|  |
| --- |
| Gwent Police  Strategic Risk Management Framework |
|  |
| 2024 - 2026 |
| Review – November 2025 |

1. **Introduction**

This Gwent Police 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.

This Strategic Risk Management Framework sets out the Gwent Police’s approach to strategic risk management and outlines the supporting governance framework.

Risk management is fundamental to any organisation’s strategic management processes and controls. Risk Management is referred to throughout this Framework but incorporates both the Management of Risks and Issues**.**

We break down the framework into strategic risks and issues, and the impact they have on the Organisation as a whole. This framework will be underpinned by a Corporate Risks & Issues Register which holds the details of the controls and reactive measures put into place to manage each risk and issue.

Risk management aims to support the priority areas of strategic focus for the Office of the Police and Crime Commissioner’s (OPCC) Police, Crime and Justice Plan and focus on the risks and issues to delivering against the objectives of the plan:

* Preventing Crime and anti-social behaviour
* Making communities safter
* Protecting the vulnerable
* Putting victims first
* Reducing reoffending

**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 arise from the fundamental decisions taken by the Police and Crime Commissioner (PCC) and Chief Constable (CC) in relation to the choice of the strategic direction to be taken and consequent achievement of those strategic objectives

Strategic risks are something else and reflect risks associated with poor strategic direction/ articulation of strategic objectives and the risks arising from changed political parties and the impacts of changes regulation inspection regime etc

• Operational risks are those that affect our key organisational enablers and our ability to respond effectively to external incidents.

Operational risk refers to risks around people (not enough/ incompetent etc), process (e.g. process for evidential storage is inadequate), IT systems and of course risks around external events (fire, flood, cyber-attack etc).

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

Strategic Issues are slightly different to Strategic Risks, in that the event has already happened and this event has affected the achievement of the organisation’s strategy and objectives. There is no need to consider the probability of the event occurring, only the impact this event now causes to the Organisation.

1. **Objectives**

Risk management will be:

* An essential part of governance and leadership, and fundamental to how the Organisation is directed, managed and controlled at all levels.
* An integral part of all organisational activities to support decision-making in achieving objectives.
* collaborative and informed by the best available information and expertise.

We will do this by:

* determining a clear strategic direction and evidence-based decision making,
* having a systematic approach to identify and control risks and issues to an acceptable level,
* ensuring a timely and accurate reporting and record keeping,
* having robust risk management standards that align to and deliver the Police and Crime plan and Chief Constables delivery plan.
* having clear roles and responsibilities (see Roles & Responsibilities section),
* continuously integrating strategic risk management into the culture of the organisation and existing processes,
* learning and sharing our experiences.

1. **Roles & Responsibilities**

**Gwent Police – the organisation:**

Responsibility lies in having processes that identify and track risk management. We have woven risk management into our business planning cycle, so it positively impacts internal and external scrutiny and audit, board and meeting functionality, overall service improvement and effective planning processes (including HMICFRS Force Management Statement).

It is the role of the governance board chairs to:

* identify new and emerging risks and issues,
* assess risks for potential impact and probability,
* assess issues for their level of impact to the organisation,
* place accountability for managing risks to those best able to control them and constructively challenging them with a view to ensuring risks are being effectively managed,
* ensure balanced and informed assessments of risks are provided,
* 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 processes and transparency.

**Deputy Chief Constable:**

Responsible for the scrutiny and decision making, values, management, and governance of strategic risks on behalf of the Chief Constable.

**Head of Continuous Improvement:**

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

**Heads of Departments:**

Responsible for identifying and managing risks within their portfolios and for managing individual risks within the Strategic Risk & Issues 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.

**Risks and Issues owners:**

Responsible for completing all actions as directed by supervisors and the Governance 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.

**Governance, Policy and Risk Manager:**

Responsible for ensuring strategic risk management records are maintained and constructively challenge the adequacy of records, the Strategic Risk Management Framework, Strategy and Policy are updated where necessary, decisions are recorded accurately and that clear audit trails exist to ensure openness and accountability. Resilience of this role will sit with the Governance & Assurance Inspector.

