LINCOLNSHIRE POLICE

Risk Management Plan
2019-2022

Building Trust and Confidence by:

- Reducing Crime
- Providing a fair deal for the people of Lincolnshire
- Policing and services that are there when you need them

Lincolnshire POLICE
policing with PRIDE

Professionalism | Respect | Integrity | Dedication | Empathy

Contents

Page

Section 1: Introduction....3
Aim....3
Defining Risk....3
Corporate Governance....4
Risk Assurance....4
Section 2: What Risk Management Means To You....5
Section 3: Risk Levels and Escalation....6
Management of Confidential Risks....8
Identification and Management of information on Confidential Risks....8
Confidential Risk Board....9
Confidential Risk Management Process....10
Section 4: Roles and Responsibilities....11
Deputy Chief Constable....11
Joint Independent Audit Committee and the Office of Police and Crime Commissioner....11
Chief Officer Group....11
Risk Management Board....11
Senior Management Teams....12
Risk, Policy and review Officer (RPRO)....12
Strategic Partner....12
Section 5: The Risk Management Process....13
Risk Identification....13
Analysis of the risk....14
Evaluate the risk....15
Treat/respond to the risk Plan the response....15
Risk controls and Appetite....15
Risk Controls....16
Risk Responses....16
Implementation....17
Monitoring and Review....17
Making sense of risk scoring....17

Not Protectively Marked

Section 6: Operational Risk 18
The National Decision Model 19
ACPO 10 Principles of Risk 19
Section 7: Partners and Regional Collaboration 20
Section 8: Additional Information and Guidance 20
Appendix A: risk management board 21
Appendix B: Risk Management Process 2016-2019 24
Appendix C: Risk Scoring Matrix 25
Appendix D: National Decision Model: Aide Memoir 27

SECTION 1: INTRODUCTION

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.

As a public organisation, Lincolnshire Police is responsible for providing effective and efficient policing for Lincolnshire. It is committed to identifying and dealing with the risks it faces, both business and strategic risks, and operational risks and threats.

With continued developments in our risk management processes such as alignment with those of the Office of Police and Crime Commissioner, further risk training for staff and officers the force will be able to manage risks more effectively as a result of increased awareness allowing for better comparison and prioritisation of risk.

Aim

The aim of this strategy is to set out the Lincolnshire Police approach to risk management and define the roles and responsibilities involved within the process. It is just one of the tools used to provide assurance that we are operating our business using sound corporate governance principles.

The Strategy enables the force to be proactive in its risk management processes and receive the benefits of early identification of risks, along with the application of appropriate and targeted control measures.

Beyond ensuring resilience within its own risk management process, the force will continue to be actively involved in risk management groups and partnerships to further enhance its own processes and to contribute to the risk management processes of others.

Through the cohesive and collaborative risk management processes outlined within this strategy, Lincolnshire Police will continue to integrate and embed risk management into its core functions.

Defining Risk

Risk is defined as 'The effect of uncertainty on objectives. [1] Note – The effect may be positive, negative or a deviation from the expected. Also risk is often described by an event, change in circumstances or a consequence.

So the overriding purpose of risk management is to help organisations to identify, understand and manage their risks and opportunities, and thereby increase the likelihood of achieving their objectives by reducing uncertainty. 'Risk management is a core management discipline. Like general management or project/change management, risk management is a discipline that supports all organisational activities. The risks that organisations face change all the time, so the art of good risk management is to combine planning for what we already know has happened and might occur, with preparation for unknown situations.

[1] International Organization for Standardization (ISO, 2009)

The focus of risk management in the force is on what could prevent us from achieving our strategic aims, tasks, key functions or prevent us from offering the correct level of service to the public and our partners.

Corporate Governance

Corporate governance is the authority by which the force is directed and managed and is defined as the 'ongoing activity of maintaining a sound system of internal control'. This is controlled and directed at an organisations most senior level to ensure effective management systems are in place to protect the organisation and its reputation.

Good governance allows organisations to do the right thing, in the right way, for the right people, in a timely, open, honest and accountable way. It is vital to effective risk management.

Risk management is central to effective corporate governance and relies on the production, maintenance and use of realistic and robust risk registers.

Risk Assurance

Risk registers are a key tool in providing assurance to the force and to the Police and Crime Commissioner (PCC) that risks are being managed effectively. Assurance is achieved through the regular and continued review of the force risk register at the Risk Management Board, and the Joint Independent Audit Committee.

