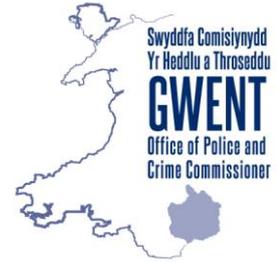


**NOT PROTECTIVELY MARKED**



Heddlu  
Gwent  
Police



**GWENT POLICE  
AND  
OFFICE OF THE POLICE AND CRIME  
COMMISSIONER**

**JOINT STRATEGIC RISK MANAGEMENT  
FRAMEWORK 2020**

Last Updated: May 2020  
Date of Next Review: May 2021

**NOT PROTECTIVELY MARKED**

## **1.0 Introduction**

- 1.1 Risk Management is a decision making tool that enables an organisation to identify and manage its risks. It enhances strategic planning and prioritisation and assists in achieving objectives while strengthening the ability to respond to challenges faced. It is therefore integral to any organisation's strategic management and is a fundamental element of good corporate governance.
- 1.2 This Joint Gwent Police (GP) and the Office of the Police and Crime Commissioner (OPCC) Strategic Risk Management Framework aims to ensure both a consistent and robust identification of risk faced by the Organisation, and the effective and transparent management of that risk. It further aims to ensure that risk management is integrated into the Organisation's culture, decision making processes, leadership, management and day to day working across all levels of the organisation.
- 1.3 The framework supports the Risk Management Principles as set out in the [Government's Orange Book 2020](#) as follows:
1. Risk management shall be an essential part of governance and leadership, and fundamental to how the Organisation is directed, managed and controlled at all levels.
  2. Risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.
  3. Risk management shall be collaborative and informed by the best available information and expertise.
  4. Risk management processes are structured to include:
    - a. Risk identification and assessment to determine and prioritise how the risks should be managed;
    - b. The selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
    - c. The design and operation of integrated, insightful and informative risk monitoring;
    - d. Timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.
  5. Risk management shall be continually improved through learning and experience.

1.4 Gwent Police and the OPCC are two corporations sole. However, the OPCC and Gwent Police have adopted a joint strategic management approach to managing strategic risk. It should be noted therefore, that where reference is made to 'the Organisation', for the purposes of this document the term refers to both the OPCC and Gwent Police jointly.

## **2.0 Declaration**

2.1 This Framework has been drafted in accordance with, and in consideration of, the principles of relevant legislation and documentation, including:

- BS ISO 31000:2018E – Risk Management Guidelines (Global Risk Management Standard)
- HM Government 'The Orange Book' Management of Risk Principles and Concepts 2020
- The Accounts and Audit Regulations 2018
- Health and Safety Act 1974
- Management of Health and Safety at Work Regulations 1999.
- National Decision Model
- College of Policing Code of Ethics
- College of Policing Ten Principles of Risk

## **3.0 Aim**

3.1 This Strategic Risk Framework sets out the OPCC's and Gwent Police's joint approach to strategic risk management and outlines the supporting governance framework.

3.2 Strategic risks are those risks that will impact on the Organisation as a whole. They therefore require higher levels of management action and monitoring due to their potential impact. This Framework will be underpinned by a Joint Risk Management Policy and the Joint Strategic Risk Register (Risk Register) which holds the details of the contingencies put into place to manage each risk.

## **4.0 Objective**

4.1 The objective of the Organisation in relation to strategic risk management is to:

- Continuously integrate strategic risk management into the culture of the Organisation and existing processes
- Prevent or minimise the potential consequences of events which could have been reasonably foreseen
- Improve decision making, planning and the allocation of resources
- Anticipate and respond to changing political, economic, sociological, technical, environmental, legal and organisational requirements
- Align risk management to the OPCC and Gwent Police's strategic purpose and objectives

## NOT PROTECTIVELY MARKED

- Maximise the opportunity to achieve objectives and underpin corporate governance
- Preserve and enhance effective service delivery
- Protect its staff, public and communities.
- Continually review and improve risk management processes within the Organisation

4.2 Risk management also aims to support the priority areas of strategic focus for the OPCC and force:

- Crime Prevention
- Supporting Victims
- Community Cohesion
- Tackling Anti-Social Behaviour
- Effective Service Delivery

These areas of strategic focus are interdependent and support the Organisation's plans to keep people safe from harm.

