ORGANISATIONAL RISK POLICY

1. Executive Summary

This policy must be read in conjunction with supporting procedural guidance.

Organisational risks and issues are those problems or events which may affect WMP's achievement of our vision, strategies and objectives. Whilst organisational risks may be identified from the following, this policy will not set the framework for dynamic risk assessments as part of operational policing, health & safety risk or project change risk, please refer to the relevant policy or processes for these types of risk management.

WMP have a responsibility to design and operate effective risk management to ensure that potential threats to achieving our strategies and objectives are identified, recorded and appropriately managed. This will ensure that WMP remains resilient and enables the successful achievement of our goals in the face of a variety of potential threats, challenges and obstacles.

2. Authorised Professional Practice (APP)

This policy has been checked against APP and there is none in relation to the subject matter of this policy.

3. Scope

The Chief Constable has overall direction and control of WMP and is ultimately accountable for all policies and supporting documents of the organisation and its actions. Adherence to this force policy will be expected from:

- all employees and representatives of WMP.

4. Objectives

The aim of this policy and supporting procedural guidance is to:

- Provide the force framework and processes for organisational risk and issue management to ensure a consistent approach across the force.
- Set our vision for risk management and risk maturity, including key performance indicators for risk management.
- Establish suitable governance to manage and oversee risk management in WMP.
- Define roles and responsibilities for organisational risk management

5. Definitions/Acronyms

RISK
• A risk is an uncertain event that has not yet occurred and may or may not happen. • It has the potential to impact the achievement of objectives. • The effect can be positive (opportunity), negative (threat) or a deviation from the expected.

ISSUE
• An issue is a risk that has happened or 'materialised'. • It is an event that is currently happening or has already happened. • It is a problem affecting our objectives at the present time. Whether some, all or none of the potential consequences have actually resulted, they are now liable to because the risk source was not successfully mitigated.

DEPARTMENTAL RISKS AND ISSUES
Departmental risks and issues are risks and issues which may have an effect on the fundamental activity of a department (or departments) and the capability to meet objectives.

CORPORATE RISKS AND ISSUES
Corporate risks and issues are risks and issues of such a significant nature it warrants the escalation and additional oversight brought by Corporate risk governance. Corporate risks and issues could be significant departmental risks or risks that have an extensive and broad impact across the organisation.

STRATEGIC RISKS AND ISSUES
Strategic risks are potentially broader and longer term risks which may impact the force's ability to achieve strategic objectives for example climate change.

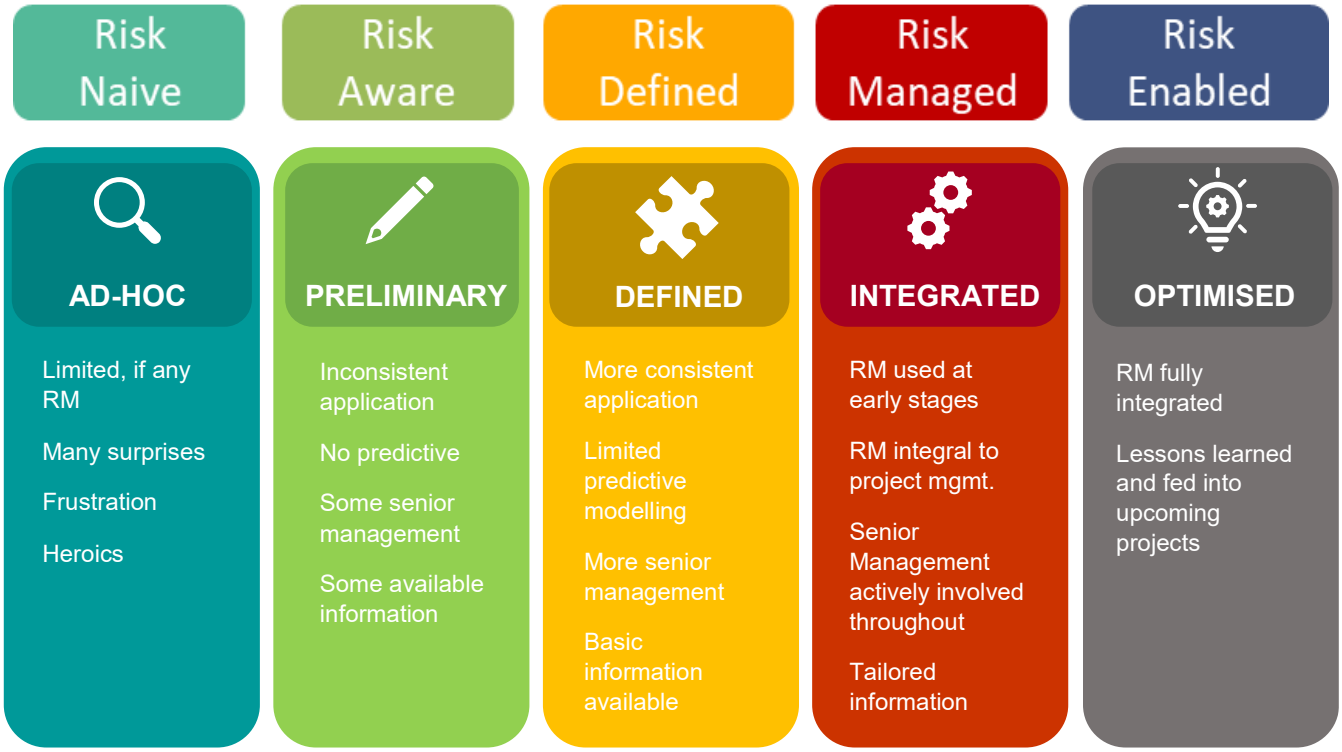
ACRONYMS

SLT- Senior Leadership Team
JAC- Joint Audit Committee
LPA- Local Policing Area
DCC- Deputy Chief Constable
ACC- Assistant Chief Constable
WMP- West Midlands Police

