The Leveson Inquiry into the Culture Practices and Ethics of the Press

Exhibit Ref:	JK/6
Witness:	ACC Jerry Kirkby
Date Produced:	21 March 2012
Description:	Surrey Police Force Information Risk Appetite Statement
Signature:	.....

Document Attached.

Force Information Risk Appetite Statement.

1 Purpose

The purpose of this document is to define the Information Assurance Risk Appetite Statement for Surrey Police. The statement will enable people, particularly those involved in Information Risk Management, to take well calculated risks when opportunities arise that will improve service delivery and, conversely, to also identify when a more cautious approach should be taken to mitigate threats or risks.

In addition, the Information Risk Appetite assists in embedding a culture of information risk management and accountability.

2 Governance

The risk appetite statement for Surrey Police is set by the Senior Information Risk Officer (Deputy Chief Constable) and validated by the National Accreditor.

3 Definitions

- **Risk Appetite** sets out the amount of risk, at a corporate level, the force is prepared to accept, tolerate or be exposed to at any point in time.
- **Risk Tolerance** allows for variations in the amount of risk the force is prepared to accept for a particular project or business activity. It will take into consideration the political or operational imperatives driving the activity, and ask in the context of the particular activity, whether there are certain categories of risk which the organisation may be more or less willing to accept.

4 Context

The strategic priorities for Surrey Police are:

- **Confidence and satisfaction** – keeping public confidence in the police high and ensuring satisfaction with the service we deliver to local people
- **Safety** - keeping people safe from harm
- **Value for money** - making the most of our people and resources.

Information is a key resource used to achieve these objectives, and the availability of that information can be imperative to our activity.

Furthermore, the police service has a high profile in the government and national media, and risks to reputation, credibility, finance, compliance (including privacy of personal data) must be considered against business

benefits whilst also maintaining confidence and reassurance that information risk is being appropriately managed.

As such, information must be protected to prevent it from becoming a liability as information breaches can easily compromise the policing objectives or an individual's personal safety.

There is a legal and regulatory requirement to protect personal and sensitive data that is owned by or managed on behalf of the Force, including the Force's delivery partners. Failure to do so appropriately can result in serious financial or reputational damage (the ICO has the power to fine up to £500,000 for data protection breaches.)

5 Description of Risk Appetite Levels

HMG Information Assurance Standard 2 refers to the five levels of risk appetite which can be applied to a broad range of corporate risks. These are defined in the table below:

Appetite Levels	Description
Averse (Low)	Avoidance of risk and uncertainty is a key objective.
Minimalist (Medium Low)	Preference for ultra safe options that have a low degree of inherent risk and only have a potential for limited business benefit
Cautious (Medium)	Preference for safe options that have a low degree of residual risk and may only have limited potential for business benefit
Open (Medium High)	Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of business benefit
Hungry (High)	Eager to be innovative and to choose options based on potential higher rewards despite greater inherent risk

Table 5.1

6 National Risk Appetite Statement

In the provision and use of National Systems, there is a wider community to consider. National systems often enable the sharing of information and intelligence, which can be crucial to efficient and effective policing. Standardisation in the protection of information provided by National Systems is offered through a consistent Information Risk Appetite across all forces/agencies using National Systems.

The risk appetite for the national police service overall in relation to the use of national systems is defined by ACPO as 'Cautious'.

This implies that forces can adopt a risk appetite of 'Cautious', or a more averse risk appetite, depending on their attitude and behaviour.

7 Surrey Police Risk Appetite Statement

Surrey Police has chosen to formally specify an '**Open**' risk appetite.

> The deviation from the national risk appetite is based on a risk-balanced requirement to support fast delivery of information solutions and communications in a rapidly changing environment and within a context of severe financial constraints and a requirement to deliver value for money for the public. It is recognised that National Systems have a wider impact, so they are deemed to attract more caution than local systems when it comes to accepting information risks.

The Risk Appetite reflects the level of residual risk the SIRO is comfortable to accept in the Force's business as usual; taking into consideration:

- Willingness to pay for adequate mitigation of information risks;
- Ongoing political context and operational imperatives of the organisation;
- Impact of information security breaches;

And weigh up the above within the following Risk Categories:

- Compromise of police operations, e.g.
  - Risk to life and safety;
  - Disruption of emergency services;
  - Hindrance to the fighting of crime;
  - Compromise to judicial proceedings;
- Damage to Police reputation and credibility;
- Undermined confidence in the government;
- Financial losses and penalties;
- Breach in legal or compliance position;
- Loss of personal or private information.

The Risk Appetite can be used in the following ways:

- To indicate to Project Owners the extent to which they need to mitigate risks to information that are inherent in new systems
- To inform the Accreditor (Force Security Advisor) and Information Asset Owners (IAOs)when they are able to sign off a risk as being acceptable to the business or when they need to escalate a decision to the SIRO
- To guide risk owners in the types and levels of risk they can accept on behalf of the force

- To inform the SIRO of when he/she cannot accept risks on national systems or on systems that have a national impact.