**Governance officers:**

Responsible for obtaining an updated risk report for submission into the Governance.

Boards and ensuring the Risk Management Officer and Board meeting attendees have

accurate updates and information pre and post Board meetings.

**Joint Audit Committee:**

Responsible for guiding and advising the service but also challenging Chief officers over the adequacy of the overall risk framework and the effectiveness of the actions being taken to mitigate risks and issues recorded on the Risk and Issues Register.

**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.

1. **Governance**

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

Strategic risks and issues are submitted and monitored within service area Governance Boards within the force governance structure. 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, and staff associations.

In respect of the OPCC scrutiny, risks and issues register updates will be discussed at Strategic Performance board but the force owns the risk or issue.

Risks and issues update meeting frequency will depend on the associated grading and the ongoing assessment of the risk or issue and with guidance from board chairs.

As per the governance structure, risks and issues will be aligned to an appropriate Assistant Chief Officer Chaired board for appropriate scrutiny and to ensure accountability of owners. Please see current governance structure.

Progress of risk and issue management will escalate through the governance structure to ensure scrutiny and awareness.

1. **Risk and Issues Register**

The Project Management Body of Knowledge (PMBOK) defines risk as, “An uncertain event or condition that, if it occurs, has a positive or negative effect” On the adverse where a risk might happen, an issue has happened. An issue always has a negative connotation.

In essence risks are something that are approaching in the future that the force anticipates will be a problem but for which there is time and opportunity to put mitigation and adequate controls in place with the potential to remove or minimise that impact. Issues relate to something that is happening now and which needs to be treated as a matter of urgency.

**Risks**

As risks are potentials the methodology that should be applied is in –

1. Identifying the risk

2. Assessing the risk (utilising the grading matrix – risks will have a probability rating)

3. Controlling the risk (4T approach and governance – risks will have a mitigation plan to influence the likelihood of occurrence)

4. Reviewing the controls

The skill in risk management is to apply phases 1-4 successfully before a risk becomes an issue.

**Issues**

The process for the management of issues follows a similar methodology for the management of risks with the exception that once classified as an issue they must be addressed with a response plan. Additionally, they will not have a probability of occurrence as they will have already happened or be happening, and they will not have a mitigation plan for the same rationale.

The debate at boards, in addition to its resolution, should then be around how a risk became an issue and whether the mitigation that is/ was in place was robust.

Dependent on grading and urgency of the concern, the timeliness of updates should be –

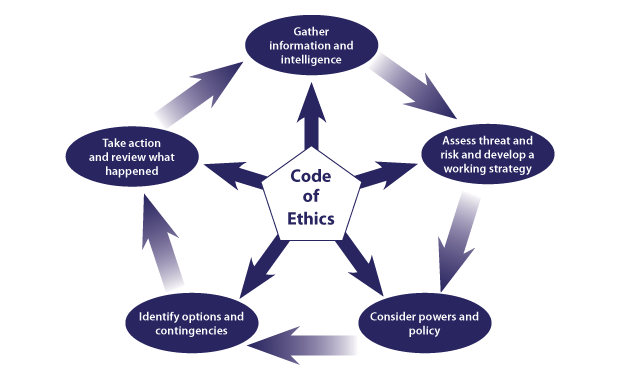
* Issues: weekly/ fortnightly > monthly
* Risks: monthly > quarterly

Response should be organisational wide, whilst accepting that all risks and issues will have an identified owner at the point a concern has been classified as an issue it has been accepted that there is more urgency required to the resolution of the problem than previously acknowledged.

Depending on the response / success of actions and mitigation and milestone achievement a concern can flex and move between being a risk or an issue but the change in approach will provide a more focused review and response as to hindrance factors and prevent mission drift.

1. **Our Approach**

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.

**Risk & Issues Identification / Assessment**

In order to manage risk, the organisation needs to know what risks or issues it faces, and to evaluate them accordingly. Risk and Issues 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.

Risk & Issue identification may arise from operational policing, the Force governance, 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 any concerns they identify.

