RISK MANAGEMENT

Owning Department: Strategic Business and Operational Services (SBOS)

Department SPOC: Risk and Compliance Manager

Governing Policy: Risk Management

Risk Rating: Low

Legal Sign Off: 04/12/2023

JNCC: December 2023

Published Date: 31/03/2025 (v2.1)

Review Date: 04/12/2027

Index

1. Summary of Changes

1.1 This is a review of a joint procedure, incorporating developments in a maturing approach to risk management, and reflecting recommendations from internal audit.

1.2 This procedure replaces the following document:

- Monitoring and Review of Risk (Procedure)

2. Procedure Aim

2.1 This procedure outlines the processes to follow to undertake risk management as part of the risk framework for Norfolk and Suffolk Constabularies (together 'the Constabularies'). It describes the main processes required to successfully deliver the joint risk management policy, ensuring organisational risk is managed effectively.

2.2 All officers and staff are encouraged to be risk aware in order that risks can be identified, assessed and managed, therefore embedding risk management throughout the Constabularies.

3. Applicability

3.1 Unless otherwise stated, this procedure applies to all police officers (including officers of the Special Constabulary) and all members of police staff (including police support volunteers).

4. Overview of the Risk Management Process within the Framework

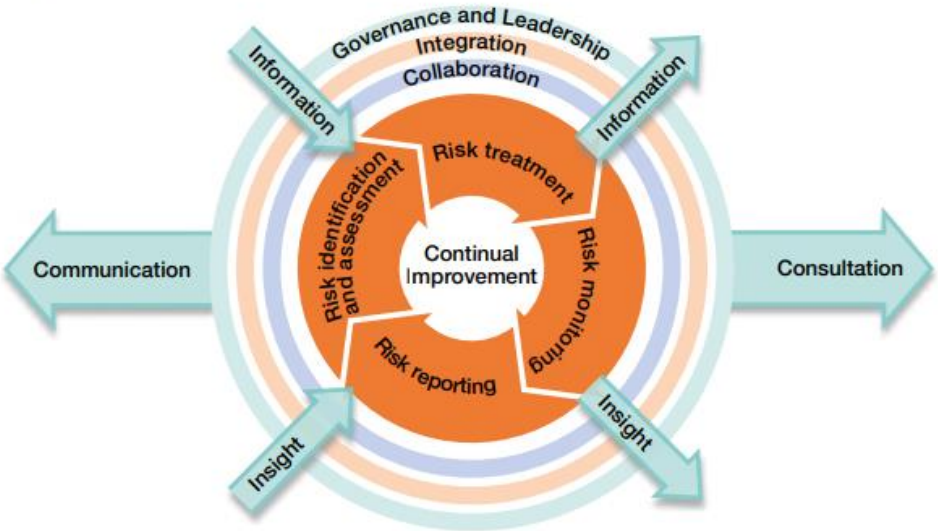
4.1 The risk management process is the planned and systematic approach to the identification, assessment, evaluation, treatment, monitoring and reporting of risks in order to aid operational effectiveness, continuous improvement and deliver organisational objectives. Risk controls and mitigation plans can reduce the probability of a risk occurring to an acceptable level or if the event does occur, reduce its level of impact.

4.2 An effective risk management process is critical for the organisation to help ensure that it reduces the frequency of risk events occurring, mitigates the impact they may have on service delivery and strategic objectives, and enhance strategic planning and prioritisation.

4.3 As per the policy, the Constabularies aspire to follow the 'Orange Book: Management of Risk – Principles and Concepts' guidance produced by the Government Finance Section which sets out the following Risk Management framework and processes.

