

# WARWICKSHIRE POLICE AUTHORITY

## RISK MANAGEMENT FRAMEWORK

September 2008



**Warwickshire**  
POLICE AUTHORITY

*The authority behind the force*

**Introduction**

This document describes the framework within which risk management will be developed and monitored by the Authority and provides a step-by-step guide to the Authority’s risk management process. It should be read in conjunction with the Authority’s risk management policy statement.

There are four main stages to the risk management process:

**Identification** – the means by which threats and opportunities are identified and turned into manageable statements.

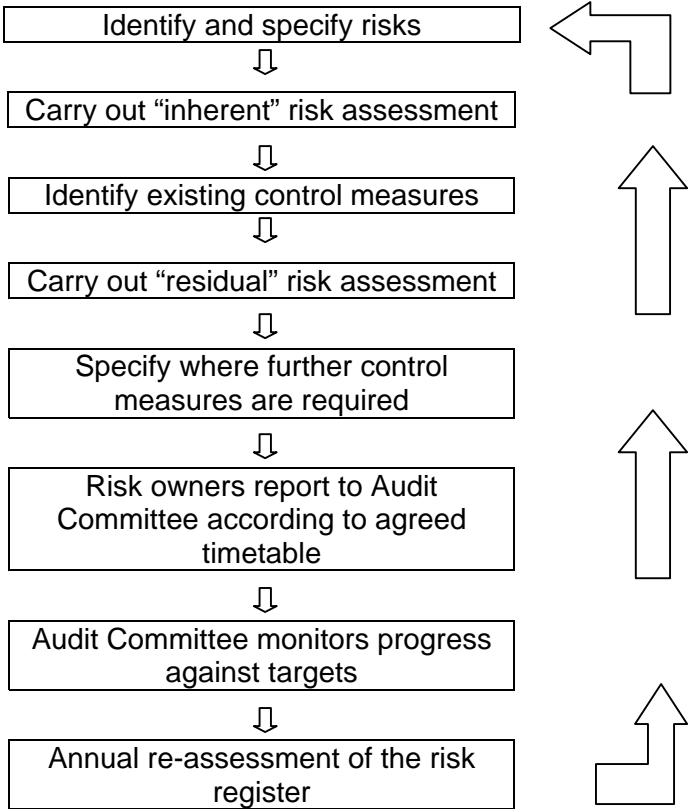
**Assessment** – estimating the levels of likelihood and impact of the risks and opportunities and assessing which pose the greatest threat.

**Management and Control** – developing and putting into place actions and control measures to treat or manage the risk.

**Review and reporting** – monitoring that the actions and control measures are appropriate, effective and still relevant, identifying changes in circumstances and environment and checking the effect on risk priorities, reporting on progress to the Authority.

This document deals in turn with these four stages, describing processes, responsibilities and timescales.

**Flowchart showing the risk management process:**



## Step 1 - Identification

This task can be separated into two distinct phases:

**Initial risk identification** – for organisations that have not previously identified risks in a structured way

**Continuous risk identification** – to identify new risks that did not previously arise, changes to existing risks and risks which have ceased to be relevant.

In either case, risks should be related to objectives. The Police Authority risk framework is organised into the three governance streams and lead responsibilities in order to allow for risks to be associated with the Authority's strategic objectives. However, care should be taken to identify generic risks which will impact on business objectives but may not be immediately apparent in thinking about a particular business area.

It helps to think about risks in two basic categories, strategic and operational. Strategic risks focus on identifying the key barriers to successful achievement of the organisation's objectives. Operational risks are more likely to focus on continuity of business services. Both strategic and operational risks can be driven by either external or internal factors, or a combination of the two. A statement of risk should encompass the cause of the impact, and the impact on the objective (e.g. missing a train makes me late for a meeting). Avoid stating risks that are simply the converse of the objectives.

### Tips on identifying and constructing risks

The following prompts should help to identify the areas of risk. Common areas are:

<b>Strategic</b>	Doing the wrong things as an organisation. Missing opportunities.
<b>Financial</b>	Losing resources or incurring liabilities.
<b>Reputation</b>	The Authority's image. Loss of public confidence.
<b>Political</b>	Political embarrassment. Not delivering on local or national policies.
<b>Partnerships</b>	Specific risks to the Authority as a result of being in a given partnership.
<b>Legal/regulatory</b>	Claims against the Authority. Non-compliance.
<b>Operational</b>	Service delivery failure, targets missed.
<b>Information</b>	Loss of, or inaccurate data, systems or reported information.
<b>Customer/citizens</b>	Understanding their needs, delivery of services.
<b>Environmental</b>	Things outside of our control. Environmental impact of the Authority.
<b>People</b>	Employees, management, Members, Senior Police Officers.