6. Policy Statements

RISK MANAGEMENT MATURITY & VISION

- We utilise the Institute of Internal Auditors Risk Maturity Model to define our risk maturity in WMP:



- The Deputy Chief Constable has set a force ambition and vision to achieve a maturity level of 'Risk Enabled', however, the acceptable level is to achieve and maintain a minimum standard of 'Risk Managed'.

- The Central Risk Team will conduct periodic internal risk maturity exercises. The reporting and results of which will be delivered to the force and are available on the Risk [redacted].

RISK FRAMEWORK

- Risk Management is an integral part of strategy, planning and decision making, when undertaken effectively it will assist in the achievement of our objectives and be able to provide the ability to be agile in response to challenges.

- WMP utilises an Enterprise Risk Management (ERM) based approach.

- Enterprise Risk Management (ERM) is an integrated and joined up approach to managing risk across an organisation. It enables a force-wide singular and comprehensive view of all risks/issues.

- An ERM approach will provide:

- Consistent and effective identification, management and recording of risks and issues
- Structured and reliable analysis and reporting
- A holistic approach to the management and mitigation of risk, working in collaboration with others, focussing our effort and resourcing to remove duplication and increase efficiency and effectiveness.
- A more risk focussed culture for WMP.
- Identification and management of the interrelations and interdependencies between risks, key stakeholders and other functions within WMP (i.e. HMICFRS, Org. Learning, Audit).

- In line with the ERM approach, departments must not utilise independent risks registers, all organisational risks and issues must be captured onto the WMP Risk Register.

- Activity and reporting from other areas of Corporate Development such as Organisational Learning where appropriate will be used to inform the context of risks/issues, support treatment/management, provide closure rationale and provide further assurance.

GOVERNANCE

- Organisational risk management has been designed to use and work in conjunction with the pre-existing governance structures of the force.

- Our approach to risk management will be adaptable to any governance restructures or changes in force.

- The Deputy Chief Constable (DCC) is the Force Executive Lead for organisational risk management.

- It is intended that the below governance boards will have autonomy to deal with the risks and issues within their sphere of influence and in line with the risk appetites.

- Management of risks and issues is a continual process and not inhibited by waiting for specific meetings to authorise acceptance, mitigation and other activities.

FORCE EXECUTIVE LEAD – DEPUTY CHIEF CONSTABLE									
PORTFOLIO BOARDS									
CRIME	**COMMERCIAL**	**DCC**	**CORP COMMS**	**CHANGE**	**LOCAL POLICING**	**OPERATIONS**	**PEOPLE**	**CONTACT**	**SECURITY**
ACC (Crime)	Director Commercial Services	DCC	ACC (Comms)	ACC (Change)	ACC (Local Policing)	ACC Operations	Director People Services	ACC (Contact)	ACC (Security)
SENIOR LEADERSHIP TEAM (SLT) MEETINGS									
PPU MCU Intelligence Forensics CJS	CAM Finance Contracts & Procurement IT&D IM	PSD Corporate Development Legal Services			BH LPA DY LPA CV LPA SW LPA SH LPA WS LPA WV LPA	Operations	People Services Training	Force Contact	ROCU CTU NABIS
CORPORATE DEVELOPMENT RISK TACTICAL BOARD									
RISK TEAM – CORPORATE DEVELOPMENT									
ADDITIONAL SCRUTINY (Corporate & Critical/High Departmental)									
Joint Audit Committee (JAC) PCC/CC Weekly Briefing DCC Risk & Organisational Learning Board (RAOL)									

CORPORATE DEVELOPMENT RISK TACTICAL BOARD

- Due to the various compliance and assurance functions within Corporate Development, the Corporate Development Risk Tactical Board aims to ensure a holistic and interconnected approach is taken within WMP.

- The Board will ratify all risk decisions being made in force against other interconnected functions, for example we would not ratify a closure of a risk if there is an outstanding connected HMICFRS recommendation.

- Risk Managers will be able to escalate any issues to the Board for support from Corporate Development SLT.

- The purpose of the Board will be to:
    - Ratify that risks and issues are suitably recorded and allocated appropriately.
    - Provide advice, guidance and SLT support for the management of risks and issues
    - Provide any relevant and supporting information from other functions of Corporate Development or from meetings attended by a representative of the department.
    - Oversee and manage the corporate escalation/de-escalation process.
    - Ensure evidence, assurance and organisational learning is captured.
    - Ensure the governance reporting and performance monitoring is conducted.

JOINT AUDIT COMMITTEE (JAC)

- Joint Audit Committee is an external independent body and checks both West Midlands Police and the PCC are following national and local regulations, handling public finances in accordance with the law and not taking undue risk.

- Governance and scrutiny provided by JAC supports the fourth line of defence in our assurance framework and will provide a level of credibility thereby building and maintaining trust in confidence in our ability to manage risk.

- Videos of the Joint Audit Committee meetings are available to the public via the WMPCC's YouTube Channel.