4.4 Orange Book Risk Management Framework:

Risk Management Framework



4.5 The essential elements of the risk management process (covered in more detail in the subsequent sections) are as follows:

- Sources of risk (causes)
- Identification (impact on objectives)
- Assessment (analysis of impact and evaluation)
- Appetite and Tolerance
- Treatment
- Monitoring
- Reporting

5. Sources of Risk

5.1 Risks can be identified from a number of different existing conditions, either internal or external.

5.2 Examples of internal and external sources:

INTERNAL	EXTERNAL
Staff and officers at all levels	National Police Chiefs Council
Changes in the operating environment	Office of Police and Crime Commissioner (OPCC)
Strategic Assessment	College of Policing (CoP)
Force Management Statements (FMS)	Government reports and reviews, e.g. National Risk Register
SWOT analysis	Partners
Risk identification exercises such as Bowtie	Professional bodies or organisations, e.g. World Economic Forum, ALARM, CIPD.
Outcome Based Budgeting process (OBB)	External environment (PESTLE) analysis
Programme RAID	HMICFRS
Audit	Horizon scanning
Portfolio Management Office (PMO)	

5.3 Horizon scanning: The Organisational Analysis Team undertakes regular horizon scanning which the Risk and Compliance Manager reviews on a quarterly basis. It is also periodically included in the FMS evergreen updates.

5.4 Both force executives monitor national reports and reviews, and the potential risks and impacts.

5.5 The categories below should be used to aid thinking:

Category	Description
Public Confidence	Risks that will negatively impact public or stakeholder trust, expectation or perception.
Finance and Money	Risks that will impact the ability to meet the Medium Term Financial Plan or stay within budget, that will incur additional costs or financial loss, or developments that affect financial plans e.g. decrease in funding
Compliance (Legal / Statutory)	Risks that will mean a failure to obtain the appropriate approval or standard, or mean we are unable to meet statutory or regulatory obligations, or that involve

	unexpected licensing requirements or new/changes to legislation
Resources (People)	Risks that will limit resource availability, result in a lack of skills, negatively impact on health and wellbeing, or succession planning
Service Delivery and Performance	Risks that will impact on the efficiency of core processes, on quality or performance, or business continuity, result in an excessive increase in demand, mean we are unable to meet internal or external service level agreements, or is a contractual issue i.e. failure of suppliers / contractors / partners to deliver

6. Identification

6.1 'Risk is the effect of uncertainty on objectives'.

6.2 Risk identification is the process of identifying and describing risks that could impact on the Constabularies achieving their objectives.

6.3 A **risk** is a problem, uncertainty or event which may happen.

6.4 An **issue** is an event that has happened and now requires management action, or a risk that has come to fruition where you can no longer stop the impact.

6.5 The treatment of an issue differs to a risk, as it is by nature, more urgent and management action should be taken quickly.

6.6 It is the responsibility of staff and managers at all levels to be aware of the risks they face while undertaking their day-to-day activities. Once a new risk has been identified, it can be added to the relevant Risks and Issues Log (R&I Log) or Strategic Risk Register (SRR), see section 12 Recording.

6.7 The Risk and Compliance Manager checks the R&I Logs on a bi-monthly basis for new risks but ideally the new risk should be raised in conjunction with the Risk and Compliance Manager to aid consistency.

6.8 New SRR risks are raised through the SRR review process. They can be identified by chief officers or the Risk and Compliance Manager and then taken to the relevant chief officer meeting for ratification.

7. Assessment (analysis and evaluation)

7.1 Risk assessment is the process of analysing and evaluating risk(s) once they have been identified.

7.2 Risk Analysis: While each risk identified is important, some form of measurement is necessary to evaluate their significance to support decision making. A standard approach to risk analysis aids comparison

and aggregation and therefore prioritisation of risks across the Constabularies.

7.3 Risk analysis looks at what the consequences of the identified risk(s) are (Impact) and how likely they are to happen (Likelihood).

7.4 The criteria for assessing risks are defined using a 4 x 4 matrix:

RISK SCORE MATRIX		LIKELIHOOD			
		Remote Possibility (1)	Possible (2)	Likely (3)	Almost Certain (4)
IMPACT	Critical Impact (4)	4	8	12	16
	Serious Impact (3)	3	6	9	12
	Marginal Impact (2)	2	4	6	8
	Negligible Impact (1)	1	2	3	4

7.5 To aid analysis the following definitions are available:

7.6 Impact for Risk and Issues Logs:

DEFINITION OF IMPACT SCORE		
No	**DESCRIPTION**	**IMPACT**
1	Negligible	Negligible service disruption, no or little deviation from departmental/command plans, negligible financial impact, little or no impact on public confidence.
2	Marginal	Limited service disruption, short term and minor deviation from departmental/command plans, minor financial impact; little public or partner dissatisfaction, minor negative impact on public confidence.
3	Serious	Significant service disruption, medium term and serious deviation from departmental/command plans, noticeable public/ partner dissatisfaction, significant financial impact, negative impact on public confidence.
4	Critical	Major service disruption, significant recovery time required, long term and severe deviation from departmental/command plans, severe financial impact, possible public or other enquiry, negative and long term impact on public confidence.