7 Applying the Risk Appetite

7.1 Surrey Local Systems

New information systems are subject to an Accreditation process whereby risks to information are assessed and a decision made on how to mitigate and manage them is made. (Live systems are subject to an accreditation review on an annual basis.) Project Managers must provide a Risk Management and Accreditation Document Set (RMADS) to the Accreditor capturing information about the system, the risks and the mitigations, and the Accreditor then makes a judgement on whether the risks are sufficiently mitigated to go live. Residual risks of sufficient concern should then be the subject of assessment against the risk appetite.

Therefore the Risk Appetite is an expression of attitude or behaviour which must map to something useable by individuals within the risk management hierarchy; ie the maximum level of residual risk that can be accepted on behalf of the force at each level in the risk management chain.

The delegation matrix for local systems is shown below:

Residual Risk Level	Risk Appetite				
	Risk Averse	Minimalist	Cautious	Open	Hungry
Very Low	Accreditor	IAO	IAO	IAO	IAO
Low	SIRO	Accreditor	IAO	IAO	IAO
Medium	SIRO	SIRO	Accreditor	IAO	IAO
Medium-High	SIRO	SIRO	SIRO	Accreditor	IAO
High	SIRO	SIRO	SIRO	SIRO	Accreditor
Very High	SIRO	SIRO	SIRO	SIRO	SIRO

Table 7.1

For example, for an information system under the 'Open' appetite:

- The maximum level of risk acceptable at IAO level is Medium
- The maximum level of risk acceptable at Accreditor level is Medium-High
- High or Very High Risks require escalation to the SIRO.

7.2 Nationally Connected Systems

As the ACPO National Risk Appetite is Cautious (overall) any information systems which connect to the National Systems must also have an equal or more averse appetite. This will also apply to any Surrey Police local system which meets any of the following criteria:

- the system takes or holds copies of data from a national system
- the system produces or holds data which subsequently becomes national data
- the system receives data originating from national systems and/or other forces, including email.

The delegation matrix for national systems, or local systems that meet the above criteria, is shown below:

Residual Risk Level	Risk Appetite				
	Risk Averse	Minimalist	**Cautious**	Open	Hungry
Very Low	National SIRO	Surrey SIRO	**Surrey Accreditor**	Surrey Accreditor	Surrey Accreditor
Low	National SIRO	National SIRO	**Surrey SIRO**	Surrey Accreditor	Surrey Accreditor
Medium	National SIRO	National SIRO	**National SIRO**	Surrey SIRO	Surrey Accreditor
Medium-High	National SIRO	National SIRO	**National SIRO**	National SIRO	Surrey SIRO
High	National SIRO	National SIRO	**National SIRO**	National SIRO	National SIRO
Very High	National SIRO	National SIRO	**National SIRO**	National SIRO	National SIRO

Table 7.2

This means for an information system under the 'Cautious' appetite:

- The maximum level of risk acceptable at Accreditor level is Very Low
- The maximum level of risk acceptable at Surrey SIRO level is Low
- Risks above Low require escalation to the National SIRO.

8 Setting the Risk Tolerance

A Risk Tolerance may be set to adjust the Risk Appetite, representing a greater or lesser Appetite for information risks posed by a specific local system. *(NB: A risk tolerance may not be set for any national systems or local systems which connect to a national system or hold data that subsequently becomes national data.)* For example, the force may be more or less averse to certain categories of risk and in different contexts (e.g. political/operational drivers), so the Project Manager or System Owner may wish to request a Risk Tolerance.

In doing so the Project Manager or System Owner should ask the following questions and confirm the proposed Tolerance with the Accreditor:

- In the context of this system are we averse to certain types of threat sources, e.g. serious and organised crime? (It is worth consulting the National and Local Threat Assessment to understand the current threats to police, and their severity.)
- In the context of this system are we averse to certain types of incidents, e.g. interception by criminal groups?
- Are we less concerned about certain types of risks, e.g. unauthorised access by third party staff?
- Are there particular political or operational imperatives relating to the system?
- Have incidents in the past indicated a tendency for risks to this information to be exploited?
- If we are handling data owned by partners or third parties, what is their Appetite / Tolerance for information risk associated with this system? What rules do they have for handling that information?
- If we are passing data to partners or third parties, do we trust their handling of our sensitive data, and are we sensitive to any risks that they pose to the information?
- Are we more or less willing to pay to mitigate risk?
  - Because in the context of this system, the risks of disclosure, confidentiality, integrity of the information are NOT deemed to have serious impacts?
  - **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 influence the SIRO decision not to spend on the risk mitigation options proposed in a Risk Balance case.**
- Are the aspects explored above time-bound or permanent?

9 Applying the Risk Tolerance

The level of acceptable risk for new systems and processes are agreed in advance of a project and, if appropriate, a Risk Tolerance applied. It will not be permissible to allow informal or arbitrary decision making attributed to 'budgetary constraints' that are outside of this process.

This is to prevent systems and processes from being implemented without a calculated and acceptable level of residual risk, as defined in the Force Risk Appetite Statement.