OWNERSHIP OF RISKS AND ISSUES

- All risks and issues will:
    - Have an allocated individual to be an owner and will be responsible for the management and our response to the risk or issue
    - Be allocated to the most appropriate department for accountability and governance for the management and response to the risk or issue
    - Be allocated to an ACC led portfolio

- The risk/issue owner has overall accountability for the management of the risk or issue, however,
    - Key Partners (see below) may be required to support the management and treatment.
    - Action owners can be assigned to implement specific response activities.

DEPARTMENTAL RISKS AND ISSUES

- Overall ownership and accountability for departmental level risks will be with the Chief Superintendent or Head of Department for the allocated owning department.
- The Portfolio ACC Lead for the department will have oversight of departmental level risks through the established governance and reporting arrangements for organisational risk.

CORPORATE & STRATEGIC RISKS

- Corporate and strategic risks and issues will be overseen by the Organisational Risk & Learning Board chaired by the Deputy Chief Constable (DCC).
- Overall ownership and accountability for corporate & strategic level risks will be with the Portfolio/Gold ACC Lead.
- It is likely for corporate and strategic risks that management and individual ownership for the register will be allocated to a department and lead.

KEY PARTNERS

- Risks and issues will be owned by the department where the event or problem will occur and the outcome of which will or has impacted.
- However, it is acknowledged in order to manage or treat a risk/issue effectively other departments may be instrumental and a 'key partner'.
- For example, a department has a risk around an IT system which may affect their service delivery. This risk will be owned by the department as it is their service delivery which is impacted but IT&D will be a key partner in order to manage/treat the risk.
- Responsibility to task and discuss collaborative key partner working requirement rests with the risk/issue owner.
- The owner must specify for the risk register what support is required from the key partner(s) in line with the ERM open and holistic approach.
- The expectation is that owners and key partners will collaborate effectively to drive the management and treatment of the risk/issue.
- The Risk Team will provide monthly reporting to both owning departments and key partners on the collaboration as part of monthly SLT inputs.
- Where required, support, assistance and escalations can be referred to the Risk Team and managed through the established risk governance.

RISK SYSTEMS & PLATFORMS

[redacted]

- We will record and manage all risks and issues on a central 'master' register which will be contained on a Risk Hub [redacted] platform.
- The force risk register will be the single source of truth and contain the latest information on the identification and management of risks and issues in WMP.
- The Risk Register is accessible and open to view by all. The register will include information across all departments, filters are available which can be applied as needed to tailor the information provided.
- To maintain data integrity and accuracy the Central Risk Team will be responsible for editing the risk register and [redacted] platform.
- To enable a level of self-service for the platform, limited editing ability has been granted for standard users to edit:
    - Latest Activity Update Comments Box
    - Latest Score Review
    - Actions
    - Document attachments
- An audit system is in place on the [redacted] for the Risk Team to track any changes to the register, enabling a system administrator to revert to a previously saved version of the register as required.

SENSITIVE RISKS AND ISSUES

- It is acknowledged certain risks and issues will be unsuitable for open viewing, known as sensitive risks and issues and measures are in place on the system to restrict access.
- Sensitive records will be hidden from view and only available to the Risk Team or appointed system administrators.
- Where necessary and appropriate the Risk Team will share information and details of sensitive risks on a need to know basis and with no further dissemination restrictions in place.
- Any document referencing sensitive risks and issues will be redacted or password protected.

[redacted]

- We will use an [redacted] to capture new risk and issue submission information.
- The Risk Team will periodically download submissions to excel to be retained for corporate memory.

[redacted] DASHBOARD

- We will use a [redacted] dashboard as a platform for self-service risk performance and data visualisation.
- The [redacted] dashboard will use data downloaded from the Risk Register and the data will be refreshed on a weekly basis every Monday.
- Unlike the Risk Register, users will be able to access numerical data inclusive of sensitive risks and issues (without the content or context).

SUBMISSIONS

- We will utilise the process set out in the Risk & Issue Management Process Procedural Guidance to manage our risks and issues through their lifecycle.
- Newly identified risks and issues for consideration of inclusion onto the force risk register will be submitted to the Risk Team via [redacted].
- The Submission Form consists of 12 questions which should provide sufficient information for the Risk Team to consider the risk or issue.
- Information, guidance and examples are included to support the completion of the form.
- When completed and sent, the new risk or issue will be directed to the Central Risk Team in Corporate Development.
- Upon receipt of a new risk or issue submission the Central Risk Team will:
  - Check the risk register for any previous or similar records. Where similar records are found the risk team will take the most appropriate action to avoid duplication on the register.
  - Create a record on the central master register on [redacted] and mark as a pending item.
  - If further context or information is required, the team will contact the submitter to discuss.
  - Send recognition via myservice to the sender to acknowledge the submission and engagement with risk.
  - Propose the new risk or issue to the appropriate boards and meetings for approval and ownership onto the risk register in line with the governance structure detailed in this policy.

NATIONAL RISKS AND ISSUES

- We must register all risks and issues that may impact on our ability to achieve our objectives and strategies. Therefore, we must consider national risks and issues.
- Where a national risk or issue affects WMP locally, we must capture it a new risk or issue on the register. We can ensure within the context it is clear and apparent it is a national risk/issue.
- Mitigation and treatment may be led nationally and must be captured on the record, however, we may implement local controls, treatments and monitoring and we must also capture this as evidence against the risk/issue.
- Where a national risk or issue does not affect WMP locally we do not need to record any information on our risk register.

