



Hampshire Police Authority Risk Management Policy & Strategy

1) Scope

- 1.1. Risk management is the process of identifying risks or opportunities, evaluating their potential consequences, considering the current controls in place, and determining and implementing the most effective way of monitoring and mitigating them.
- 1.2. Risk Management is one of the pillars of corporate governance. Good governance relies on risk management being embedded into the culture of the organisation, with Members and officers recognising that risk management is a shared responsibility.
- 1.3. The Police Authority's duties for risk management are twofold. Firstly, the Hampshire Police Authority has a responsibility for putting in place arrangements to manage risks it faces, separate from those of the Force, and secondly for ensuring that the Constabulary itself has adequate arrangements for risk management in place.
- 1.4. This document, therefore, sets out the Risk Management Policy of Hampshire Police Authority. It refers to the management of risk within the Police Authority office and its immediate operating environment and the way in which the Police Authority will monitor the management of risk in the Constabulary.

2) Policy Statement

- 2.1. The Authority will seek to identify, analyse and prioritise the risks it faces. It will seek to manage and control risks in order to maximise the quality and efficiency of its service provision and to uphold its reputation.
- 2.2. The Authority recognises that risk management is as much about exploiting opportunities as it is managing threats.
- 2.3. A certain amount of risk taking is both inevitable and essential if the Authority is to achieve its objectives. The Authority recognises that the way that it manages the many risks facing it contributes towards the successful achievement of its objectives.
- 2.4. A systematic and consistent approach to identifying and analysing risks will be an integral part of all key management and governance processes, rather

than a separate initiative, and will be implemented using the simplest possible means.

3) Introduction

- 3.1. Effective management of risk will assist in the achievement of the Authority's vision and strategic objectives, optimise the quality and efficiency of its service delivery, and uphold and enhance its reputation.
- 3.2. Risk management must be clearly aligned to the organisation's strategic objectives, ensuring that there is a strong focus, at the top of the organisation, on those most significant risks that would prevent the Authority achieving its vision and strategic objectives; or would impact on its partners.
- 3.3. Hampshire Police Authority's commitment to risk management is a key part of its Code of Corporate Governance.

4) Risk Management Objectives

- 4.1. Increase the likelihood of achieving the Police Authority's vision and strategic objectives.
- 4.2. Prevent or reduce the potential consequences of events which could have been reasonably foreseen.
- 4.3. Prevent or reduce events or actions that could damage the reputation and public confidence of the Police Authority.
- 4.4. Improve decision making and planning; assist in the allocation of resources.
- 4.5. Integrate risk management into the culture of the Police Authority and its processes.
- 4.6. Raise awareness of risk management in all Members and staff, making it an integral part of their thinking and actions.
- 4.7. Satisfy the requirements of corporate governance for the Annual Governance Statement, and the internal and external auditors in relation to the effectiveness and adequacy of risk management.

5) Principles

- 5.1. Activity will be aligned to the vision and strategic objectives of the Authority.
- 5.2. It will:
 - a) Encompass all strategic and functional risks that may prevent the Authority from fulfilling its objectives.
 - b) Anticipate and manage risks rather than deal with the consequences.

- c) Avoid creating a risk adverse culture by taking an approach which considers the risks of not undertaking activities and not exploiting opportunities.
- 5.3. Mitigation measures should be effective, appropriate, proportional, affordable and flexible. Controls are not to be set up where the cost and effort is disproportionate to the expected benefits.
- 5.4. Procedures and controls are to be implemented with minimum bureaucracy.
- 5.5. Risk should to be managed rather than avoided and consideration of risk should not stifle innovation. Risk management will therefore be used to promote innovation as well as to help secure existing objectives.
- 5.6. The Authority will consider risk when reaching decisions on new and innovative projects and will take a proportionate response to managing risk.