7.7 Impact for SRRs:

DEFINITION OF IMPACT SCORE (SRR)		
No	**DESCRIPTION**	**IMPACT**
1	Negligible	Negligible service disruption: no or little deviation from strategic plans; negligible financial impact, little or no impact on public confidence.
2	Marginal	Limited service disruption: short term and minor deviation from strategic plans; minor financial impact; little public or partner dissatisfaction; minor negative impact on public confidence.
3	Serious	Significant service disruption: medium term and serious deviation from strategic plans, noticeable public/ partner dissatisfaction; significant financial impact; negative impact on public confidence.
4	Critical	Major service disruption: significant recovery time required; long term and severe deviation from strategic plans, severe financial impact; possible public or other enquiry; negative and long term impact on public confidence.

7.8 Likelihood for SRRs and Risk and Issues Logs:

DEFINITION OF LIKELIHOOD SCORE			
No	**DESCRIPTION**	**PROBABILITY**	**LIKELIHOOD**
1	Remote Possibility	5% - 20%	The risk or event is very unlikely to occur at the current time, there is currently no indication that the risk or event will happen
2	Possible	20% - 50%	The risk or event could occur, you cannot be certain that it will not
3	Likely	50% - 80%	The risk or event is more likely to happen than not
4	Almost Certain	80% or more	The risk or event is expected to occur or occurs regularly, there is a very significant chance it will happen

7.9 Each risk should be given a score before and after mitigation is in place using the R&I Log or SRR to record this.

7.10 It is recognised that rating a risk is not an exact science and should be informed by evidence where possible, i.e. data, trends, historic information/events etc., however it is also about applying collective professional knowledge and judgement. The Risk and Compliance Manager will evaluate the scoring for appropriateness and consistency.

7.11 Risk evaluation compares the results of the risk analysis with the nature and extent of risks that the organisation is willing to take (its risk appetite), to determine where and what additional action is required.