PROJECT AND CHANGE RISKS

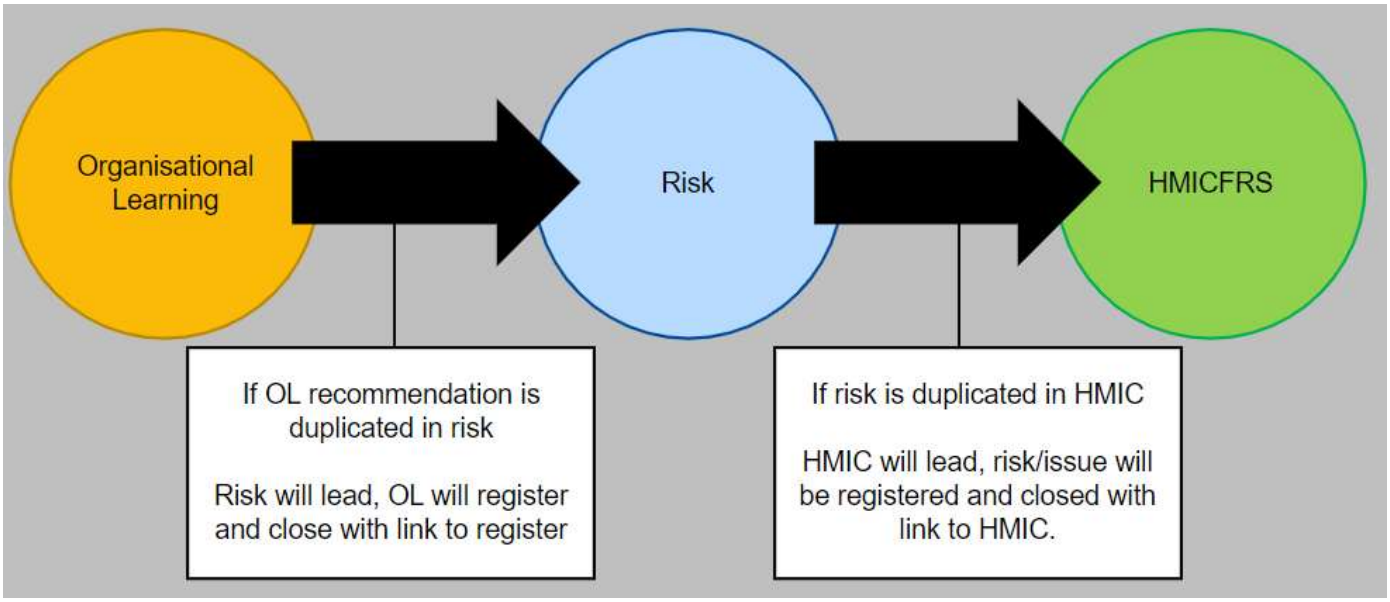
- Change and innovation involves both risk taking and risks which may impact our achievement of the aim of the project, commonly known as 'project risks'.
- Risks of this nature will be managed by Corporate Change as part of the project.
- It is acknowledged as part of business decisions being made for projects we may generate risks which will impact business as usual (BAU) or may last beyond the lifespan of the project.
- Where a risk has been identified, it is likely to impact BAU or is still open upon closure of the project, Corporate Change will refer these risks to the Risk Team for consideration of the force risk register.
- Contact may be direct or via the project closure report. Contact or receipt of the report must be timely to enable the force to manage the risk appropriately.

HEALTH & SAFETY RISKS

- Risks and issues related to Health & Safety matters will be managed by the Health & Safety Team.
- Where a risk or issue may impact force objectives, significantly impact the force or bring the force into disrepute, consideration must be made to escalate to the Risk Team for inclusion on to the force risk register.

RISKS, HMIC RECOMMENDATIONS AND ORGANISATIONAL LEARNING

- HMIC audit and organisation learning recommendations will present risks and issues for WMP.
- To reduce duplication across these three separate functions, the following governance will be applied as a general rule:



- Risk/issue opening and closure will be presented at SLT meetings/governance boards and Risk Tactical Board in line with the standard process.
- Exceptions may be made where it is deemed more appropriate for differing functions to lead or where a risk/issue is serious of nature and warrants the duplication and management through both functions.

SCORING

- All risks and issues will be scored against our Scoring Matrix.
- Risk and issue scoring are generated from a 5x5 assessment based on the likelihood of the risk occurring and the severity of potential consequences if it did.
- Due to issues being risks which have already materialised and the problem is already occurring, a likelihood score of 5 will be used for all issues to generate a score.
- Risk and issue scoring will be subjective and based on professional judgement and information available at the time. Rationale for scoring decisions will be captured on the register.
- To set a common language and understanding of scoring, once a score is generated it will be assigned a level and RAG status:

1-5	6-15	16-24	25
LOW RISK	MEDIUM RISK	HIGH RISK	CRITICAL RISK

- Owners must conduct regular score reviews so that the score is reflective of the current position and considers any changes and demonstrates the effect of any treatments or controls. implemented.
- A prompt to review the scoring will be generated with each update added onto the system, to enable to update to be saved the scoring review box must be completed as well.
- Due to system editing restrictions only the Risk Team can amend scoring on the system. Therefore, for any proposed changes to scoring a comment must be left under latest score review in the updates tab on the Risk Register record.
- When proposing changes, refer to the Scoring Matrix and provide the new numerical scores for the likelihood and impact. The Risk Team will be unable to amend scoring from new category descriptions i.e. “now a low risk”.