6) Risk Process

- 6.1. Risks are identified by Members of the Authority, Chief Executive, Authority Officers or report writers as part of day to day business. The description is drafted by the Chief Executive's office in consultation with the risk owner who will then score the risk accordingly. The risk is then presented for approval at the next Governance meeting.
- 6.2. The Chief Executive will oversee all amendments to the risk register prior to presentation to the quarterly Governance meeting.
- 6.3. Risk owners will consider the following:
 - a) Tolerating the risk.
 - b) Treating the risk.
 - c) Transferring the risk.
 - d) Terminating the risk.
 - e) Alternatively a risk, after evaluation, may present the organisation with an opportunity to deliver savings or efficiencies.
- 6.4. A clear methodology is used to evaluate risks in a consistent way (a copy of this methodology is appended to this Strategy). Once a risk has been identified, evaluated and scored it will be entered on the Risk Register in red text until approved by the next meeting of the Governance Committee.
- 6.5. The entry will include:
 - a) The risk, clearly defining its cause, effect and consequence
 - b) The strategic objective to which it poses the greatest risk
 - c) The overall risk value
 - d) The control measures attributable to the risk
 - e) An owner responsible for managing the risk
- 6.6. Entries mitigated or risks that are no longer considered a risk will be archived once agreed by the Governance Committee.

7) Risk Appetite Statement

- 7.1. The Authority recognises that the levels of risk that it may be prepared to take are dependent on:
 - a) The nature of the risk concerned
 - b) Its capacity to control a particular risk
 - c) Its prior exposure to risk and the amount of risk it is currently controlling.
- 7.2. The Authority will consider the above factors in its decision making processes to ensure that it balances the risks it takes.
- 7.3. It has determined a scoring mechanism for the risks contained within its risk register by which the levels of control and intervention are proportionate to the level of risk, i.e. it will concentrate mitigation actions on higher risks.
- 7.4. There are some activities of the Authority where it may accept higher risk, for example to support innovation. However, it has a low risk appetite where matters of public confidence are concerned.

8) Statement of Responsibilities

8.1. AUTHORITY

- a) Approving a statement of the Authority's Risk Management Strategy and subsequent revisions, on the recommendation of the Governance Committee.
- b) Receiving an annual report in February on risk management activity from the Governance Committee.

8.2. CHIEF EXECUTIVE

- a) Overseeing the corporate approach to risk management.
- b) Maintaining the Authority's Risk Register.
- c) Additions/deletions/amendments to risks, in consultation with the Risk Owner;
- d) Implementing Committee requests to include new risks in consultation with the Risk Owner;
- e) Ensuring that all service deliverers (including volunteers, contractors and other partners) are made aware of their responsibility for risk management and the mechanisms for feeding concerns into the Authority's formal management processes, through inclusion in contract documents, service level agreements etc.
- f) Nominating appropriate Authority staff for risk management training, as identified through the performance review process.
- g) Ensuring that all reports emanating from the Authority office, policy decisions and operational changes include, where appropriate, an adequate assessment of risks and how they will be managed.

8.3. CHIEF CONSTABLE

- a) Maintaining the Risk Register in relation to the Constabulary, including as a result of decisions made by the Authority or its Committees.
- b) Ensuring compliance with Constabulary risk management standards.

- c) Ensuring that all reports emanating from the Constabulary, policy decisions and operational changes include, where appropriate, an adequate assessment of risks and how they will be managed.
- d) Reporting on a quarterly basis the key risks facing the Constabulary to the Governance Committee.

8.4. **GOVERNANCE COMMITTEE**

- a) Considering arrangements for the identification, assessment and management of risk.
- b) Receiving progress reports from the Chief Executive.
- c) Receiving reports from the Chief Constable on the key risks facing the Constabulary on a quarterly basis.
- d) Through reports received (a) to (c), preparing an annual report on risk management to the Authority.
- e) Reviewing the Annual Governance Statement.

8.5. **REPORT WRITERS**

- a) Decisions by the Authority and its Committees need to be taken in the full knowledge of all relevant risks. Accordingly, all reports must include an assessment of the risks associated with the content of the report and how they are to be managed or mitigated, which register the risk is on, the reference number, the risk owner, the current status of the risk and whether mitigations are sufficient. If there are no risks then this should be clearly stated. In the production of the report the originator should examine the Authority's Risk Register in order to establish whether there will be any impact upon the entries contained within the Register as a result of the report content. If any changes are foreseen, the report should contain sufficient information to enable the Register to be updated. The proposed additions or changes to the risk register should be specified.
- b) Reports should, where appropriate, give Members options, and clearly explain the costs and effects on risks of the different options.