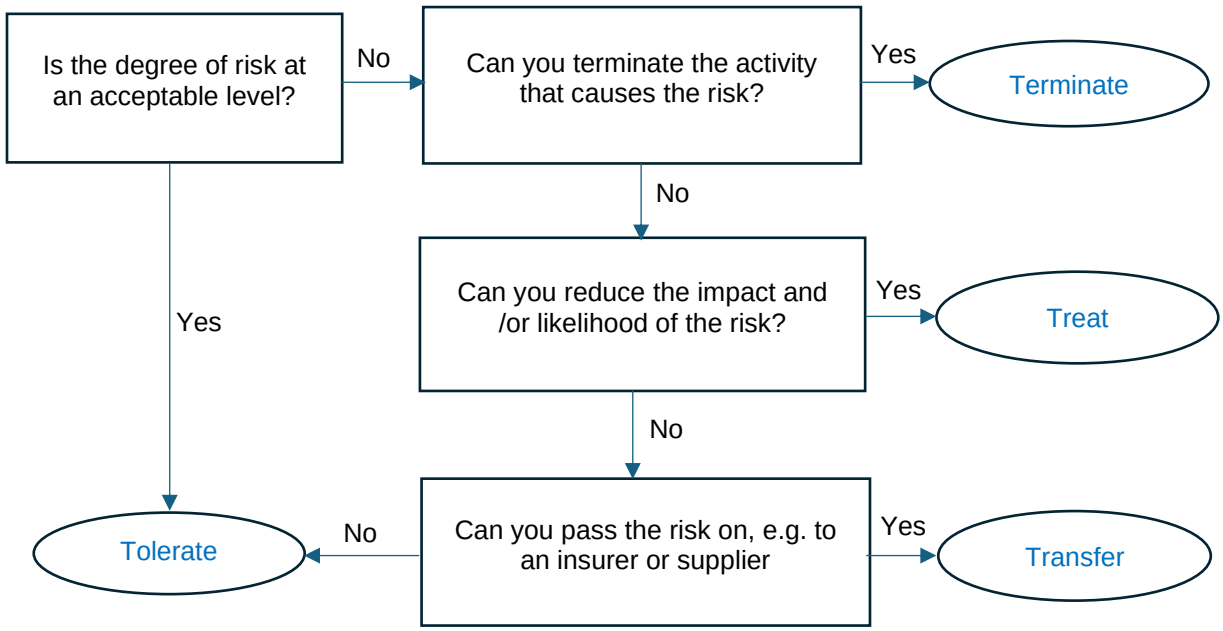
8. Treatment

8.1 Risk treatment is the selection, design and implementation of options that support the achievement of intended outcomes and manage risks to an acceptable level.

8.2 Treatments fall into four categories known as the 4Ts as outlined in the table below. (Also see the flow diagram which will aid decision making):

Risk Treatment (the 4 Ts)	
T . . .	**Description**
Terminate	Stop the activity causing the risk. For the constabularies this is likely to be difficult to achieve as many activities are mandated or operationally necessary.
Treat	Reduce the likelihood and / or impact of the risk to an acceptable level by applying appropriate controls and counter measures. The majority of risks will be addressed in this way.
Tolerate	The degree of risk is at an acceptable level, and you don't intend to take any further action(s). Risks may also have to be tolerated if there is limited / no ability to act; or the cost of any action is disproportionate to the level of benefit gained.
Transfer	Transfer the risk to another party, i.e. insurer or an external supplier. Some risks, particularly financial ones or risk to assets, may be addressed by taking out insurance or transferring to a partner agency or a contractor. However, the constabularies can pass on the activity (outsourcing the service) but not the legal responsibility (liability) or the accountability for ensuring that it is carried out correctly.

8.3 Flowchart for application of the 4Ts



9. Controls

9.1 Controls include any process, policy, device, practice or other actions which modify the risk.

9.2 The term mitigation is interchangeable with the term control.

10. Tolerance – this section currently applies to Norfolk SRR only

10.1 Risk Tolerance is a standard risk management term that is easier to understand if described as *In*tolerance. It refers to risks that are outside of our risk tolerance and that the Constabularies have the capacity to control. In other words, risks that the Constabularies do not want to tolerate.

10.2 The current risk tolerance level is for any risks scoring up to and including 8, indicated by the black line on the matrix below (10.3). These risks are within tolerance and are considered to be controlled to a satisfactory level.

10.3 Risk Score Matrix with Tolerance Level:

RISK SCORE MATRIX		LIKELIHOOD			
		Remote Possibility (1)	Possible (2)	Likely (3)	Almost Certain (4)
IMPACT	Critical Impact (4)	4	8	12	16
	Serious Impact (3)	3	6	9	12
	Marginal Impact (2)	2	4	6	8
	Negligible Impact (1)	1	2	3	4

10.4 Risks within tolerance do not have to be controlled any further.

10.5 Risks scoring above 8 (outside of tolerance) should, where feasible and affordable, have additional controls applied to them to bring them within risk tolerance.

10.6 Tolerance Level and Response

Mitigated Risk Score	Within Tolerance	Response
1 – 6	Yes	No further controls required.
8	Yes	No further controls required.
9 – 16	No	Where feasible and affordable, additional controls should be applied to bring within standard risk tolerance (mitigated score of 8 and below).

10.7 If agreed by chief officers, a greater or lower level of risk tolerance can be applied.

10.8 Applying Non-standard Risk Tolerance Levels and Actions

Tolerance Level Applied	Description	Action
Lower	Management have a lower level of risk tolerance	Further controls applied to reduce risk to the desired level
Higher	Management have a greater level of risk tolerance	No further controls required. Score can remain at the level agreed.

10.9 The SRR entry should be updated accordingly.

10.10 It is envisaged that the use of risk tolerance will be rolled out wider, as a pre-cursor to the application of risk appetite.

11. Appetite

11.1 Risk Appetite looks at the pursuit of risk to achieve objectives – identifying what risks the organisation is prepared to take in pursuit of its goals.