RISK & ISSUE RESPONSE

- We will utilise the process set out in the Risk & Issue Management Process Procedural Guidance to manage our risks and issues through their lifecycle.
- Clear allocation and accountability will be defined throughout all stages of the process.

RISK APPETITES

- This section must be read in conjunction with our Risk Appetite Procedural Guidance.
- Our response to risks and issues must be in line with WMP’s Risk Appetite.
- Risk Appetites will guide our response to risks and issues in line with our strategic objectives for the level of risk the force is willing to tolerate or the amount of effort/resources it is willing to use to manage the risk or issue.

RESPONSES

- Our response to risks and issues will be guided by the context, scoring and risk appetite.
- An element of professional judgment will always be necessary to support the overall risk management process.
- Professional judgement involves the use of individual or organisational knowledge and experience to inform and provide rationale for decision making.
- Our response(s) to risks and issues can be categorised into the following four response options available:

TREAT	Implementing controls or measures designed to eliminate or reduce the likelihood of the risk or the impact of the consequences.

	It may be necessary in line with our Risk Appetite to only partially treat a risk with an aim of bringing it to a tolerable level, the remaining element of the risk will move to 'Tolerate'.

TOLERATE	Making an informed decision that the:
	• Risk or issue is within a tolerable level in line with our Risk Appetite before any treatment
	• The cost of the treatment outweighs the benefit
	• The risk/issue or part of the risk/issue remains following treatment and
	  • The risk/issue level is now within tolerable levels
	  • Other treatment options have been exhausted
	  • Further treatment is considered excessive in terms of time or expense

TERMINATE	We stop doing the activity associated with the risk. This may not always be possible and may create risks elsewhere as a result.
TRANSFER	We avoid the risk for WMP through a contractual transfer of the risk to a third party. This might be a contractor or an insurer.

- Our response to and management of risks and issues must be necessary, proportionate and appropriate.

- It is our ambition, through implemented treatments or measures to eradicate our identified issues and eliminate the likelihood and impact of all our potential risks.

- Due to the nature of risk and issue management it is unlikely we will be able to achieve the above ambition in every case. However, mitigation can and should reduce both the impact and likelihood of the risk.

- It is acknowledged that where appropriate in line with the Risk Appetite Framework, we can tolerate appropriate risks/issues with no treatments put in place.

- If treatment options are considered, it is likely due to the types of risks and their consequences raised on the register we will need multiple and varied treatment options to provide enough assurance the risk has been suitably managed and responded to.

- Management of the risk/issue and any treatment activity will be directed by the allocated owner under the governance of the aligning department SLT and Portfolio lead.

ASSURANCE

- This section must be read in conjunction with the Procedural Guidance – Organisational Assurance Framework.

- Assurance is a tool by which leaders, managers and decision makers in WMP can have confidence that the governance arrangements, measures and mitigations that they have approved to manage our risk and recommendations are being implemented, regularly reviewed, operating as intended, and remain fit for purpose.

- We have established an Organisational Assurance Framework for Risk, Organisational Learning and HMICFRS which will provide a consistent and holistic approach to assurance across these areas of Corporate Development.

- Assurance for individual risks and recommendations will be reviewed and reported on for:

    - **Progress Reviews or Deep Dives**
      Review of completed and planned treatment/measures whilst the risk or recommendation is open to ensure that WMP is content with the current and potential levels of assurance in those areas. Focus will be given to our high and critical risks and issues.

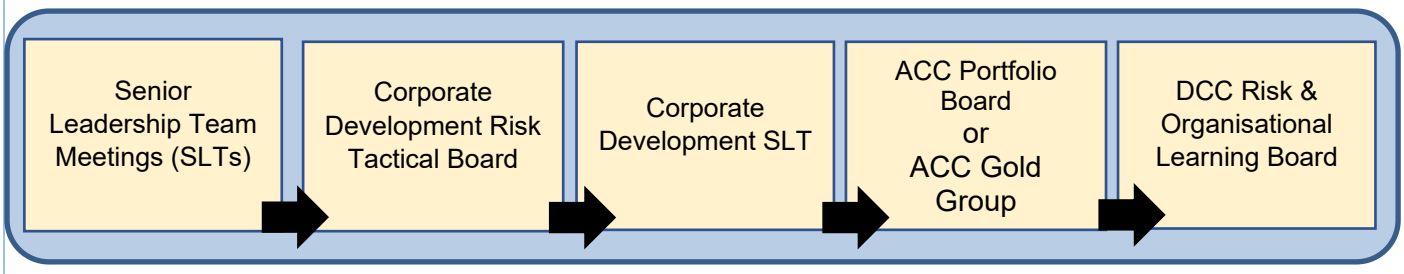
    - **Closure**
      Assurance evidence will be requested and documented as part of any closure requests and will be reported on in line with agreed processes.

    - **Follow up Review**
      Assurance review conducted 6 months after closure to confirm that measures remain in place and are sustainable and effective.

CORPORATE LEVEL ESCALATION/DE-ESCALATION

- See definition above.

- Due to the additional scrutiny and reporting over corporate level risks and issues, additional governance and approval measures are in place:



- Approval must be gained at all levels with the Deputy Chief Constable having final approval of all corporate escalations and de-escalations.

- For urgent escalations and de-escalations, if meeting schedules do not allow timely review, approval may be sought outside of presentations at boards.