8.6. **COMMITTEES**

- a) When receiving and considering reports, Committees should include assessment of risks, options and costs as part of their decision making.
- b) When deciding upon items to be included in the risk register, the Committee must provide sufficient detail to enable the register to be updated i.e. the completion or amendment of the risk type, risk, likelihood, impact, risk classification, risk owner.
- c) Every six months, Committees should review those items in the risk register that are within their responsibility and agree any amendments as necessary.

8.7. **RISK OWNERS**

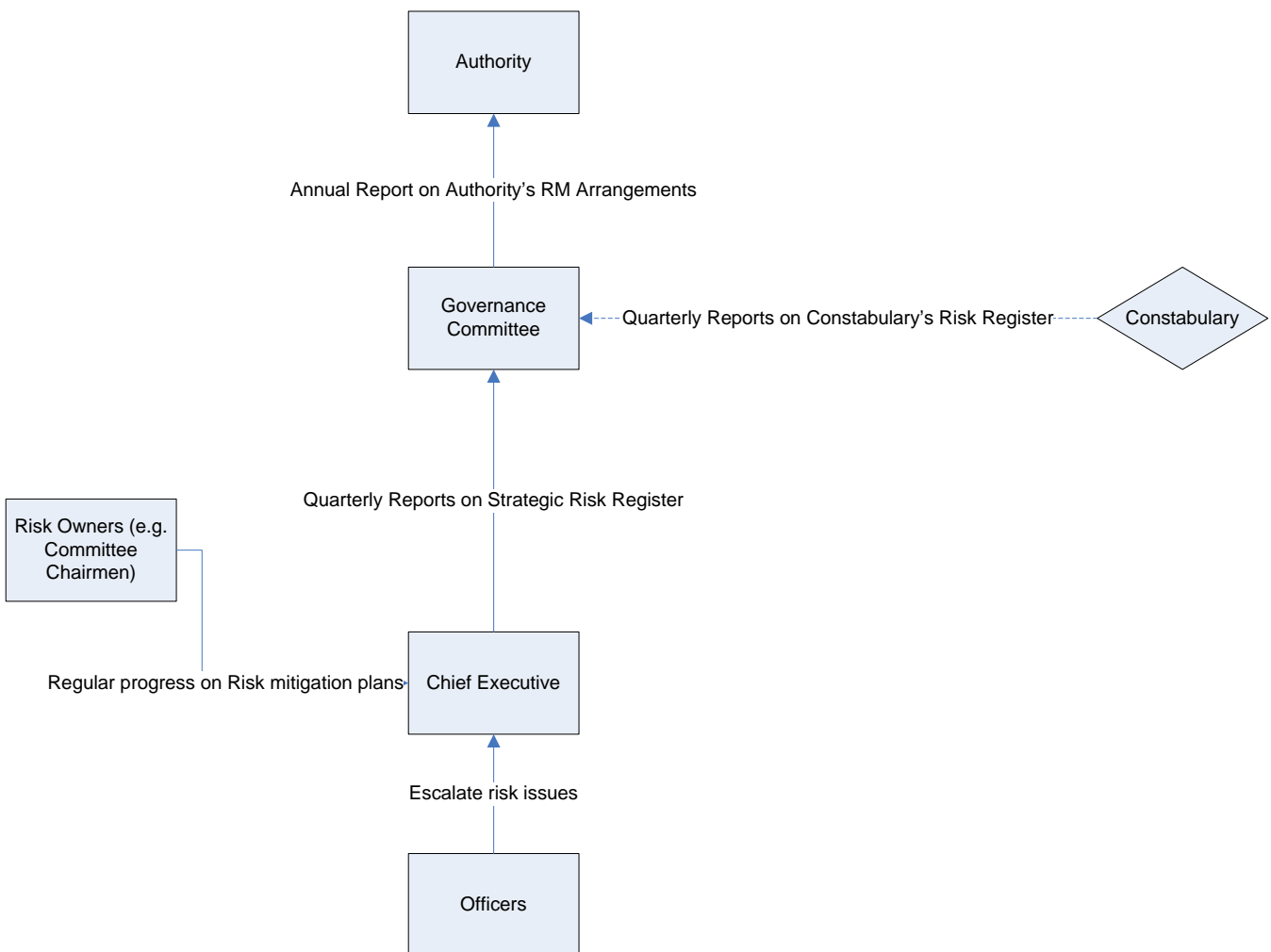
- a) Receiving updates of entries in the risk register from the Chief Executive and taking ownership of the risk
- b) Re-scoring the risk/s they are responsible for on a quarterly basis.
- c) Enter on the risk tracking summary sheet the predicted status of their risk

