PROCEDURE

PROCEDURE
MONITORING AND REVIEW OF RISK

Owning Department:	Corporate Development and Change		
Department SPOC:	Risk and Compliance Manager – Marina Harlow		
CPU Lead:	Helen Connors		
Governing Policy:	Risk Management		
Risk Rating:	N/A	Legal Sign Off: Date:	N/A N/A

Approved by

JNCC:	04.12.18		
Published Date:	05.12.18	Review Date:	05.12.22

Index

1. Summary of Changes

1.1 This is a new joint policy and procedure for risk management.

1.2 This policy and procedure replaces the following policy;

- Risk Management Policy (2016)

2. Aim

2.1 This procedure outlines the risk management framework for Norfolk Constabulary and Suffolk Constabulary (the Constabularies). It describes the processes required to successfully deliver the joint risk management policy and defines the roles, responsibilities and practices which ensure 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 both organisations.

3. Risk Definition

3.1 Risk is defined by the International Standards Organisation (ISO 31000) as:

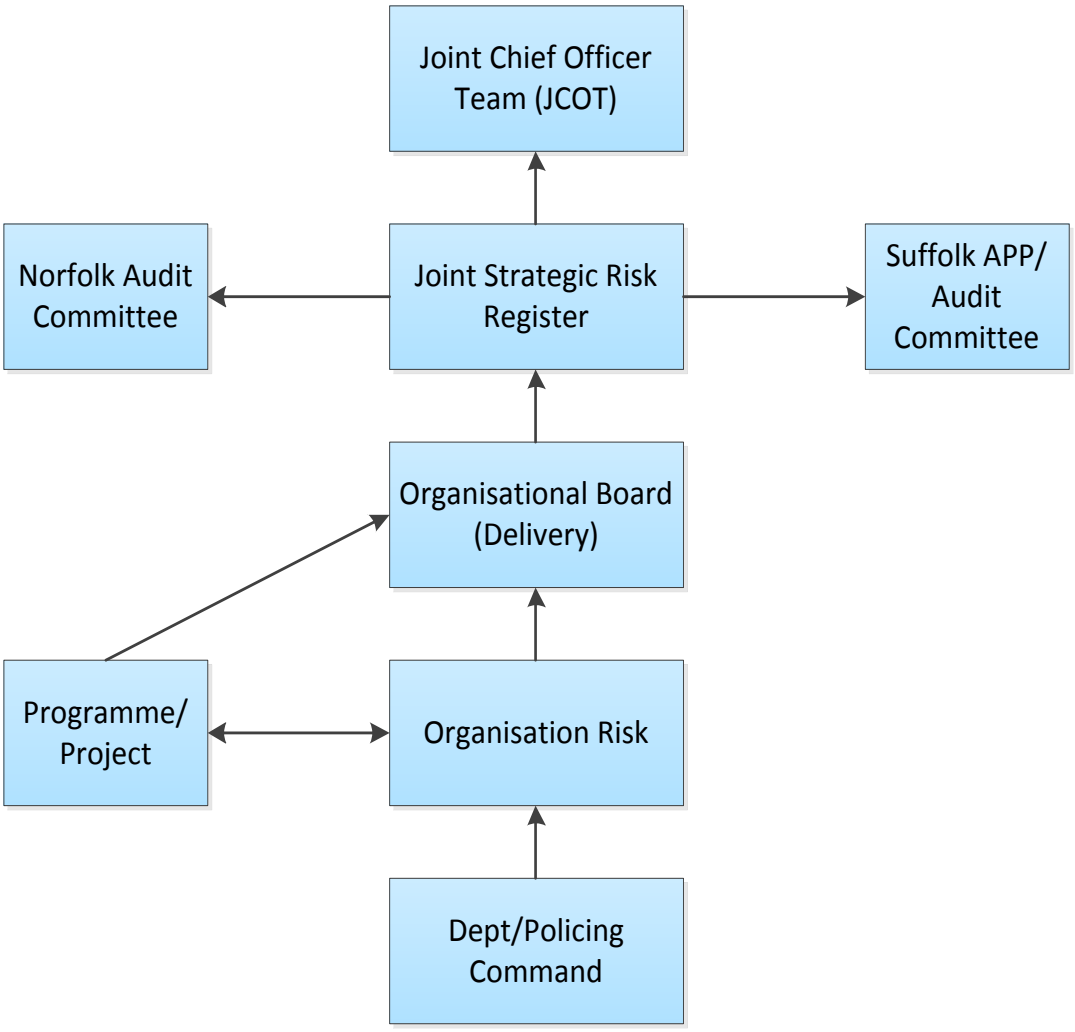
"The effect of uncertainty on objectives, the effect can be positive (opportunity), negative (threat) or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence".