REPORTING

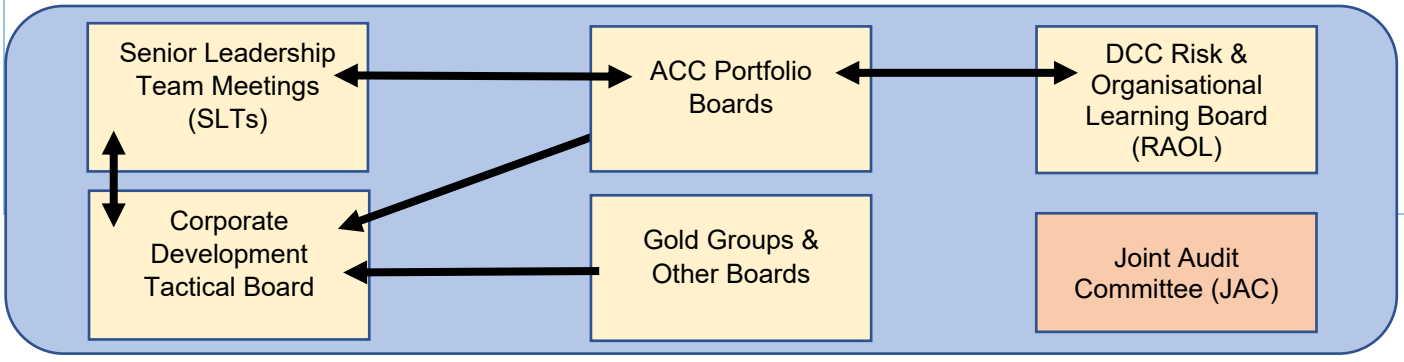
REPORTING INTO RISK TEAM

- Unless otherwise determined, risk owners or suitable points of contact must provide updates to the Central Risk Team on the following basis:
    - Open risks & issues – Monthly update on activity and a scoring review
    - Monitored risks & issues – Update on activity every 3 months and a scoring review
    - Strategic risks & issues – Update on activity every 3 months and a scoring review.
- Updates must be meaningful, detailed and informative of the current activity, management and response to risks and issues.
- As part of the update, owners must review the current risk/issue scores to accurately reflect the current position and demonstrate the effect of any treatments that have been put in place.
- Workflows on the Risk [redacted] system will generate and send designated owners a review prompt in line with the above schedule via email. The email will contain a direct link back to the risk register record.
- Updates must be provided in the first instance directly to the risk record on the register. A user guide is available with instructions. There may be occasions where the risk team can support some of these updates.
- Both the latest activity update and score review boxes need to be completed to enable the system to save the update.
- For sensitive risks and issues which cannot be accessed by users via the system, owners must provide any relevant updates and reporting to the Risk Team either via direct contact or email.

REPORTING FROM THE RISK TEAM

- Copies of reporting documents will be made available on the Organisational Risk & Issue [redacted].
- Open access will only be granted to redacted versions of documents where sensitive information is included. If you need the full reporting including the sensitive information please speak to a member of the Risk Team.

Risk reporting pathway:



SENIOR LEADERSHIP MEETINGS

- The Risk Team will attend a Senior Leadership Team meeting once a month to deliver risk reporting.

- Reporting as standard will include:
  - Force Performance for risk and risk KPIs
  - Risk Team updates or information
  - Departmental overview of owned risks and issues
  - Departmental overview of nominated key partnerships
  - Training opportunities in risk
  - Horizon scanning relevant to the department
  - Periodic reporting on risk assurance, risk appetites, risk maturity and risk culture.

PORTFOLIO GOVERNANCE BOARDS

- The Assurance Lead or member of the risk team will attend the ACC Portfolio Governance Board once a month or as scheduled to deliver risk reporting.

- Reporting as standard will include:
  - Force Performance for risk and risk KPIs
  - Portfolio overview of owned risks and issues
  - Escalations – where action is required from the Board or for corporate escalation approval
  - Periodic reporting on risk assurance, risk appetites, risk maturity and risk culture**.**

RISK AND ORGANISATIONAL LEARNING BOARD (RAOL)

- The Assurance Lead or member of the risk team will attend the Risk & Organisational Learning Board once every three months or as scheduled to deliver risk reporting.

- Reporting as standard will include:
  - Force Performance for risk and risk KPIs
  - Portfolio overviews of owned risks and issues
  - Escalations – where action is required from the Board or for corporate escalation approval
  - Periodic reporting on risk assurance, risk appetites, risk maturity and risk culture.

CORPORATE RISKS/ISSUES & HIGH OR CRITICAL SCORED DEPARTMENTAL RISKS AND ISSUES

- Due to the nature of these risks and issues higher governance, scrutiny and review is required.

- Therefore, the following additional reporting will apply to corporate level and high or critical scored records:

  - Joint Audit Committee (JAC): Reporting will be delivered to the committee every quarter (3 months)
  - PCC/CC Weekly Briefing: Reporting will be provided on a weekly basis via email
  - DCC Risk & Organisational Learning Board: Reporting will be presented to the Board every quarter (3 months)

CORPORATE DEVELOPMENT RISK TACTICAL BOARD

- Members of Corporate Development will meet on a monthly basis to discuss organisational risk.
- Reporting as standard will include:
  - Force Performance for risk and risk KPIs
  - Overview of risk team work and progress to support delivery against risk vision/KPIs
  - Overview and decisions for the framework and approach for organisational risk as a force.
  - Overview of the force's decisions and management of risks and issues for ratification
  - Escalations – where action is required from the Board or for corporate escalation/de-escalation approval
  - Periodic reporting on risk assurance, risk appetites, risk maturity and risk culture.