Not all parts of the organisation will have risks under all these categories.

Expressing risks as a statement can be harder than it first seems. Try to include the following three parts in a risk statement: CAUSE – UNCERTAINTY – EFFECT .

Typical phrasing could be:

Loss of.....	leads to.....	resulting in.....
Failure of.....		
Lack of.....		
Partnership with.....		
Development of.....		

## Step 2 – Assessment

There are three important principles for assessing risk:

- Ensure that there is a clearly structured process for which both likelihood and impact are considered.
- Record the assessment of risk in a way that facilitates monitoring and the identification of priorities.
- Be clear about the difference between inherent and residual risk.

Some types of risk lend themselves to objective diagnosis, e.g. financial risks, while others, e.g. risk to reputation, may be more subjective. Our framework allows for assessing all types of risk together. The assessment should draw on unbiased independent evidence where possible and should consider the perspectives of the whole range of stakeholders likely to be affected.

The assessment needs to be done by evaluating both the likelihood of the risk being realised and the impact if the risk is realised. As a minimum, simple high/medium/low categories could be used but these are generally found not to be sufficiently sensitive when the management of the risk is discussed. Many organisations similar to our own are using five point scales broadly as follows:

### Likelihood

Scale/ Level	Descriptor	Description	Probability in any given year
1	Rare	May only occur in exceptional circumstances. Less than once in 30 years.	Less than 3%
2	Unlikely	Could occur at some time. Likely to be once in every 10-30 years.	3 to 10%
3	Possible	Fairly likely to occur at some time or in some circumstances. Likely to be once in every 3-10 years.	10+ to 33%
4	Likely	Will probably occur at some time or in most circumstances. Likely to be once in every 1-3 years.	33+ to 99%
5	Almost certain	Is expected to occur in most circumstances. Likely to be every year or several times a year.	99+%

## Impact

Scale/ Level	Descriptor	Description			
		Financial	Regulatory/Compliance	Service	Reputation
1	Insignificant	<1% of budget	HMIC or government note non-compliance but no further action.	No significant disruption to service.	No impact outside of the organisation.
2	Minor	1 to 2% of budget	Some corrective action required.	Some disruption to service.	Negative local publicity. Minimal long-term damage to reputation.
3	Moderate	2+ to 3% of budget	Major corrective action required. Possibility of legal action.	Noticeable disruption to service. Some damage to the organisation's ability to function.	Extensive negative local publicity. Limited national coverage. Medium-term damage to reputation and public confidence.
4	Major	3+ to 4% of budget	Major corrective action required. Possibility of sanctions and/or legal action.	Major disruption to service. Serious damage to the organisation's ability to function	Significant local and national media coverage. Long-term and significant local damage to reputation and public confidence. Some damage to national reputation.
5	Catastrophic	>4% of budget	Major and immediate corrective action required. Sanctions and/or legal action probable.	Breakdown or major, long-term disruption of service. Significant damage to the organisation requiring resignations and major systemic change.	Very significant, long-term damage to reputation and public confidence at local and national levels.

The first assessment of risk levels against these criteria should take no account of any measures or factors that may be in place or planned to moderate the risk. This establishes the level of the “Inherent Risk”. In Step 3 of this framework guide, we shall discuss how these moderating measures are taken into account to establish a “Residual Risk”.

**Risk Matrix**

Having used the tables above to score the inherent risk (i.e. the risk before any corrective action is applied) The next step is to plot the inherent risks on a matrix as shown below.

		<b>LIKELIHOOD</b>				
		<b>Rare</b>	<b>Unlikely</b>	<b>Possible</b>	<b>Likely</b>	<b>Almost certain</b>
<b>I M P A C T</b>	<b>Catastrophic</b>	5	10	15	20	25
	<b>Major</b>	4	8	12	16	20
	<b>Moderate</b>	3	6	9	12	15
	<b>Minor</b>	2	4	6	8	10
	<b>Insignificant</b>	1	2	3	4	5

We will add more detail to this matrix in the next stage of our process.

**Process for assessing risk**

A workshop comprising Stream Leads and Audit Committee Members will review risks for the Authority and carry out an inherent risk assessment in early summer each year.

## Step 3 – Management and Control

Stages in this section include:

- Assessing the residual risk
- The risk prioritisation matrix
- Addressing risks

### Residual Risk

Having carried out the inherent risk assessment, the next task is to establish what control measures exist. These could include, policies, protocols, regular meetings or any other activity that has the effect of moderating the identified risk. Once the control measures are identified and validated, a second risk assessment should be performed, again using the Likelihood and Impact criteria in Step 2 but this time taking account of the known control measures. The result of this second assessment is the “Residual Risk”.

### Risk Prioritisation Matrix

The table below shows the matrix discussed in the previous section with colour coding to indicate levels of prioritisation. This should be read in conjunction with the key below.