4.3 Risk Management supports these areas of focus by:

- Establishing clear roles, responsibilities and reporting lines for risk management
- Identifying and assessing on an on-going and timely basis the risks to which the Organisation is exposed
- Considered decision making, planning and prioritisation using unified procedures
- Maintaining a Joint Strategic Risk Register aligned to the OPCC and Force's purpose and objectives
- Encouraging all staff to develop and maintain a risk management ethic and to report concerns accordingly.
- Ensuring that risk management is integrated into the Organisation's core management processes

## 5.0 Definition of Risk Management

5.1 The management of risk can be defined as:

"The combination of the probability of an event and its consequences (ISO/IEC Guide 73). *Institute of Risk Management – Risk Management Standard 2002*

- Strategic Risks are those that may affect the achievement of the organisation's strategy and objectives.
- Operational risks are those that affect an organisation's ability to execute its strategic objectives

The task of risk management is to manage exposure to risk, which is the probability of specific risks occurring and the potential impact if they did occur. However, risk management is also a tool for exploiting opportunities as well

## NOT PROTECTIVELY MARKED

as being a safeguard. Best practice in Risk Management recognises that a certain amount of risk taking may be desirable in order to maximise opportunities but negative threats can potentially have a disastrous impact on delivery objectives.

## **6.0 Organisational Approach**

6.1 Risk management should be an integral part of all organisational activities to support decision-making in achieving objectives (Principle 2). It should be an embedded part of, and not separate from:

- Setting strategy and plans
- Projects and delivering programmes
- Prioritising resources
- Supporting efficient and effective operations
- Managing performance
- Managing assets
- Delivering improved outcomes.

6.2 There will be a two-tiered approach to managing risk within the Organisation. Firstly, the departmental/local level where risks relate to day-to-day, operational activities specific to that area. Where necessary, local area risks should be escalated by managers to strategic risk level by using the risk process set out within this Risk Framework. Secondly, the strategic level, which involves management of high level, corporate risks that could impact the OPCC and Force as a whole and upon the achievement of the objectives of the Organisation<sup>1</sup>.

6.2 The OPCC may maintain its own risk register, holding those risks specific to the business of the OPCC only. Where necessary risks will be escalated to the strategic level and monitored through the relevant Governance Board.

6.3 Strategic risks are submitted and monitored within service area Governance Board meetings within the Organisation's Governance Framework. This ensures that risk management is an essential part of governance and leadership and underpins how the Organisation is directed, managed and controlled at all levels (Principle 1). Meetings take place on a monthly basis and are chaired by the service area Lead. Oversight of decisions made at these meetings is held within the Deputy Chief Constable's Scrutiny and Executive Board (SEB) attended by Heads of Service Areas, representatives from the OPCC, and staff associations.

6.3 It is the role of the Service Area Boards, SEB and the OPCC to:

- identify new and emerging risks
- assesses risks for potential impact and probability
- place responsibility for managing risks to those best able to control them
- ensure balanced and informed assessments of risks are provided

---

<sup>1</sup> Refers to both force and PCC objectives and priorities.

- review and direct the management of principal risks including taking cost-effective action to reduce risk to a tolerable level, acting proportionately and consistently
- ensure that risk management is anticipating, detecting, and responding to changes and events in an appropriate and timely manner
- put into place mechanisms to absorb and control any consequences arising from a risk
- act as the driver for implementing strategic changes in risk management;
- integrate the management of risk with the business of the Organisation and;
- ensure ethical process and transparency.

## 7.0 The Risk Process (Principle 4)

7.1 In order to successfully manage risks, the Organisation follows the five effective stages of the Risk Management Cycle which are based upon the National Decision Model. These should be considered when assessing a risk:



The risk management process that is followed is set out in Appendix 2.