HORIZON SCANNING

- The Risk Team will conduct monthly horizon scanning of news reporting, social media, research and external risk reporting.
- Any articles of interest to support proactive risk identification will be compiled into a [redacted] document.
- The horizon scanning [redacted] will be shared as part of the monthly risk bulletin.
- Tailored information and articles relevant to departments will be presented to SLTs as part of the risk team monthly presentations.

ADDITIONAL REPORTING

- Where risks and issues align to known Force Gold Groups, risk reporting can be provided to the group to enable risk informed decision making.
- The monthly Risk Bulletin will provide updates, news and key risk reporting information including performance, submissions and risk register decisions.
- Additional risk and issue reporting will be provided to any other meetings, boards or governance groups such as Major Incident Readiness Board (MIRB) where required.
- If any work being completed by the force which would benefit from risk and issue reporting this can be provided on an adhoc basis on request, please speak to a member of the risk team.

KEY PERFORMANCE INDICATORS (KPIs)

- The DCC has established three key performance indicators (KPIs) for the organisation for risk:

- It must be acknowledged that the Central Risk Team cannot achieve these KPIs on behalf of WMP.
- Successful achievement of the KPIs as a force will be reliant on the engagement and investment in risk by departments and SLTs.

COMMUNICATION

- Key organisational risk information will be disseminated by the Risk Team via the following methods:
  - [redacted] Risk Site announcements
  - Newsbeat Articles
  - Monthly Risk Bulletin
  - Message of the Day
  - Agenda items at appropriate Governance Boards & Meetings
  - Email distribution to appropriate recipients

TRAINING

- Organisational risk will utilise a COM-B approach to structure training options to target the three necessary components required for behaviour or change to occur (Capability, Opportunity, Motivation).
- Training for organisational risk management will be provided by the Central Risk Team, within Corporate Development.
- Training will be offered through a variety of methods:
  - Trainer led sessions (in person, [redacted])
  - Risk Lunch & Learns
  - Go to Guides – Organisational Risk Chapter (available on desktop and mobility devices)

- College Learn Organisational Risk Training Package
  - Mandatory training for Sgt rank and above (including police staff equivalent)
  - Required completion as part of new starter induction and checklist
  - Available for self-directed CPD learning through Risk [redacted]
- SLT and Away Day inputs
- Training videos

SCHEDULE FOR TRAINING

- Any schedule for upcoming training sessions will be shared by the Risk Team via the risk bulletin, Newsbeat articles and SLT meetings.

- It is requested SLTs, risk contacts and managers disseminate training offerings wider to colleagues in their departments and teams to enable everyone to have the opportunity to attend.

TRAINING MATERIALS

- Training materials and slide decks will be available on the Risk [redacted] – Training.

- Where appropriate, video versions of training will be made available.

7. Roles and Responsibilities

ALL OFFICERS AND STAFF

- Everyone in WMP has a responsibility to help the force identify organisational risks and issues and report them to the Risk Team.
- Attending or accessing appropriate training for your role for organisational risk.

RISK OWNERS

- Manage risks and issues appropriately in line with the risk appetite, context and scoring.
- Implement and embed any treatments or controls to manage/reduce the risk or issue.
- Request and manage any collaborative working with key partners.
- Provide timely updates which are detailed and meaningful and include a latest score review in line with the schedule detailed in this policy (See Reporting to the Risk Team)
- Obtain and provide any relevant documentation or evidence for assurance (data, meeting minutes, documents).
- Request appropriate changes to the Risk Team for approval (monitoring/closure/escalation/de-escalation).

SENIOR LEADERSHIP TEAMS & ACC PORTFOLIO BOARDS

- Allocate ownership of risks and issues and ensure continual ownership is maintained.
- Review and approval of risk decisions (approval, closure, escalations etc)
- Governance and oversight of the management and treatment of risks and issues.
- Ensuring our response to risks and issues is in line with agreed risk appetites.
- Support and assistance offered for escalations and issues raised by Risk Team
- Embedding and supporting a positive risk culture, encouraging proactive risk identification and submissions.

- Promoting risk informed decision making and integration of risk management into business decisions, strategy and policy formation.

CENTRAL RISK TEAM (CORPORATE DEVELOPMENT)

- Assess, review and record all new reported risks and issues
- Maintain WMP Risk & Issue Register on [redacted].
- Produce and deliver risk presentations, products and reporting to the force, meetings and boards in line with reporting section of this policy.
- Attend meetings and boards as appropriate
- Make recommendations for the management of risks and issues including approval, allocation, monitoring, closure, escalation/de-escalation.
- Alignment of risks and issues to the force risk appetites. Conduct quarterly reviews of progress against the risk appetite and deliver subsequent reporting and recommendations.
- Review of national and external risk registers and provide recommendations of new risks to the force as well as any potential mitigation and treatment being implemented nationally.
- Provide risk management support, advice and training
- Identify and manage interconnections, thematic connections and trends for risks and issues.
- Conduct and report horizon scanning on a monthly basis
- Conduct assurance reviews, periodic maturity assessments and periodic culture reviews.
- Develop, manage and maintain WMP's risk appetite statement, risk strategy, risk policy & framework, risk vision and risk management process.