The PCC and Force maintain a comprehensive and effective assurance map for the purpose of assuring on established mitigations and scoring of strategic risks. The assurance map is based on the three lines of defence approach and is suitably comprehensive and effective for the purpose of assuring on established mitigations and scoring of strategic risks.

The purpose and aim of the Assurance map is to provide an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management and control processes for the organisation. Also to facilitate escalation of risk and control issues requiring visibility and attention by senior management, by providing a cohesive and comprehensive view of assurance across the risk environment.

In addition to these internal assurances, there are external organisations such as Internal and External Auditors as well as Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) that work with the force and the Office of Police and Crime Commissioner (OPCC) to ensure that the risk management process is effective and robust.

SECTION 2: WHAT RISK MANAGEMENT MEANS TO YOU

Risk Management is a process to help manage your work by identifying what may go wrong and the actions you could take to prevent this from happening, or to take full advantage of emerging opportunities presented by the risk.

By carrying out risk assessments on your area of work, you can request that risks identified are added to a risk register that acts as an audit trail of decisions and actions which can be used to assist in assessing priorities for allocation of resources.

It also demonstrates support of the corporate governance structure of the force and can be used as effective evidence to support any planning and financial assumptions.

Risk management should be seen as a tool, creating an audit trail to demonstrate:

a. that you have thought about areas within your business that could be improved or processes that could be made more effective and efficient;
b. that you have taken steps to; respond to, treat or control the identified areas;
c. that you have identified any additional finances and/or resources you might need; and
d. that you can prove the importance of allocating the additional finances and/or resources should you need them;

It should be an integral part of how you plan and manage your finances and resources to run your business area and achieve your objectives.

Acknowledging risks in advance places the force in a strong position to address them, and allows for the implementation of control measures prior to the risk occurring. This often results in saving significant finances and resources and contributes to elevated levels of public satisfaction.

Managers at all levels should be aware of the risks they face as part of their business so they can manage the effects of these risks through mitigation or, realise the benefits or opportunities they present.

Not Protectively Marked

SECTION 3: RISK LEVELS AND ESCALATION

The force risk management process focuses on five levels of risk which can pass through a process of escalation depending on the scale of risk and effect it may have at either: project, programme, department or force level.

Risk Level	Description
Force	• Risks at the highest level. • They are so significant that they threaten or enhance the long-term achievement of corporate objectives. • Will be discussed at Risk Management Boards, Chief Officer Group meetings and the Joint Independent Audit Committee. • Departments/Business Areas will escalate risks from their departmental risk register which have become force risks, through the Risk Management Board, for inclusion on the Force Risk Register.
Department/ Business Area	• Risks that threaten or enhance the delivery of department or business area objectives. • Will be discussed at Senior Management Team meetings. • Escalated up through the Risk Management Board if they pose a threat to corporate objectives and the Head of Department's limit of authority to manage the risk has been reached.
Programme	• Risks that threaten or enhance the delivery of a programme. • Will be analysed and scored in relation to the programme. • Will be discussed at Programme Board meetings. • Escalated through the Risk Management Board if they pose a threat to corporate objectives, and the Programme Managers limit of authority to manage the risk has been reached.
Project	• Risks that threaten or enhance the delivery of a specific project. • Will be analysed and scored in relation to the project. • If they are serious enough to impact on the Programme and the Project Manager's limit of authority has been reached, they should be escalated to Programme level.
Operational	• Risks concerning the day-to-day issues that Lincolnshire Police is confronted with as it strives to deliver its objectives. • Only escalated to the Force Risk Register if they pose a threat to corporate objectives

Not Protectively Marked

The below flow chart shows the process for escalation of a departmental risk onto the Force Risk register.

Process of Escalation

Not Protectively Marked

Management of Confidential Risks

Lincolnshire Police also maintains a Confidential Risk Register for those risks where it is not appropriate for them to be recorded on the Force Risk Register. The types of risk envisaged as falling within this category are those that would cause significant **operational**, **financial** or **reputational** harm to Lincolnshire Police or partners, **AND** where premature or unauthorised disclosure of the risk could significantly worsen the potential impacts. These would typically be classified as Official sensitive under the Government Security Classifications (GSC), but in exceptional circumstances could be a higher classification.

Confidential risks could include risks related to the potential, current and ongoing impact of tribunals, misconduct cases, legal cases, public inquiries, court cases and police operations. This list is not exhaustive and it is *not* intended to cover all such activities, but focuses on those issues that provide specific details of significant and imminent risks to the force and authority arising from such activities. For example high profile public inquests can take significant senior management resources from the force, and could have significant reputational impact, and this needs to be managed through a structured risk management process.