When a risk or issue is identified for the strategic register a full assessment should be undertaken and returned to the Governance supervisor 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 remaining after additional controls are applied). In completing the risk assessment, evaluation should be collaborative and informed by the best available information and expertise. 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.

The Risk and Issues 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 and an Issues Matrix is provided within the blank Risk Assessment Form. The Matrices outline numbered levels of risk that can be used as a guide to obtain a final risk score.

As the matrices 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.

1. **Assessing a risk or an issue**

Risk and Issues Assessment Matrices sets out a number rating system of 1 – 4 (1 = Low, 4 = Critical) to assist the measurement of level and threat (as outlined below and on the Strategic Risk Assessment form shown in Appendix 1).

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Gross Risk Score** (*Impact x Likelihood)* = | | | | | | | | |
| Impact 1-4 | | | Probability 1-4 | | | | | |
| **Impact** | 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 |
| **Probability** | | | | | | | |
| Risk Level | | | | | | | | |
| Low: 1, 2, 3 | | Medium: 4, 6, 8 | | | High: 9, 12 | | Critical: 16 | |

|  |  |
| --- | --- |
| Critical 4 | * Major impact on finances/assets greater than £1million * Effect on Organisation/ Beyond Strategic – force boundaries, Home Office, partnerships, public, community * National media attention * Exceptional damage to reputation and public confidence * Multiple fatalities or permanent injuries * Very high impact upon business continuity / service disruption * Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having very high impact * National procedures, external facing policies |
| High 3 | * Serious impact on finances/assets greater than £500,000 * High effect on the organisation * Regional media attention * Significant reputational damage and public confidence * Multiple fatalities or multiple permanent injuries * High impact upon business continuity/ service disruption * Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having high impact * External facing policies |
| Medium 2 | * Significant impact on finances/assets greater than £250,000 * Effect on Division/ Department level * Local media attention * Some negative reputational consequences and public confidence * Single Fatality or severe injury to staff member or public * Medium impact upon business continuity/ service disruption, relevant and noticeable by stakeholders * Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having medium impact * External/ internal facing policies |
| Low 1 | * Minor impact on finances/assets up to and greater than £100,000 * Unit/ Section level/ individual * Low impact upon business continuity/ service disruption * Minor/contained negative consequences relating to reputation and public confidence * Minor or slight injury to staff member or public * Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having low impact * Internal facing policies |

The Organisation can use the same risk matrix to evaluate the severity of issues. Since issues have a likelihood of “occurred” the risk matrix can also be used to accommodate the rating of issues without the need of having a separate issue rating table. Likelihood is no longer needed for consideration. This means that only impact would be considered when grading the Issue from Low, Medium, High to Critical (using the descriptives of “Impact” provided within the Risk Assessment)

Issues will be graded as Low, Medium, High and Critical impact, using the descriptives below. No number value will be used as there is no requirement to multiply the Impact by Likelihood, as we already know it is occurring.

**Gross Issue Score** (*Impact level of Low, Medium, High or Critical) =*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood | | Impact / Consequence | | | |
| Low | Medium | High | Critical |
| ISSUE | Occurred |  |  |  |  |
| 4 | Almost Certain |  |  |  |  |
| 3 | Likely |  |  |  |  |
| 2 | Possible |  |  |  |  |
| 1 | Unlikely |  |  |  |  |

Risk appetite or 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).

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.

By establishing a clear position on risk appetite, decisions can be made as to how to prioritise and mitigate each risk.

Where a risk has become an Issue during its time on the force register, the same options would be available to the owner, and a treatment method identified.

**Treatment**

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.

Treatment options are provided in the table below.

|  |  |
| --- | --- |
| * 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. |

When completing the Assessment Form, the relevant Owner should initially choose how to treat a risk based on the four options presented, while guided by the Governance & Assurance and Joint Audit Committee, when necessary. Careful consideration should also be given to the scoring given on the risk assessment, as it will assist the Owner when deciding on a treatment plan. The Owner should specify in as much detail how any risk treatment plan will be implemented so that arrangements are understood, and effectiveness can be monitored.

This should include:

* The rationale for selection of the option, including 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. This timeline needs to be clearly laid out to ensure the plan is met.