8. Relevant Legislation / Policies / Procedural Guidance

Procedural Guidance:

- Risk Appetite
- Assurance Framework
- Risk Process
- Risk Scoring Matrix

Useful Links:

Risk [redacted] Home Page
Risk Register Direct Link
Risk Reporting
[redacted] Dashboard
New Risk Submission Form

9. Equality Impact Assessment

WMP places trust in their employees to comply with force policies and to work in accordance with and in support of:

WMP Vision and Values
Code of Ethics | College of Policing

	What impact has this policy **had** on the nine protected	How **will** this updated policy positively impact each of the nine protected characteristics in

	characteristics in relation to the three general duties? (If applicable)	relation to the three general duties? If not, explain why it will not.
Age	Whilst this policy does not impact age directly, there may be occasions where people of a younger age/ younger in service (culturally) are discouraged to raise a risk, the policy however allows anyone within the organisation to raise a risk. The Risk Team would present the risk to SLT for approval therefore taking away the onerous on individuals to present to the SLT. All Police Staff and Officers will be provided with the relevant training and encouraged to proactively report on risk	The policy and procedure aim to ensure that potential risks are identified to prevent or manage threats to for the organisation as well as those when responding to the public. For the Public it ensures that systems are in place to ensure the effective running of our services and procedures and the ability to meet our objectives It ensures that should when risks are identified, mitigation is put into place to address the risk or mitigate to the point that is tolerated.
Disability	None	The policy has been written in line with the branding guidelines. The process itself around risk management again would not have any impact on those with disability. We work with individuals on a one to one basis where required when they are trying to submit a risk. Disability is also considered when we put on train to ensure people are accommodated. The policy is also made accessible to all via the WMP Policy portal which has previously been subject to equality impact assessment.
Gender Reassignment	None	The language used does not reflect or make any reference to gender identity. The risk management process does not disadvantage those undergoing or in the process of or having completed gender reassignment, internally or externally**.**
Pregnancy & Maternity	Whilst the risk management policy may not directly impact those on maternity, they may not be able to attend training days that we put on, however we do offer one to one session should an individual one when they are back in work. All our training is also accessible through the Risk SP in terms of videos for individual CPD. We can also repeat training where required	The policy and procedure aim to ensure that potential risks are identified to prevent or manage threats to for the organisation as well as those when responding to the public. For the Public it ensures that systems are in place to ensure the effective running of our services and procedures and the ability to meet our objectives It ensures that should when risks are identified, mitigation is put into place to address the risk or mitigate to the point that is tolerated
Marriage & Civil Partnership		The policy and procedure aim to ensure that potential risks are identified to prevent or manage threats to for the organisation as well as those when responding to the public. For the Public it ensures that systems are in place to ensure the effective running of our services and procedures and the ability to meet our objectives It ensures that should when risks are identified, mitigation is put into place to address the risk or mitigate to the point that is tolerated.
Race	None	The policy and procedure aim to ensure that potential risks are identified to prevent or manage threats to for the organisation as well as those when responding to the public.

		For the Public it ensures that systems are in place to ensure the effective running of our services and procedures and the ability to meet our objectives It ensures that should when risks are identified, mitigation is put into place to address the risk or mitigate to the point that is tolerated.
Religion or Belief	None	The policy and procedure aim to ensure that potential risks are identified to prevent or manage threats to for the organisation as well as those when responding to the public. For the Public it ensures that systems are in place to ensure the effective running of our services and procedures and the ability to meet our objectives It ensures that should when risks are identified, mitigation is put into place to address the risk or mitigate to the point that is tolerated**.**
Sex	None	The policy and procedure aim to ensure that potential risks are identified to prevent or manage threats to for the organisation as well as those when responding to the public. For the Public it ensures that systems are in place to ensure the effective running of our services and procedures and the ability to meet our objectives It ensures that should when risks are identified, mitigation is put into place to address the risk or mitigate to the point that is tolerated.
Sexual Orientation	None	The policy and procedure aim to ensure that potential risks are identified to prevent or manage threats to for the organisation as well as those when responding to the public. For the Public it ensures that systems are in place to ensure the effective running of our services and procedures and the ability to meet our objectives It ensures that should when risks are identified, mitigation is put into place to address the risk or mitigate to the point that is tolerated

10. Publication Instructions

Suitable for publication to public

11. Document Control

Strategic Lead: *[role and name]*	[redacted]
Policy Author(s): *[role and name]*	[redacted]
Effective Date:	08/07/2026
FET Lead: *[role and name]*	A/DCC Jennifer Mattinson
Version Number:	2.3
Review Date:	03/03/2029

Any enquiries in relation to this policy should be made directly with the Strategic Lead.

All policies are subject to a formal consultation process which encompasses Legal, Professional Standards, Faith Groups, Trade Unions, Independent Advisory Groups and wider force groups and any other relevant parties. A record of consultation can be found on the Policy Portal.

It is responsibility of the Strategic Lead to ensure that all links within the policy are correct and accessible.

Amendment History:

Version Number:	Effective Date:	Summary of Amendments:	Author:
2.0	01/04/2025	Re-write and amendments made to entire policy	[redacted]
2.1	23/09/2025	Added into policy the relationship and process between organisational learning, HMIC and risk (7.3)	[redacted]
2.2	29/01/2026	Inclusion of project risks and health & safety risks and how these work with the risk team/organisational risk	[redacted]
2.3	08/07/2026	Amendment to definitions	[redacted] DCC RAOL Board June