8.8. **ALL EMPLOYEES**

- a) Maintaining an awareness of risk and feeding this into the formal management and reporting processes.
- b) supporting and participating in risk management activities

9) **Reporting Framework**

- a) The diagram below summarises the key reporting arrangements with respect to risk management.



LEGISLATIVE AND RISK CONSIDERATIONS

Human Rights Act 1998

This policy has been drafted with the Human Rights Act 1998 taken into consideration.

Race Relations Amendment Act and Disability Discrimination Act

This policy has been drafted with the Diversity Policy and the Race Equality Scheme taken into consideration.

Freedom of Information Act

This Policy is suitable for publication under the Freedom of Information Act.

Health and Safety

This policy has been drafted with the Health and Safety legislation and guidance taken into consideration.

Anti Corruption

This Policy has been drafted with risk to integrity and unethical conduct taken into consideration.

FREEDOM OF INFORMATION ACT

This policy is not Protectively Marked however, the Police Authority's Strategic Risk Register and Hampshire Constabulary's Strategic Risk Register will not be disclosed under the Freedom of Information Act, and all papers relating to the management of risks will be classed as '**Restricted**'.

REVIEW

The Risk Management Policy and Strategy will be subject to an annual review by the Governance Committee (in March) to ensure its continued relevance as risk management develops and becomes more embedded in the Authority.

Appendix to Strategy - Hampshire Police Authority Guidance on Completing the Strategic Risk Register

Instructions for use

- 1 Define the risk(s) explicitly in terms of the adverse impacts(s) that might arise from the risk.
- 2 Use table 1 to determine the impacts score(s) (I) for the potential adverse outcome(s) relevant to the risk being evaluated. Impact can be assessed in terms of its effect on **Cost**, **Time** and **Quality**. Choose the most appropriate domain for the identified risk from the left hand side of the table. Then work along the columns in same row to assess the severity of the risk on the scale of 1 to 5 to determine the impact score, which is the number given at the top of the column. There may be more than one impact, choose the most appropriate i.e. the one with the highest level.
- 3 Use table 2 to determine the likelihood score(s) (L) for those adverse outcomes. If possible, score the likelihood by assigning a predicted frequency of occurrence of the adverse outcome. If this is not possible, assign a probability to the adverse outcome occurring within a given time frame, such as the lifetime of a project. If it is not possible to determine a numerical probability then use the probability descriptions to determine the most appropriate score.
- 4 Calculate the risk score the risk multiplying the impact by the likelihood: $I \text{ (impact)} \times L \text{ (likelihood)} = R \text{ (risk score)}$.