3.2 The effective management of risk is critical for any organisation to ensure that it maintains its services and continues to progress effectively towards achieving its strategic aims.

3.3 Risk management is the planned and systematic approach to the identification, assessment/evaluation and management of risks in order to achieve operational effectiveness, continuous improvement and to 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. Risk Reporting Structure

4.1 The current risk reporting and escalation process for organisational risks is shown below:



4.2 The risk reporting process involves:

- Bi-monthly review and submission of departmental/policing command risk registers.
- Review and analysis of all risks by the Risk & Compliance Manager.
- Organisational/operational risk register compiled from risks within the departmental risk registers.
- Higher level risks (red and 9 amber) are submitted for consideration and discussion at the bi-monthly Organisational Board (Delivery).
- Risks with a significant impact or likelihood organisationally or key red risks are escalated to the Joint Chief Officer Team (JCOT) via the Joint Strategic Risk Register.
- Quarterly submission of the Joint Strategic Risk Register is made to Norfolk Audit Committee and Suffolk Accountability & Performance Panel (APP) Meeting.
- Joint audit and compliance review by internal auditors (TIAA).

5. Risk Management Process

5.1 The diagram below shows the key elements that make up the overall risk management process which should be used for the identification, assessment, evaluation and treatment/control of a risk should it occur. This is the information used to articulate and manage risks within the risk registers.

5.2 The risk management process is designed to support both Constabularies in the delivery of their strategic and operational objectives, the Vision, Mission and Values and the Norfolk PCC and Suffolk PCC aims and objectives within their respective Police and Crime Plans. Potential risks should be identified against these objectives, as a result this concept can quite easily be used against departmental or personal aims or objectives.

6. Risk Identification

6.1 It is the responsibility of all managers and staff at all levels to be aware of the risks they face while undertaking their day to day activities. Once a risk has been identified, it can be added to a risk register that acts as an audit trail of decisions and actions taken which in turn can be used to assist in assessing priorities and allocation of resources.

6.2 Identifying risks is something everyone does automatically, every day and can be seen as a tool used to demonstrate:

- You have thought what could go wrong or what unforeseen event could occur;
- You have taken steps to stop it from happening;
- That any additional resources or action to be taken has been identified.

6.3 Risks can be aligned to the following:

- Force Vision, Mission and Values
- Operational and Strategic Objectives
- Police and Crime Plan Objectives and Aims
- Any key risks associated with the operational policing model, Strategic Assessment, National Decision Model, THRIVE principles etc.
- HMICFRS reports, Force Management Statement (FMS), Internal and External Audit reports, Internal Controls
- Compliance with Statutory Requirements and Recommendations
- Key Financial Risks or Performance Activity
- Partner Organisations or External Agencies i.e. Ambulance Service, Courts etc.

6.4 When describing a risk you are telling a story in three parts:

- The risk source (or causes) – in other words, the risk itself.
- The uncertain event and the consequences.
- The effects of the risk on the organisation.

6.5 Risk is the combination of a **source / cause** of risk and an **event / threat** that gives rise to a **consequence / effect** which might be considered as abnormal.

6.6 Risks may be positive (opportunity) or negative (threat). Think:

Cause ⇨ Threat ⇨ Consequence
or
Source ⇨ Event ⇨ Consequence

6.7 To correctly describe a risk, the **cause / source** together with the **event / threat** and **consequence** should be stated.