## 7.2 Risk Identification / Assessment

7.3 In order to manage risk, the Organisation needs to know what risks it faces, and to evaluate them accordingly. Risk identification and assessment is an essential process as it defines what we are to manage, measure and monitor. Any subsequent action plans to mitigate a risk will be flawed and ineffective if the risk is not correctly identified.

- 7.4 Risk identification may arise from operational policing, the OPCC, the Force Corporate Governance framework, internal and external audit and inspection activity, partnership and collaborative projects and service delivery. All staff members within the Organisation have the responsibility to identify and raise risks.
- 7.5 When a risk is identified for the strategic register a full risk assessment<sup>2</sup> should be undertaken and returned to the Force Risk Manager for onward submission to the relevant Governance board. There are two stages when assessing a risk – the initial phase that gives Risk Owners the *inherent risk score* (the current risk level given the existing set of controls) and the post evaluation phase that achieves the *residual* risk score, (the level of risk remaining after additional controls are applied). In completing the risk assessment, evaluation should be collaborative and informed by the best available information and expertise (Principle 3). This may mean that full assessment is gained by informed internal and/or cross-organisational information from a range of public, private or third-sector partners and advisors.
- 7.6 The Risk Assessment Form requires two main functions. 1. An outline of the risk, current and planned mitigation and 2. a risk score to be provided, achieved by multiplying the perceived likelihood with the perceived impact. To assist with scoring a Risk Matrix is provided within the blank Risk Assessment Form. The Matrix outlines numbered levels of risk that can be used as a guide to obtain a final risk score. Staff completing the Risk Assessment Form should carefully consider the criteria outlined in the Risk Matrix to enable a true assessment of the risk's impact and probability.
- 7.7 As the risk matrix criteria sets out, careful consideration should be given to impact upon:
- Risk to life, health and safety
  - Financial impact, resources and assets
  - Code of Ethics
  - Service Delivery
  - Reputation and public confidence
  - Information Security
  - Business continuity and service disruption
  - Breaches of compliance, law and regulation
  - Privacy Impact
  - Staff, public and community
  - Collaboration / partnership opportunities
- 7.8 All risk assessment is affected to some degree by impression and subjectivity but the Risk Assessment Matrix sets out a number rating system of 1 – 4 (1 = Low, 4 = Critical) to assist the measurement of risk level and threat (as outlined on the Strategic Risk Assessment form shown in Appendix 1).

---

<sup>2</sup> The Strategic Risk Assessment Form is available from the Force Risk Manager

**NOT PROTECTIVELY MARKED**

7.9 The score attained from any of the columns in the Impact table should be multiplied by the Probability to give an initial risk score:

<b>Impact</b>	Critical	4	8	12	16
	High	3	6	9	12
	Medium	2	4	6	8
	Low	1	2	3	4
		Unlikely	Possible	Likely	Almost Certain/ Certain
<b>Probability</b>					

Overall Risk Score = Impact Score x Probability Score

<b>Risk Level</b>			
Low: 1, 2, 3	Medium: 4, 6, 8	High: 9, 12	Critical: 16

7.10 Risk appetite – Risk evaluation should involve evaluating the risk through the matrix and comparing the nature and extent of the risks with the risk appetite which is defined as “The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time” (HM Treasury).

- 7.11 Options may involve one or more of the following:
- Avoiding the risk by deciding not to start or continue the activity that gives rise to the risk;
  - Taking or increasing the risk in order to pursue an opportunity;
  - Retain the risk by informed decision;
  - Changing the likelihood where possible;
  - Changing the consequences, including planning contingencies;
  - Accepting the risk.

7.12 By establishing a clear position on risk appetite, decisions can be made as to how to prioritise and mitigate each risk. The Organisation adopts a ‘Cautious/ Medium’ approach to strategic risk management with a preference for treating risks where possible.

7.13 Risk Treatment

7.14 It is important that as much relevant detail as possible is included in the risk assessment, and mitigation plans are clear. These plans should include an action plan, tasks, cost, and timescales and risk treatment options should be prioritised in order of when they should be pursued and for how long.

7.15 Once completed and scored, the Risk Assessment Form should be sent directly to the Risk Manager for onward submission to the relevant Board for review. This scoring process will assist the Board in the overall assessment, treatment and management of that risk.