Risk matrix - Table 1 Impact scores

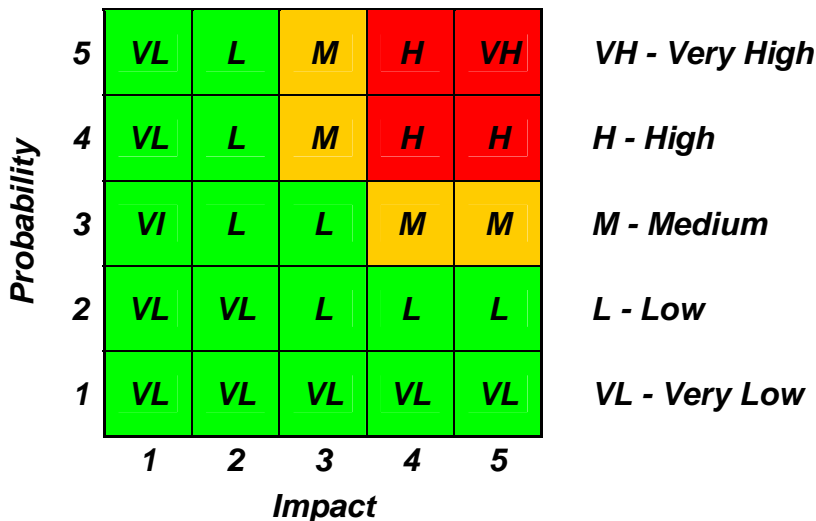
		Impact score (severity levels) and examples of descriptors				
		1	2	3	4	5
Domains		Negligible	Minor	Moderate	Major	Catastrophic
Cost		Small loss / Insignificant cost increase Affects service budget by less than £25,000 Variations manageable by virement against internal budget headings	<5 per cent over project budget Affects service budget by between £25,001 & £100,000 Requires some additional funding from the partner organisation	5–10 per cent over project budget Affects service budget between £100,001 & £400,000 Requires significant additional funding from one of the partners	10–25 per cent over project budget Affects service budget between £400,001 & £800,000 Requires significant reallocation of funds from one or more partner organizations to meet objectives	>25 per cent over project budget Affects service budget by more than £800,000 Increases threaten the viability of the partnership
Time		Slight Slippage against internal targets	Slight slippage against key milestones or published targets	Delay affects key stakeholders & causes loss of confidence in the enterprise	Failure to meet deadlines in relation to priority outcomes	Delay jeopardizes viability of the enterprise or partnership
Quality	Business objectives/ projects	Barely noticeable reduction in scope or quality	Minor reduction in quality/scope	Reduction in scope or quality	Failure to meet secondary objectives	Failure to meet primary objectives
	Service/ business interruption	Little or no impact on service delivery	Minimal service disruption having limited impact on service delivery	Moderate service disruption having adverse impact on service delivery	Major service disruption having serious impact on service users	Major service disruption having serious impact on the public Permanent loss of service or facility
	Statutory duty/ inspections	No or minimal impact or breach of guidance/ statutory duty	Breach of statutory legislation Reduced performance rating if unresolved	Single breach in statutory duty Challenging external recommendations / improvement notice	Multiple breaches in statutory duty Critical report /Improvement notices / Enforcement action Low performance rating	Multiple breaches in statutory duty Prosecution Complete systems change required Severely critical report
	Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. Total loss of public confidence
	Sustainability / Environmental impact	Minimal or no impact on the environment or sustainability targets	Minor impact on environment or sustainability targets	Moderate impact on environment or sustainability targets	Major impact on environment or sustainability targets	Catastrophic impact on environment or sustainability targets

Table 2 Likelihood score (L)

What is the likelihood of the risk occurring?

The frequency-based score is appropriate in most circumstances and is easier to identify. It should be used whenever it is possible to identify a frequency.

Likelihood score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost certain
Frequency How often might it/does it happen	This will probably never happen/recur (0 to 5% chance of occurrence)	Do not expect it to happen/recur but it is possible it may do so (6 to 20% chance of occurrence)	Might happen or recur occasionally (21 to 50% chance of occurrence)	Will probably happen/recur but it is not a persisting issue (51 to 80% chance of occurrence)	Will undoubtedly happen/recur, possibly frequently (81 to 100% chance of occurrence)



Score	Risk Level	Recommended Response
16 – 25	High Threat	Immediate action or detailed planning to be included within implementation plans
11-15	Medium Threat	Measures to be included into action plans and monitored
1-10	Low Threat	Limited action and review will be undertaken

Very High = 21 - 25
 High = 16 – 20
 Medium = 11 – 15
 Low = 6 – 10
 Very Low = 1- 6