- The **source / cause** is the intrinsic thing which may cause harm.
- The **event / threat** is the 'something' that could occur that would give rise to the risk.
- The **consequence** is the outcome or impact of the risk.

Example:
A garage may run the risk of a catastrophic release (consequence) of flammable liquid (source) if an earthquake (event) ruptures the four hundred tonne tank of petrol being stored on the forecourt.

Example:
A spark (event) from a non-flameproof electrical switch may ignite (consequence) the flammable liquid (source) which has been released from the storage tank.

6.8 Ideally, a description of risk will also contain within it, **when** and **where** the event could occur.

Example:
Our reputation will be sullied (consequence), if we do not react within the first hour (when) of a hazardous liquid spill (event) in our factory (where) in immediately getting information to the public in order to stop misinformation (source) spreading.

6.9 It is not necessary to put all of this into one sentence. What is key is to ensure the risk and its actual impact on the department and/or organisation is properly described.

<u>Articulation of Risk:</u>

6.10 Examples of typical wording of individual risks:

The risk is……

The risk of……could lead to

Inability to……..

Reduction of……

Failure of / to……..

Lack of…….. could lead to…….resulting in……..

Threat of…….could result in……..

Possibility of…….

Reduction of……

Increase in……..

Lack of…….

Example:
Failure of uninterrupted power supply could lead to inability to power up computer systems during a power outage resulting in personnel unable to use the computer systems to undertake their normal duties.
Insufficient training in the use of hazardous machinery may lead to inappropriate use by staff resulting in possible injury.

Risk vs. Issue – What's the Difference?

6.11 The formal definition of risk is the 'effect of uncertainty on objectives', whether the effect is a positive opportunity or a negative threat.

6.12 Think of it as:

- An **issue** is a problem *today*
- A **risk** *may* become a problem in the *future,* it hasn't yet occurred but it may.

6.13 A risk is a 'future event' that could have an impact on organisational objectives. It may happen or it may not. You can plan for a risk based on its likelihood and potential impact – risks can be avoided completely, minimised and tolerated, transferred to another party or dealt with by controls and strategies to deal with their effect.

6.14 An issue is a 'present problem or concern influencing organisational objectives' – it has already occurred and is affecting our objective at the present time. In other words, an issue is raised when something has gone or is going wrong.

When does a Risk become an Issue?

6.15 A risk could become an issue if it materialises – when you can no longer stop the impact, it is an issue.

Example:
You are planning to travel to an all-day meeting which is some distance away by train as your car is out of action. However you have heard the train drivers may go on strike

within the next week. This is a **risk**! You know it might happen so you have the opportunity to manage the risk.

You may decide to minimise the risk by investing in a bus timetable, seeing if there are any lift sharing options travelling with a colleague or hiring a vehicle. Therefore if the strike does occur you can still get to the meeting and achieve your objective – you have put in place a **mitigating control** or action.

You go to the meeting and whilst there receive a text saying the train drivers have in fact gone on strike! You now have an **issue** which you must resolve – the potential risk has become an issue as it has occurred. You therefore have to catch the bus home!

7. Types of Risk

Type of risk	***Explanation***
Strategic	This is a risk requiring review and intervention at a strategic level due to the potential scale of impact on priorities and resources and/or where action to address the risk cannot be adequately provided by the command or department.
Command/ Departmental	This is a risk which may have a significant impact on the command or department's capability to address force priorities and action to address the risk lies within the remit of the command or department.
Programme	This is a risk requiring intervention at a programme level due to the potential scale of impact on priorities and/or resources and action to address the risk cannot be adequately provided at project level.
Project	This is a risk which may have a significant impact on the delivery of the project however action to address the risk lies within the remit of the project.

Operational Risk

7.1 Although the focus of this procedure is around 'business', 'organisational' or 'strategic' risks, operational risk is a key and important factor in the day to day business of policing. Operational threat, risk and harm is identified in line with the Strategic Assessment but not in line with 'business' risk due to the differing nature and impact it has, along with the more localised considerations and intelligence that is required for assessment.

7.2 However, where appropriate, operational risk relating to an area of business should be recorded under a departmental risk register in line with the scoring and assessment outlined above and as set out within the joint risk management policy. It should be escalated through the risk management process where there is a potential for it to have an organisational as well as operational impact.