7.16 How a risk will be addressed will be considered by using one of the approaches described below:

**NOT PROTECTIVELY MARKED**

**NOT PROTECTIVELY MARKED**

- Transfer This may be done through conventional insurance methods etc.
- Tolerate The ability to take effective action against some risks may be limited, or the cost of taking action may be disproportionate to the potential benefit gained.
- Treat Most risks will be in this category. The purpose of treatment may not necessarily be to terminate the risk but to plan a series of actions to contain the risk to an acceptable level.
- Terminate This involves quick and decisive action to eliminate the risk altogether.

7.17 The relevant Governance Board should initially choose how to treat a risk based on the risk assessment. The Board should specify how any risk treatment will be implemented so that arrangements are understood and effectiveness can be monitored. This should include:

- The rationale for selection of the options included the expected benefits to be gained
- The proposed actions
- Those responsible for approving and implementing the options
- The resources expected to be required, including contingencies
- The key performance measures and controls
- When actions are expected to be undertaken and completed.

7.18 Regular review and scrutiny of actions against the agreed timetable will allow the governance Board to monitor progress on risk mitigation and where necessary to decide when to tolerate the risk.

7.19 Key risk decisions from the Governance Boards, such as an intention to remove or lower/escalate a risk, will be escalated to the SEB for final decision by the Chair (DCC). No single risk owner is able to remove their own risk. All risk decisions and removal must be approved through the SEB and Chair and cannot be actioned through other meeting groups.

7.20 A risk owner must be both aware of a wish to remove and give approval to that removal. Risk removal or proposed removal cannot take place without the approval of the risk owner.

7.21 Where a risk has been mitigated and a new risk arises within the same risk area, a new risk assessment must be provided before the original risk can be removed.

7.22 Risk Assessment Forms will be retained by the Risk Management Officer and the information contained within the Risk Assessment Form will be entered onto the Joint Strategic Risk Register.

7.23 It is the duty of the Risk Management Officer to collate updated information on each risk to be presented at the Service Area Boards. It is the duty of the Force Governance Officer to collate the risk papers to be submitted to these

**NOT PROTECTIVELY MARKED**

Boards and inform the Risk Management Officer of the risk management action carried out at the Governance Boards.

7.24 Insurance

Part of the Joint Risk Management Framework Framework includes the purchase of insurance cover to protect assets and liabilities. Insurance is a mechanism for the funding of losses, which cannot be reduced or eliminated, i.e. it is a means to transfer the risk. It is not a substitute for risk management and must not be viewed as justification for unmanaged risks.

7.25 Monitoring/ Mitigating Risks

7.26 Once control action has been agreed by the Board these actions must be effectively monitored and managed and continually updated in response to changing external and internal events. Monitoring should be undertaken before, during and after implementation of risk treatment. Ongoing and continuous monitoring provides understanding as to the extent to which internal controls are operating and provides assurance over the management of risks to an acceptable level in the achievement of organisational objectives.

7.27 To ensure this, assigned risk owners must provide update accounts to the assigned Governance Board within agreed timeframes. Risks that can be discharged following approved mitigation action can only be removed from the Risk Register following agreement by the SEB.

7.27 New risks and risk updates should be delivered at the relevant Governance Board by the appointed Strategic Risk Owner. Risk owners are therefore accountable and if they are unable to attend the Board they should ensure that a suitably informed delegate is in attendance at the meeting to present the risk.

7.28 When an established risk is reviewed by the relevant Governance Board, assessment cannot be based upon subjectivity or perception. Re-prioritisation and risk decisions should be continually based upon the force's risk matrix criteria, taking into account the revised likelihood and impact score.

7.29 The results of monitoring and review should be incorporated throughout the Organisation's wider performance management, measurement and reporting activities where possible.

7.30 All strategic risks are held on the Joint Strategic Risk Register. The Risk Register acts as one of the primary assurance mechanisms of risk management and corporate control.