11.2 As the constabularies' approach to risk management matures, it is envisioned that the setting and application of risk appetite will be introduced. This would involve consulting with chief officers to understand and then set an appetite statement that can be used to guide decision making. It is widely accepted however that Risk Appetite is a complex area, and the organisation would benefit from a gradual / carefully considered introduction of the concept. As the IRM Risk Appetite & Tolerance Guidance paper suggests: *'Risk appetite can be complex. Excessive simplicity, while superficially attractive, leads to dangerous waters: far better to acknowledge the complexity and deal with it, rather than ignoring it'.* The

current focus is on the introduction of Risk Tolerance, and once this is successfully embedded Risk Appetite will be progressed.

12. Recording

12.1 The Constabularies currently use the following risk templates to capture the identification and assessment of risks and aid decision making, monitoring and review:

- Strategic Risk Register (SRR) for the reporting and management of high-level risks that, should they occur, would impact upon the organisation's ability to deliver its high-level vision / plan.
- Risk and Issues Logs: used to record command/departmental organisational risks.
- Programme and project Risk, Assumption, Issue and Dependency (RAID) Logs: used to capture risks, etc. that may threaten programme delivery or cause disruption to the delivery of a project. These risks are co-ordinated by the Portfolio Management Office (PMO).
- Ad hoc registers can also be produced if required.

12.2 The respective risk owners, risk SPoCs, head of command/department or project managers are responsible for ensuring the maintenance of the above.

12.3 Each template includes details of the risks, owners, scoring, treatment and status (except SRR) and current and future controls.

13. Monitoring

13.1 Ongoing monitoring should support understanding of whether and how the risk profile is changing and the extent to which internal controls are operating as intended, in order to manage risks to an acceptable level for the purpose of achieving organisational objectives (Orange Book).

13.2 The Risk and Compliance Manager reviews the R&I Logs on a bi-monthly basis to check for compliance. Updates and new risks that have been raised are also reviewed for consistency and quality.

13.3 Each command/department Senior Leadership Team (SLT) should ensure the R&I Log is reviewed on a monthly basis to ensure controls are still in place/on target for delivery, and that the scoring and controls are still appropriate, and then update as required.

13.4 Risks scoring nine and above should be reviewed on a monthly basis until management are satisfied that controls are in place or future delivery is assured, or as and when required if being tolerated, or when changes or issues with controls occur. Longer review periods can be utilised if controls are in place or future delivery is assured.

13.5 Risks can also be reviewed at longer periods if the risk is low (less than 9), the controls are stable, the risk is being tolerated or there is no further treatment available.

13.6 The SRRs are reviewed by the Risk and Compliance Manager before submission to chief officer meetings. They are then reviewed by chief officers (risk owners) and updates agreed/applied.

13.7 Chief officers, the PMO and Organisational Analysis Team (including the Risk and Compliance Manager) monitor the internal and external environment for significant changes that could give rise to new strategic risks, provide additional controls or effect current controls that are in place.

14. Reporting

14.1 Risks scoring nine and above are reported to chief officer meetings.

14.2 The SRRs are reported to respective Chief Officer management meetings.

14.3 The SRRs are also reported to Norfolk OPCC Audit Committee, and Suffolk OPCC Accountability and Performance Panel.

14.4 The Risk and Compliance Manager oversees the reporting to the above meetings.

15. Escalation / Aggregation of Organisational Risks

15.1 The Risk and Compliance Manager reviews the R&I logs on a bi-monthly basis and will highlight any risks that require escalation. Managers can also escalate risks to department heads via internal departmental processes and via SLT.

15.2 Project risks are escalated via the highlight reporting process and scrutiny of RAID logs by the PMO. The Risk and Compliance Manager attends the six weekly PMO briefing to highlight current and emerging risks and themes.

15.3 To enable the aggregation of risks, the Risk and Compliance Manager reviews the R&I logs on a bi-monthly basis. As part of the reporting to chief officer meetings the risks are collated into one document. The Risk and Compliance Manager also reviews the FMS statements and the evergreen updates, and the gap analysis produced as a result.