8. Risk Register

8.1 The risk register is the tool used to hold all the information and details of each risk. It identifies:

- The department.
- Category / type of risk.
- Date the risk was first identified.
- Risk description.
- Risk owner.
- Initial scoring of the risk likelihood/impact at its inherent level ie. the level of risk at the time it is entered onto the risk register and before any controls or mitigation action has been taken.
- Details of the control(s) or counter measures taken to manage the risk to an acceptable level and within the risk appetite. The controls should be specific and measurable – not just updates on any action taken.
- The secondary level of risk likelihood/impact score ie. the residual or current level of risk. This scoring is important as it will show whether or not the controls taken are working to bring down the risk likelihood and/or impact. If the residual risk score remains the same as the inherent then further controls or action plans will need to be considered in order to bring down the risk to an acceptable level.
- Risk control response, i.e. the 4T's - Treat, Tolerate, Terminate or Transfer (see Section 11).
- Risk status – live, new or closed.

8.2 The risk registers are maintained at departmental/local policing level and these are used to feed into the organisational risk register and ultimately depending on the nature and seriousness of a particular risk, the Joint Strategic Risk Register.

8.3 The Constabularies currently operate the following risk register templates:

- Joint Strategic Risk Register for the reporting and management of significant risks which threaten or enhance the long term achievement of corporate objectives. These risks could also cause reputational damage or operational/organisational disruption;
- Organisational Risk and Issues Register for the reporting of all organisational risks escalated from departmental or command risk registers and encompassing all organisational risks including information management, health and safety and business continuity related risks.
- Programme and Project Risk, Assumption, Issue and Dependency (RAID) Logs for the reporting risks that may threaten programme delivery or cause disruption to the delivery of a specific project. These

risks are managed by the Programme Management Office (PMO) working with the Risk and Compliance Manager to ensure risks of a significant nature are captured and reported through the Organisational Board.

8.4 By bringing all the relevant information together in a single format, the risk register allows all staff, managers, chief officers, auditors and external inspectors to see the overall risk situation at any given time as well as future plans and historic progress.

9. Risk Assessment

9.1 Once identified, risks will need to be rated on the basis of the likelihood of the risk materialising and the impact this would have should the risk occur – see definitions and matrix below – the criteria for assessing risk areas are defined by using a 4 x 4 matrix.

9.2 It is recognised that rating a risk is not an exact science and should be informed by evidence where possible ie. economic forecasts, trends, historic information/events etc., however it is also about applying collective professional knowledge and judgement and the active consideration of the likelihood and impact of a risk materialising that is also important.

9.3 The purpose of rating a risk is to focus attention to ensure appropriate and proportionate controls and mitigation plans are in place.

DEFINITION OF IMPACT SCORE

		SERVICE DELIVERY	FINANCIAL	STRATEGIC	REPUTATION
1	Negligible	Negligible service disruption No impact to any key services/objectives Negligible public dissatisfaction	Negligible financial impact (<1% of budget/cost savings)	Negligible deviation from strategic direction. Negligible impact on strategic aims or delivery plan	No Impact
2	Marginal	Limited service disruption Minor public/partner dissatisfaction No impact on key services although may impact on minor services	Minor financial impact (2-3% of budget/cost savings)	Minor deviation from strategic direction. Minor impact on strategic aims and delivery plan	Little impact inside or outside the force itself
3	Serious	Significant service/dept disruption Noticeable public/ partner dissatisfaction Impact on some services/some key objectives or targets are not met	Measurable financial impact (3-4% of budget/cost savings)	Medium term and serious deviation from strategic direction, aims and delivery plan. Measurable impact on strategic direction	Negative local or regional media coverage. Regional public/political concern.
4	Critical	Major service disruption	Severe financial impact (>5% of budget/cost savings)	Long term severe deviation from strategic direction, aims and delivery plan. Long term impact on strategic objectives Significant recovery time required	Long term local, regional or national media coverage Major public/political concern Possible public or other enquiry