7.31 Operational / project risk registers may be held locally by Departmental Leads. However to ensure appropriate scrutiny and governance these registers should be held centrally by the Continuous Improvement Department for oversight. Where appropriate local area risks should be

escalated by managers to the strategic risk level by using the risk process set out within this document.

- 7.32 Risks raised should always be submitted to the relevant Governance Board in the first instance. Where a risk is submitted past the date of a Governance Board, it will be managed until it can be scrutinised at the next Governance Board. Only in exceptional operational circumstances will a risk be raised at SEB without scrutiny at the relevant Board. Operational leads are responsible for the submission of risks and late submission of risks and papers will not be submitted until the following Board.

## **8.0 Governance**

- 8.1 Strategic Risk Management is reviewed within all of the Service Area Governance Board meetings together with other key strategic risk and business elements to ensure that risk awareness, identification and mitigation is fully integrated into all areas of the Organisation's business. Outside of the Service Area Governance Boards, risk management and reporting should run as a central theme through all meetings, ensuring that risks are discussed, registered and mitigated where necessary.
- 8.2 Risk Management is a key aspect of The Annual Governance Statement.
- 8.3 The management of Strategic risks will be reviewed on a regular basis by the Organisation's Joint Audit Committee meeting. Processes will also be reviewed by the Organisation's auditors and risks will occasionally be subject to "deep dive" reviews. The Force's approach to the management of risk will also form elements of regular inspection by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS).
- 8.4 Risk management shall be continuously improved (Principle 5) as a result of ongoing review through the governance structure and internal and external scrutiny. Continuous monitoring will enable improvements to the suitability, adequacy and effectiveness of this risk management framework.

## **9.0 Roles and Responsibilities**

- 9.1 Deputy Chief Constable:  
Responsible for the scrutiny, values, management and governance of strategic risks on behalf of the Police and Crime Commissioner for Gwent and the Chief Constable.
- 9.2 OPCC:  
Jointly identify, prioritise, manage and control risks facing the organisation and the public, maintain the OPCC risk register if held, maintain a strategic overview of risk management issues and report as appropriate to the relevant Governance Board. Responsible for joint oversight and scrutiny of the Force's Strategic Risk Management.
- 9.3 Head of Continuous Improvement:

Responsible for the effective oversight of the Strategic Risk Register, authorising the Corporate Strategic Risk Management Framework, Policy and Strategy and ensuring they remain up to date and fit for purpose.

9.4 Divisional Commanders and Heads of Departments:

Responsible for identifying and managing risks within their portfolios and for managing individual risks within the Strategic Risk Register. Each identified strategic risk will have an appropriate appointed owner responsible and accountable for ensuring that prepared responses are timely and implemented and that overall progress of risk mitigation is monitored.

9.5 Operational Owners/ Heads of Service Areas:

Responsible for completing all actions as directed by supervisors and the Governance Service Area Boards and providing timely updates in relation to progression of risk mitigation. Identify and make decisions in respect of risks facing their department and escalate risks to a strategic level where appropriate.

9.6 Risk Management Officer/ Governance Officer:

Responsible for ensuring strategic risk management records are properly maintained, the Strategic Risk Management Framework, Strategy and Policy are updated where necessary, decisions are recorded accurately and that clear audit trails exist in order to ensure openness and accountability.

9.7 All Staff:

Responsible for identifying any potential areas of risk or opportunity impacting on the organisation and bringing any risks to the attention of their line manager.

**Appendix 1**

**RISK MANAGEMENT  
RISK ASSESSMENT FORM**

Please complete the assessment below as fully as possible and return to Rachel Jones, Service Development Department.