		LIKELIHOOD				
		Rare	Unlikely	Possible	Likely	Almost certain
I M P A C T	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Insignificant	1	2	3	4	5

### Key to Prioritisation Matrix

Level of risk (inherent risk score)	Indicated by	How risk should be managed
Very high risk (16-25)	Red	Requires active management. <i>High impact/high likelihood: risk requires active management to manage down and maintain exposure at an acceptable level.</i>
High risk (10-15)	Orange	Contingency Plans <i>A robust contingency plan may suffice together with early warning mechanisms to detect any deviation from profile.</i>
Medium risk (5-9)	Yellow	Good housekeeping <i>May require some risk mitigation to reduce likelihood if this can be done cost effectively, but good housekeeping to ensure the impact remains low should be adequate. Reassess frequently to ensure conditions remain the same.</i>
Low risk (1-4)	Green	Review periodically <i>Risks are unlikely to require mitigating actions but status should be reviewed frequently to ensure conditions have not changed.</i>

## Addressing risks

We now need to consider what action is needed to manage the residual risks.

The main options for addressing residual risk are:

**Tolerate.** Is the exposure tolerable without any further action being taken? Even if it is not tolerable, ability to do anything about some risks may be limited or the cost may be disproportionate to the potential benefit gained. This option may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

**Treat.** By far the greater number of risks will be addressed in this way. While continuing the activity that gives rise to the risk, action is taken to constrain the risk to an acceptable level (see below).

**Transfer.** For some risks, the best response may be to transfer them. This might be done by insurance or by paying a third party to take the risk in another way. This may be considered appropriate because it reduces the risk to the organisation or because another organisation is more capable of managing the risk.

**Terminate.** Some risks will only be treatable or containable to acceptable levels by terminating the activity. This is generally accepted to be a limited opportunity in the public sector because activity may well be driven by legislative requirements.

**Taking the opportunity.** This is not really an alternative to the options above; rather it is an option that should be considered whenever tolerating, treating or transferring a risk. There are two main aspects to this. The first is whether or not at the same time as mitigating threats, an opportunity arises to exploit positive impact. For example, if a large sum of money is to be put at risk in a major project, are the control measures judged to be good enough to justify increasing the sum of money at stake to gain even greater advantages. The second is whether or not circumstances arise which, while not generating threats, offer positive opportunities. For example, a fall in the cost of goods or services frees up resources which can be re-deployed. Being risk aware is not the same as being risk averse.

## Treating the risk

Where the decision is to Treat the risk, further actions need to be defined.

It is important that any additional action is proportional to the risk. Apart from the most extreme undesirable outcome, it is normally sufficient to design controls to give a reasonable assurance of confining any loss to a level that is acceptable to the organisation. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk it is controlling.

## Process for Addressing risk

A risk workshop with Stream Leads and Members of the Audit Committee will carry out the initial assessment and will take an early view on control measures.

Officers will compile a draft list of control measures which a second Workshop will review before carrying out the residual risk assessment.

The residual risk assessment will be carried out in late summer or early autumn and reported to the Police Authority.

## Step 4 - Review and Reporting

It is important that the management of risk is reviewed and reported on for two reasons:

- To monitor whether or not the risk profile is changing
- To gain assurance that risk management is effective and to identify when further action is necessary.

Audit Committee will be the responsible body for ensuring that the Police Authority risk register is compiled and kept under review. The Committee will commission work as necessary from Stream Leaders and risk owners to ensure that control measures are in place appropriate to the severity of the risk.

### Monitoring and Review

Risks should be monitored according to the following criteria:

Level of residual risk		Action
Very high risk (16-25)		Stream Leads to keep under constant review. Quarterly monitoring report to Audit Committee.
High risk (10-15)		Stream Leads to review quarterly. Six-monthly monitoring report to Audit Committee.
Medium risk (5-9)		Stream Leads to review six-monthly. Annual report to Audit Committee.
Low risk (1-4)		Stream Leads to review annually.

### Cycle for Monitoring and Reporting

The Audit Committee will receive reports in accordance with the table above and will present regular update reports to the Police Authority as follows:

Audit Committee Meeting	Action	Police Authority Meeting	Action
September	Receive annual reports on all risks. Workshop to complete annual review of risks.	September/October	Report on annual review of risk register and presentation of register for the coming year.
December	Receive 1 <sup>st</sup> quarterly reports	December/January	Report on any urgent issues.
April	Receive 2 <sup>nd</sup> quarterly and six-monthly reports.	April/May	Half-year update report.
June	Receive 3 <sup>rd</sup> quarterly reports. Workshop to begin annual review of risk.	June/July	Report on any urgent issues.

Tony Brown  
September 2008