15.4 The Risk and Compliance Manager monitors the R&I Logs and SRRs for patterns and themes. Each business area/command/department should monitor their area of business for patterns in operational events and include in the R&I Log in consultation with the Risk and Compliance Manager as appropriate. Key business areas such as PSD, H&S, L&D, Legal are also able to escalate any risks or issues to the respective R&I Log.

15.5 The Risk and Compliance Manager meets with the Business Continuity Manager on a bi-monthly basis to consider any changes to the internal or

external environment. Any new risks will be put forward to the relevant head of department/manager by the Risk and Compliance Manager.

16. Escalation of Operational Risks

16.1 Operational risks are covered by National Decision Making Model and the Risk Authorised Professional Practice (2013). The functions primarily concerned with their management are Health, Safety and Wellbeing, Learning and Development, Professional Standards Department and Norfolk Legal Department. Where there is the potential for an operational risk to have an organisational impact it can be escalated and included in the relevant R&I Log via the existing management structures. Although much less likely to occur, they may also be included in the SRRs via consultation with the Risk and Compliance Manager and relevant SRR risk owner, if it is deemed that they could have an impact on achieving strategic objectives.

17. Risk Closure

17.1 Strategic risks can only be closed off by the risk owner and with the agreement at the relevant chief officer meeting. The Risk and Compliance Manager will have oversight as part of the reporting process and should be consulted first. The change will then be reported to the relevant OPCC committee / meeting for oversight via the reporting structure in place.

17.2 When closing a command/departmental risk within the respective R&I Log the risk owner or command/departmental head should change the status to 'closed' and highlight this in blue. The Notes/Updates column must be updated with the rationale, who has closed it and the date. If applicable, the change should then be highlighted by the risk owner to the Head of Command/Department for agreement. Once closed it should be left until it has been reviewed by the Risk and Compliance Manager who will then filter it out (see 16.3 below).

17.3 Closed risks should not be deleted as it is important to keep an audit trail and they could need to be reopened. The column filter within the R&I Log will be used to hide closed risks and closed risks within the SRR will be greyed out and eventually hidden but not deleted.

18. Oversight, Scrutiny and Moderation

18.1 The three lines of defence model ensures there is oversight and scrutiny in place. The risk management roles and responsibilities within the model and across the organisations are as follows:

- **First line**: Risk owners, managers, senior managers
- **Second line**: Risk and Compliance Manager
- **Third line**: Internal Audit

18.2 The Risk and Compliance Manager reviews the R&I Logs on a bi-monthly basis to check for compliance. Updates and new risks that have been raised are also reviewed for consistency and quality.

18.3 Risks scoring nine and above are reported to chief officer meetings. A report including all risks scoring nine and above is also provided to the PMO Briefing for oversight and scrutiny.

18.4 See also Section 14 Reporting, and the Risk Management Policy: Section 5 Oversight and Governance, and the policy definitions.

19. Training

19.1 The policy and procedure documents provide guidance on how to undertake risk management within the Constabularies. They are published on the Constabularies' intranet and internet sites and are available to all.

19.2 As required/appropriate the Risk and Compliance Manager works with practitioners and leaders on a one to one basis to develop the organisational skill set.

19.3 The R&I Logs and SRRs contain additional guidance within the guidance tab and instructions within the column headers, e.g. how to write a risk description, what to do when closing a risk, etc.

19.4 The SBOS intranet pages contain a specific area for risk management.

19.5 New senior leaders will receive an invite to have a 1:1 regarding the risk management policy and procedure with the Risk and Compliance Manager.

20. Continual Improvement

20.1 Risk management shall be continually improved through learning and experience. (Orange Book)

20.2 The Risk and Compliance Manager will annually review the risk process (and framework) to address internal and external changes, thus ensuring it remains fit for purpose and supports the achievement of the Constabularies objectives and those set out in the risk management policy.

20.3 It is intended that the FMS evergreen approach will be utilised (approx. May each year) to review and set the Constabularies risk appetite(s) as applicable.

20.4 The risk management policy and procedure will be routinely monitored and reviewed by the Risk and Compliance Manager, the Central Policy Unit and internal audit to ensure it remains fit for purpose and supports the achievement of the objectives set out in the policy.