Idenitfy the assessed risk ranking from table 2 above.	Idenitfy the assessed risk appetite from table 3 above
1	Name the system to which this assessment is taking place			
2	List the categories of Information Assets involved in the project from table 2 of appendix 2 of the Information Risk Management Policy here and assess the risks to each information category separate by completing separate assessments for each category of information.			
3	Willingness to pay for adequate mitigation of information risks			
4	Are there particular political or operational imperatives relating to the system?			
5	Impact of information security breach			
6	Compromise of police operations, e.g. > Risk to life and safety; > Disruption of emergency services; > Hindrance to the fighting of crime;			
7	Compromise to judicial proceedings			
8	Damage to Police reputation and credibility			
9	Undermined confidence in the government			
10	Financial losses and penalties			
11	Breach in legal or compliance position			
12	Loss of personal data or private/sensitive information			
13	In the context of this system are we averse to certain types of threat sources, e.g. serious and organised crime? (It is worth consulti the National and Local Threat Assessment to understand the current threats to poli and their severity.)			
14	In the context of this system are we averse to certain types of incident e.g. interception by criminal groups?			

15	Are we less concerned about certain types of risks, e.g. unauthorised access by third party staff?			
16	Have incidents in the past indicated a tendency for risks to this information being exploited?			
17	If we are handling data owned by partners or third parties, what is their Appetite / Tolerance for information ri associated with this system? What rules do they have for handling that information?			
18	Are we more, or less willing to pay to mitigate risk? In the context of this system, would the risk disclosure, confidentiality, or integrity of the information have a serious impact?			
19	Budgetary pressures have become the norm; this is not therefore regarded as a reason to apply a higher Risk Tolerance for a system. However, it may influen the SIRO decision not to spend on the risk mitigation option proposed in a Risk Balance case.			
20	Are the aspects explored above time-bound or permanent?			
21	Is this system or process fully compliant with the General Data Protection Regulations and Data Protection Act 2018?			
22	Does this system or process have the ability to delete data?			
Assessment Results. – This should reflect the residual risk remaining **after controls** have been implemented to mitigate the risk. To arrive at this final assessment include below the highest risk ranking and the risk appetite closest to or 'Averse' should be taken from the answers to the questions above.				
	Final assessment result	Insert any comments you would like to ma to substantiate your assessment in li 23 below	Insert Highest risk ranking (from table 1)in line 23 below	Insert appetite closest to or Avers (from table 2) in line 23 below
23	Results line			
24	Based upon the results in line 23 the relevant role to accept or reject this risk per table 4 is	Delete as approriate	Name of person completing this assessment is	Date of completion

		SIRO IAO IAC/ITSO		

When completed, please submit this assessment to the relevant role as decided at line 24 above and in accordance with the matrix in table 4 of appendix 2. All submissions must be routed via the IS Security Coordinator (ITSO) then the Information Assurance Coordinator (IAC), the IS Security Coordinator and then the Information Asset Owner (IAO) for approval or otherwise.

Should the risk appetite indicate that the risk is to be signed off by the SIRO then the SIRO risk escalation form below must be completed and submitted via the IAC, ITSO and IAO and then to the SIRO.
The Information Assurance Coordinator will also share the result of the assessment and the decided risk appetite with the Force Risk Manager when the process is completed.

MERSEYSIDE POLICE

SENIOR INFORMATION RISK OWNER (SIRO) REPORT – Risk Escalation Case

This document must be protectively marked to a level commensurate with the content.

The ITSO and IAC will assist the author in the completion of this report if required

Protective Marking:	
Suitable for Publication Scheme? Y/N:	
Title & Version:	
Purpose:	
Relevant to:	
Summary:	
Author:	

Dept/Command:	
Date Created:	
Review Date:	

INFORMATION re ACCOUNTABILITY

As required under HMG Information Assurance Standard No 1 & 2 and the supported GPG 47 (Information Risk Management), as part of the accreditation process, Accreditors are fully accountable for their decisions and actions in their role as Information Assurance (IA) risk assessors and risk managers.

Although **not liable** in law, they can be called to account for their business actions in a legal proceeding. Liability is the responsibility of a Data Controller and/or Board, or their equivalent within a "Government Department". In the case of the Merseyside Police this relates to the role of the SIRO/Chief Constable.

This document supports the business actions performed by the Accreditor and any other relevant parties and any business decisions made are fully documented and traceable.

BACKGROUND

Example - Detail of the proposal and general information risks

ISSUES

Example - Detail of the information risks associated with the proposal that have necessitated the referral to the SIRO

REASON FOR SUBMISSION

Example - Acceptance of risks to manage operational requirements

RISKS / ISSUES / IMPACT / MITIGATION

Example - What are the risks, what is the likelihood and impact, how could the risk be mitigated, what risks would remain.

AFFECTED DATA

Type	Example - Corporate force information
Protective Marking	Example - Restricted

AFFECTED DATA	
Sensitivity	Example - Personal data – previous convictions
Quantity	Example - 100,000 nominal records

Relevant Security Policies and Standards/others

Mandatory Requirement	Requirement Details	Issues / Mitigations / Recommendations
Example - ACPO Code of Connection	Example - Mandatory controls are required to secure access by third parties	Example - Industry best practice standard ** is required at a cost of £**

Appendices
Example - signpost any appendices which you have attached to this report here

RESIDUAL RISK ASSESSMENT & RECOMMENDATIONS – NB the ITSO, IAC and IAO may insert their observations or recommendations here
ITSO – Insert Findings, further mitigations, and recommendations here.
IAC – Insert Findings, further mitigations, and recommendations here.
IAO – Insert Findings, further mitigations, and recommendations here.

SIRO RISK DECISION		
	SIRO Comments	
Accept **Reject** (delete as appropriate)		
Name/Signature:		**Date:**

Please return the document to the author following the SIRO decision and copy in the ITSO, IAC and IAO.