DEFINITION OF LIKELIHOOD SCORE			
No	**DESCRIPTION**	**PROBABILITY**	**LIKELIHOOD**
1	Remote Possibility	5% - 20%	No indication that the risk or event will happen or very likely at the current time
2	Possible	20% - 50%	The risk or event could occur within certain circumstances (remote chance and level of uncertainty that it will not)
3	Likely	50% - 80%	The risk or event is more likely to happen than not (moderate chance)
4	Almost Certain	80% or more	The risk or event is expected to occur or occurs regularly (very significant chance it will happen)

Risk Score Matrix		**LIKELIHOOD**			
		Remote	**Possible**	**Likely**	**Almost Certain**
IMPACT	**Critical**	4	8	12	16
	Serious	3	6	9	12
	Marginal	2	4	6	8
	Negligible	1	2	3	4

LIKELIHOOD X IMPACT = RISK SCORE

High (critical)	Implement immediate control measures and take action to reduce or eliminate risk. Risk to be managed at appropriate management meeting with consideration at Organisational Board. Consider whether risk should be escalated to the Joint Strategic Risk Register.
Medium (Serious)	Implement control measures to reduce and manage risk. More than one control may be used. All controls should be regularly assessed (monthly) to ensure they remain relevant and cost effective.
Medium/Low (Marginal)	Implement control measures to reduce risk and frequently review risk circumstances, controls and monitor any changes to the level of risk severity. Consider whether risk needs to be escalated to next level.
Low (Negligible)	No immediate action. Risk should be recorded on risk register and monitored at departmental/project manager level.

10. Risk Appetite

10.1 Risk appetite can be described as the amount of risk an organisation is willing to accept, tolerate or be exposed to at any one point. The concept of a risk appetite is key to achieving effective risk management and it is essential to consider before moving on to consider how risks can be controlled.

10.2 The level of risk may change within the organisation, depending on whether risks are speculative or mission critical, i.e. the Constabularies may tolerate a higher degree of risk for business benefit opportunities over business critical projects.

10.3 The organisational risk appetite for the Constabularies has currently been agreed as risks rated at 12 and above. This essentially means that action must be taken to proactively manage the risk. What is considered a high level of risk at one level is likely to be a lower level of risk to a higher level of management. This facilitates a risk escalation process for the taking of risk decisions and ensures appropriate delegated authority within the business area. All risks must be assessed using the 4x4 Risk Assessment Matrix and should be considered for impact on an organisation-wide basis.

10.4 Using the traffic light system to clarify:

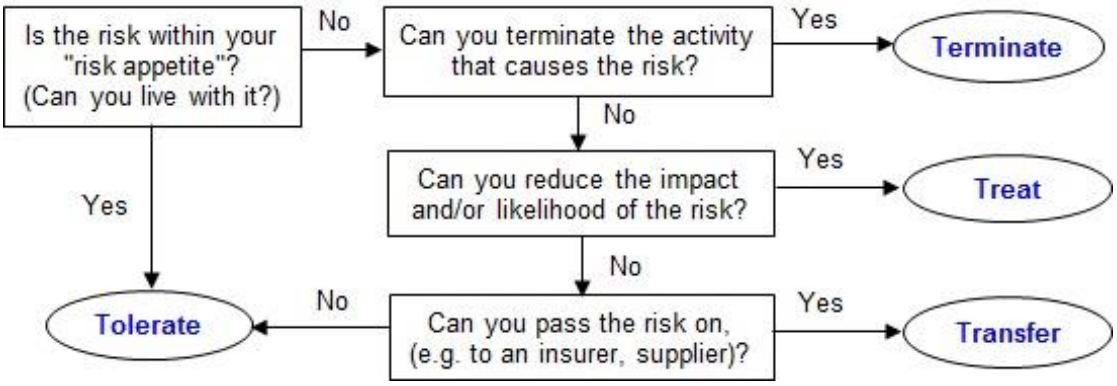
Red	These risks are not acceptable, as their combination of likelihood and impact is too high for the Constabulary to bear. These risks fall outside the risk appetite.
Amber	These risks should be reduced to a manageable level and are tolerable if a reduction is achieved. These risks therefore fall within the risk appetite.
Yellow	These risks are tolerable but further mitigations should be considered to further reduce the level of risk. These fall within the risk appetite.
Green	These risks are acceptable at the present time but should be regularly monitored. They have such a low score that should they occur their effect could be managed. These fall within the risk appetite.