<b>PART A (To be completed by the person identifying the risk)</b>			
<b>Subject</b> ( <i>Title of Potential Strategic Risk</i> )			
<b>Person Identifying</b> ( <i>Name, department</i> )		<b>Date</b>	
<b>Information Background</b> ( <i>include history of issue, source information, details of body or organisation, legislation. Attach supporting information where applicable.</i> )			
<b>Impact - Potential Risks or Opportunities Identified</b> ( <i>Nature and likely impact on Gwent Police and Gwent OPCC</i> )			
<p><i>Please consider the following when making an assessment. :</i></p> <ul style="list-style-type: none"> <li>• Risk to Life</li> <li>• Financial impact</li> <li>• Reputation</li> <li>• Service Delivery</li> <li>• Code of Ethics</li> <li>• Staff and public confidence</li> <li>• Data/ Information Security</li> <li>• Legal implications</li> <li>• Collaboration / partnership opportunities</li> <li>• Compliance/ complaints</li> <li>• Health and Safety</li> </ul>			
<b>Areas affected</b> ( <i>Departments, service areas, partnerships, public</i> ).			
<b>Suggested Action</b> <i>Please consider the following:</i>			
<ul style="list-style-type: none"> <li>• Outline action: State whether action already in place, or proposed</li> <li>• Anticipated timeframe for completion based on the above</li> <li>• Cost/ resourcing implications.</li> </ul>			
<b>Risk Score/Rating</b> (Please base your opinion on the criteria set out below:)			
Definition of Impact		Definition of Probability	
Critical 4	<ul style="list-style-type: none"> <li>• Major impact on finances/assets greater than £1million</li> <li>• Effect on Organisation/ Beyond Strategic – force boundaries, Home Office, partnerships, public, community</li> <li>• National media attention</li> <li>• Exceptional damage to reputation and public confidence</li> <li>• Multiple fatalities or permanent injuries</li> <li>• Very high impact upon business continuity / service disruption</li> <li>• Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having very high impact</li> <li>• National procedures, external facing policies</li> </ul>	Almost Certain 4	<ul style="list-style-type: none"> <li>• Already occurring, newly occurred or likely to be a regular occurrence, daily, weekly, monthly.</li> <li>• 90%-100% chance</li> <li>• This will occur in most circumstances</li> </ul>
High 3	<ul style="list-style-type: none"> <li>• Serious impact on finances/assets greater than £500,000</li> <li>• High effect on the organisation</li> <li>• Regional media attention</li> <li>• Significant reputational damage and public confidence</li> </ul>	Likely 3	<ul style="list-style-type: none"> <li>• A reasonable chance that this could happen and may have occurred recently</li> <li>• 50% - 90% chance</li> </ul>

**NOT PROTECTIVELY MARKED**

	<ul style="list-style-type: none"> <li>Multiple fatalities or multiple permanent injuries</li> <li>High impact upon business continuity/ service disruption</li> <li>Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having high impact</li> <li>External facing policies</li> </ul>		<ul style="list-style-type: none"> <li>Expected to happen</li> </ul>
Medium 2	<ul style="list-style-type: none"> <li>Significant impact on finances/assets greater than £250,000</li> <li>Effect on Division/ Department level</li> <li>Local media attention</li> <li>Some negative reputational consequences and public confidence</li> <li>Single Fatality or severe injury to staff member or public</li> <li>Medium impact upon business continuity/ service disruption, relevant and noticeable by stakeholders</li> <li>Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having medium impact</li> <li>External/ internal facing policies</li> </ul>	Possible 2	<ul style="list-style-type: none"> <li>Possible at some point. May occur annually or less frequently.</li> <li>25% -50% chance</li> </ul>
Low 1	<ul style="list-style-type: none"> <li>Minor impact on finances/assets up to and greater than £100,000</li> <li>Unit/ Section level/ individual</li> <li>Low impact upon business continuity/ service disruption</li> <li>Minor/contained negative consequences relating to reputation and public confidence</li> <li>Minor or slight injury to staff member or public</li> <li>Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having low impact</li> <li>Internal facing policies</li> </ul>	Unlikely 1	<ul style="list-style-type: none"> <li>Unlikely to occur at any given point. May occur annually or less frequently.</li> <li>0% - 25% chance</li> </ul>