The Risk and Issues Register is within a Microsoft Lists application and available in each Teams board channel. Updating of the register will remain with the Governance & Risk supervisor or officers. Lists application has version control functionality and storage for relevant documents such as assessments and updates.

Risks & Issues Owners will be regularly prompted to review the proposed treatment plan. If the treatment plan is no longer appropriate or effective, then it can be amended to reflect the current nature and circumstances surrounding the risk. Any decisions to change a treatment plan, would then be discussed at their individual boards and then put to the Deputy Chief Constable at the Scrutiny Executive Board (SEB) for approval.

**Residual Scoring Assessments**

Key decisions from the Governance Boards, such as an intention to remove or lower/escalate a risk or issue, will be escalated to the SEB for final decision by the Deputy Chief Constable. No single risk and issue Owner can remove their own risk. All decisions and removal must be approved through the SEB and Deputy Chief Constable and cannot be actioned through other meetings or boards.

The Owner must be both aware of a request to remove and give approval to that removal. Risk and issue removal or proposed removal cannot take place without the approval of the risk owner.

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

Assessment Forms will be retained by the Risk & Governance team and the information contained within the Assessment Form will be entered onto the Risks and Issue Register. The completed forms will be contained within the Risks and Issues Register maintained on the Microsoft Lists application.

It is the duty of the Risk & Governance officers to collate updated information on each risk to be presented at the relevant governance boards. It is the duty of the Risk and Governance Officers to collate the risk papers to be submitted to these Boards and inform the Risk and Governance supervisor the risk management action carried out at the Governance Boards especially where archiving of any risks and issues has occurred.

**Monitoring / Mitigating Risks**

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.

To ensure this, assigned owners must provide update accounts to the assigned Governance Board within agreed timeframes.

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

**Meeting frequency**

Risks relate to something that may occur in the future. This means risks could be monitored less frequently on a bi-monthly or quarterly basis through the use of Implementation / Delivery Plans that provide a timeframe to achieve outcomes.

As issues relate to managing the impact of an event that has already transpired, mitigation is more urgent, and as such, issues will be monitored on a monthly basis. Whereas updates for some risks can be less frequent as they tend to have more extended deadlines/timeframes.

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

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

Operational / project risk registers may be maintained locally by Departmental Leads but to ensure appropriate scrutiny and governance these registers should be stored 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.

**Insurance**

Part of the Risk Management 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.