11. Risk Control / Treatment

11.1 Once a risk has been assessed and scored, consideration then needs to be given what controls or mitigations need to be put in place to reduce the level of risk to a more manageable level. If initial action is failing to reduce the likelihood or impact of the risk, then further controls will need to be considered and be part of the risk review process. Care should be taken to ensure any additional controls remain cost effective to the actual level of risk.

11.2 Having determined the control and mitigation strategy to implement, the appropriate control actions need to be taken and these are known as the 4Ts:

- **Terminate** - the activity that causes the risk.
- **Treat** - the likelihood and/or impact to reduce the risk to an acceptable level.
- **Tolerate** – the risks which are acceptable and within tolerance or appetite levels.
- **Transfer** - the risk to another department or party (i.e. insurance).



Terminate the Risk

11.3 Some risks can only be addressed by terminating the activity that generates the risk. Whilst this option will not be appropriate for the majority of operational police activity, it can be of benefit in project management where anticipated outcomes or benefits are jeopardised by the risk.

Treat the Risk

11.4 The risk will be reduced from its current level with the application of appropriate controls and counter measures and regularly reviewed. The majority of risks will be addressed in this way.

Tolerate the Risk

11.5 This option may be considered where the degree of risk exposure is at an acceptable level (control/counter measures may already be in place) without further action; or where the ability to take action is limited; or the cost of any action is disproportionate to the level of benefit gained. If chosen, this option may be supplemented with a contingency plan to minimise any impact that might arise if the risk is realised.

Transfer the Risk

11.6 Some risks, particularly financial ones or risk to assets may be addressed by transferring to another department, a partner agency or a third party ie the contracting out of a particular service or taking out insurance. It should however be remembered that many legal liabilities cannot be avoided simply by having someone else carry out an activity. For

example you can pass on the activity (outsourcing service) but not the legal responsibility (liability) or the accountability for ensuring that it is carried out correctly.

Direction of Travel

 Reducing

 No Movement

 Increasing

Remember - all risks can be:

Treated by applying further controls
Tolerated but still monitored
Transferred to another department/insurance/party
Terminated when suitably mitigated

12. Residual Risk Assessment and Review

12.1 Once control or counter measures have been reviewed, then consideration of the residual or current risk score need to be undertaken. This is the actual level of likelihood and/or impact of the risk after the control(s) has been applied. This stage also acts as an assessment whether the mitigations in place are actually working or whether a change in action is required.

12.2 All risks should be monitored and regularly reviewed to ensure that the degree of likelihood or impact has not increased. The following questions should also be addressed:

- Is the risk still the same? (has the environment changed, are the scores still appropriate?)
- Are the controls/counter measures or planned actions still relevant and appropriate?
- What progress has been made in implementing those controls/actions?
- Has the cost of controls/actions been considered (i.e. time, cost, people, equipment etc.)

13. Policy and Procedure Monitoring and Review

13.1 The risk management policy and procedure will be routinely monitored and reviewed by the Risk and Compliance Manager, the policy team and internal audit to ensure it remains applicable and compliant with relevant organisational and legislative changes and requirements.

13.2 Compliance with this policy and procedure is monitored through the Organisational Board.

13.3 The Risk and Compliance Manager, working with internal audit, is responsible for reviewing this policy on an annual basis.

14. Communication and Training

14.1 To support the risk management process, an ongoing communication programme is in place to ensure that all officers and staff understand the joint force policy and procedure on risk management, what the risk priorities are and to promote individual awareness of risk and risk management.

14.2 In addition those individuals with specific key roles and responsibilities will receive additional guidance and training to ensure they are fully familiar with the risk management process and have the necessary knowledge and skills to enable them to identify, assess and manage risks.

14.3 Details of the communication and training programme can be found via the risk management section on the Intranet.