**Gross Risk Score (Impact x Probability) (Without controls in place) =**

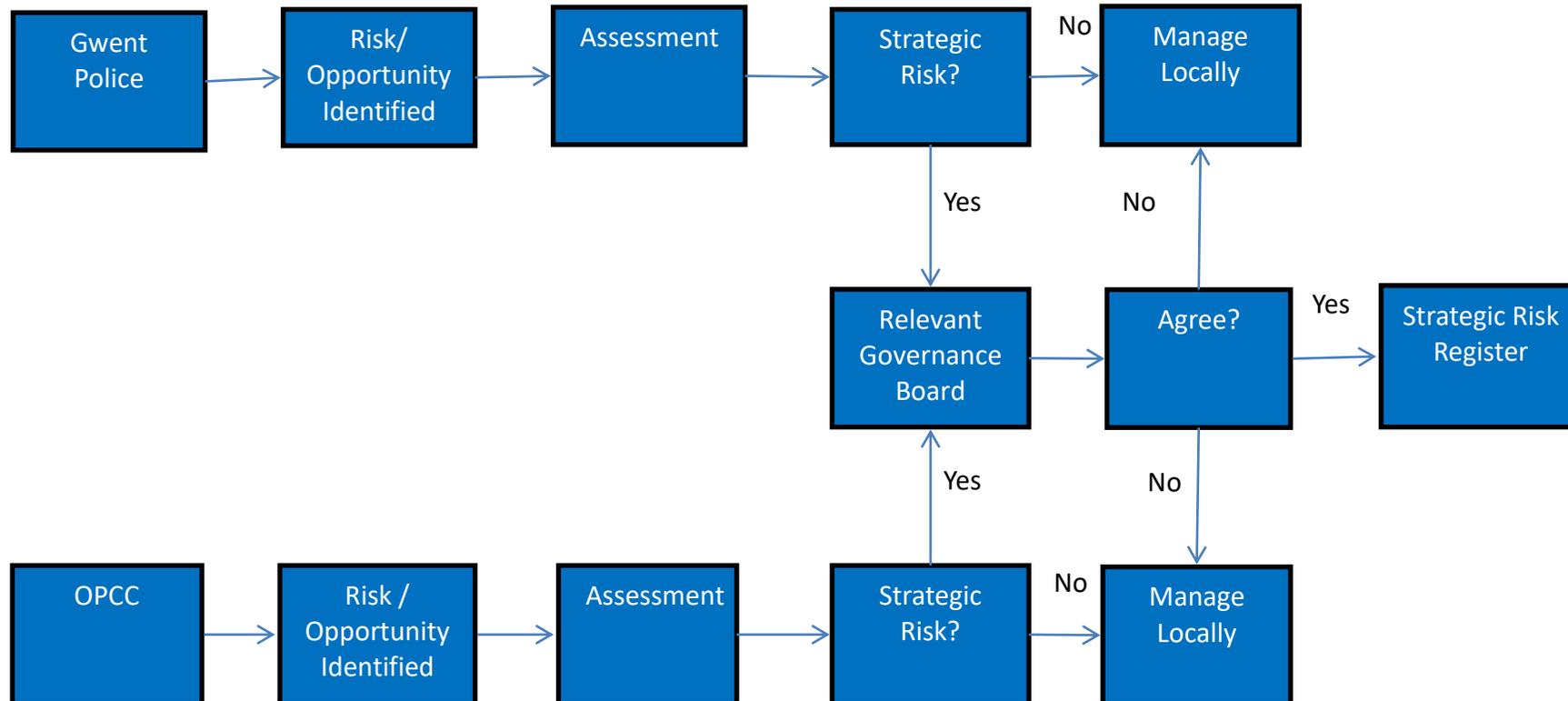
Impact 1-4		Probability 1-4			
<b>Impact</b>	Critical	4	8	12	16
	High	3	6	9	12
	Medium	2	4	6	8
	Low	1	2	3	4
		Unlikely	Possible	Likely	Almost Certain/ Certain
<b>Probability</b>					
<b>Risk Level</b>					
Low: 1, 2, 3		Medium: 4, 6, 8	High: 9, 12	Critical: 16	

**NOT PROTECTIVELY MARKED**

NOT PROTECTIVELY MARKED

APPENDIX 2

OFFICE OF THE POLICE AND CRIME COMMISSIONER AND GWENT POLICE STRATEGIC RISK MANAGEMENT PROCESS



NOT PROTECTIVELY MARKED