1. **Appendix**

**GWENT POLICE**

**STRATEGIC RISKS & ISSUES ASSESSMENT FORM**

Please complete the assessment below as fully as possible and return to Risk Management officer or Governance & Assurance officer via Gwent Corporate Risk Management email.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk & Issues Assessment: To be completed by the person identifying the risk** | | | | | | | | | | | | |
| **Risk or Issue** *(Please specify which)*  *A risk is an event that has not happened yet but may. We plan and work out mitigation for critical risks.*  *An issue is something that already has happened. Immediate action must be taken to mitigate its impact.* | | | | | | | | | | | | |
| **Subject** *(Title of Potential Strategic Risk or Issue)* | | | | | | | | | | | | |
| **Person Identifying** *(Name, department)* | | | | | | | **Date** *(original identified)* | | | | | |
| **Risk / Issue Owner** *(include history of issue, source information, details of body or organisation, legislation. Attach supporting information where applicable.)* | | | | | | | | | | | | |
| **First Point of Contact for Updates** *(Please list all applicable staff involved in the management of the risk / issue):* | | | | | | | | | | | | |
| **Information Background** (*include history of issue, source information, details of body or organisation, legislation. Attach supporting information where applicable*.) | | | | | | | | | | | | |
| **Cause of Risk / Issue** (*e.g., resourcing, IT infrastructure, policy and procedure, external factors):* | | | | | | | | | | | | |
| **Impact / Consequence** (Nature and likely impact on Gwent Police)  Please consider the following when making an assessment:  • Risk to Life  • **Financial impact (ensure completed below)**  • Reputation  • Service Delivery  • Code of Ethics  • Staff and public confidence  • Data/ Information Security  • Legal implications  • Collaboration / partnership opportunities  • Compliance/ complaints  • Health and Safety | | | | | | | | | | | | |
| **Financial Costs / Implications:** | | | | | | | | | | | | |
| **Areas affected** (Departments, service areas, partnerships, public). | | | | | | | | | | | | |
| **Action already undertaken / controls in place** *(What is already in place to mitigate this risk/ issue):* | | | | | | | | | | | | |
| **Desired Outcome of the Risk / Issue** *(Please give a brief statement of the intended outcome / satisfactory conclusion of the risk / issue):* | | | | | | | | | | | | |
| **Proposed actions to achieve outcome** *(please provide a “steps to reduce” plan for reducing the risk / issue through to closure – with timeframes attached)* | | | | | | | | | | | | |
| **Estimated Date of Closure of the Risk / Issue** *(can be reviewed and reassessed where necessary):* | | | | | | | | | | | | |
| **Force Governance Board:** | | | | | | | | | | | | |
| **Risk Score / Rating** *(Please base your opinion on the criteria set out below taking into account level of the actions already undertaken and those needed)* | | | | | | | | | | | | |
| Definition of Impact Definition of Probability | | | | | | | | | | | | |
| Critical 4 | * Major impact on finances/assets greater than £1million * Effect on Organisation/ Beyond Strategic – force boundaries, Home Office, partnerships, public, community * National media attention * Exceptional damage to reputation and public confidence * Multiple fatalities or permanent injuries * Very high impact upon business continuity / service disruption * Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having very high impact * National procedures, external facing policies | | | | | | | Almost Certain 4 | | * Already occurring, newly occurred or likely to be a regular occurrence, daily, weekly, monthly. * 90%-100% chance * This will occur in most circumstances | | |
| High 3 | * Serious impact on finances/assets greater than £500,000 * High effect on the organisation * Regional media attention * Significant reputational damage and public confidence * Multiple fatalities or multiple permanent injuries * High impact upon business continuity/ service disruption * Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having high impact * External facing policies | | | | | | | Likely 3 | | * A reasonable chance that this could happen and may have occurred recently * 50% - 90% chance * Expected to happen | | |
| Medium 2 | * Significant impact on finances/assets greater than £250,000 * Effect on Division/ Department level * Local media attention * Some negative reputational consequences and public confidence * Single Fatality or severe injury to staff member or public * Medium impact upon business continuity/ service disruption, relevant and noticeable by stakeholders * Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having medium impact * External/ internal facing policies | | | | | | | Possible 2 | | * Possible at some point. May occur annually or less frequently. * 25% -50% chance | | |
| Low 1 | * Minor impact on finances/assets up to and greater than £100,000 * Unit/ Section level/ individual * Low impact upon business continuity/ service disruption * Minor/contained negative consequences relating to reputation and public confidence * Minor or slight injury to staff member or public * Breaches of data, compliance, complaints, insensitive or unethical behaviour, corruption or misconduct having low impact * Internal facing policies | | | | | | | Unlikely 1 | | * Unlikely to occur at any given point. May occur annually or less frequently. * 0% - 25% chance | | |
| **Gross Risk Score** (*Impact x Likelihood)* = | | | | | | | | | | | | |
| Impact 1-4 | | | | Probability 1-4 | | | | | | | | |
| **Impact** | | 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 |
| **Probability** | | | | | | | | | | |
| Risk Level | | | | | | | | | | | | |
| Low: 1, 2, 3 | | | Medium: 4, 6, 8 | | | High: 9, 12 | | | | | Critical: 16 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Gross Issue Score** (*Impact level of Low, Medium, High or Critical) =*  As Issues have already occurred or currently happening, ONLY **impact** would be considered when grading the Issue from Low, Medium, High to Critical (using the descriptives of “Impact” provided within the Risk Assessment).   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Likelihood | | Impact / Consequence | | | | | Low | Medium | High | Critical | | ISSUE | Occurred |  |  |  |  | | 4 | Almost Certain |  |  |  |  | | 3 | Likely |  |  |  |  | | 2 | Possible |  |  |  |  | | 1 | Unlikely |  |  |  |  | |