Identification and Management of information on Confidential Risks

Confidential risks, most of which will be classified above official will be securely stored by the Department Head. Details of risks deemed to be confidential will be stored in accordance with the GSC and stored separately from non confidential risks. Storage will be via a Confidential Risk drive, or manual files stored under lock and key.

The Risk, Policy and Review Officer will be advised of the existence of any confidential risks although summary details only will be provided in order to keep the risk as confidential as possible.

Confidential Risks will be collated from each department by the Risk, Policy and Review Officer and held on a central confidential risk log which will be held on a secure confidential risk drive. Any risks raised via the force Risk Management Board that the Risk Officer identifies should be made confidential shall entered onto the confidential Risk Register.

Any discussion relating to confidential risks will be restricted to a small group of individuals with a clear understanding of the sensitivities involved. The detailed files that underpin each risk will remain under the control of the appropriate person within the force.

Where the Deputy Chief Constable Judges that a risk is highly confidential then the management of that risk will fall to the Deputy Chief Constable and the risk owner alone. The Confidential Risk Register will record this fact, and the risk may only be identified by a unique risk number.

The Confidential Risk Register will be maintained and held by the Risk, Policy and review officer. This register will hold minimal information on specific risks in order to maintain confidentiality and the need to know principles.

Confidential Risk Board

A closed session of the current Risk Management Board will consider confidential risks. This group (is known as the Confidential Risk Board) will be chaired by the DCC. All the members of the Confidential Risk Board need to be security cleared to the relevant level and would be involved on a 'need to know' basis to maintain confidentiality as far as possible.

The Confidential Risk Board will uphold 'confidentiality' and 'need to know' principles. Information supplied in confidence, developed to produce intelligence, used to support operational initiatives or connected with other confidential business activities, will be treated in a confidential manner and only imparted to others in the official course of duties on a strict 'need to know' basis. This requirement is supported by legislation including the Official Secrets Acts, Data Protection Act, Computer Misuse Act and the Freedom of Information Act. It should be noted that the classification of confidential does not exclude information from the scope of any of these acts.

The Confidential Risk Board will meet on a quarterly basis and will take a view on the management of individual risks, whether the risk is still classed as confidential, the scoring and prioritisation of each risk, and who needs to be informed of the risk and any mitigating actions. The ultimate decision on management of confidential risks will reside with the Deputy Chief Constable as the Senior Responsible Owner.

Not Protectively Marked

Confidential Risk Management Process

Not Protectively Marked

SECTION 4: ROLES AND RESPONSIBILITIES

For risk management to be embedded within the force, all relevant staff should have an awareness of the risk management process and how to raise risks. This ensures a full range of risks facing the force can be accurately recorded and subsequently managed. Staff awareness also facilitates partnership development and sharing of risks.

Within the risk management process there are a number of roles and responsibilities which are key to the success of the risk management process.

Deputy Chief Constable

The force's risk register and process is owned by the Deputy Chief Constable (DCC). The DCC will take the lead for the management of risk ensuring that risk is managed effectively throughout Lincolnshire Police. The DCC chairs the Risk Management Board made up of representatives from the office of the PCC and other key stakeholders. The DCC will also act on behalf of the board at force executive meetings updating on organisational risks with a score of 8 and above.

Joint Independent Audit Committee and the Office of Police and Crime Commissioner

The Joint Independent Audit Committee maintains a strategic oversight of Lincolnshire Police's risk register and risk management practices which are reviewed at quarterly committee meetings. The Joint Independent Audit Committee (JIAC) provides independent assurance to the Police and Crime Commissioner and the Chief Constable regarding the adequacy of the risk management framework and the associated control environment.

The Office of Police and Crime Commissioner also has and maintains its own risk register which is reviewed at this meeting.

Chief Officer Group

The Deputy Chief Constable will present new risks to the Chief Officer Group by exception at their discretion, and any items that had been on the risk register for a lengthy period would be considered on a six monthly basis.

Risk Management Board

The Risk Management Board reviews the force risk register, ensuring areas of significant risk are identified, analysed, monitored and reviewed. The members of the board are responsible for quality assuring risk scores, the impact of control measures, and agreeing actions for developing controls. The Risk Management Board terms of reference are included within **Appendix A.**

Senior Management Teams

Senior Management Teams (SMT) will review business area risks, determine the suitability of new risks for inclusion on departmental risks registers, and assign risk owners, actions and controls to those risks. They will review their departmental risks monthly at their senior management team meetings. They will also recommend any risks to be escalated to the force risk register level if they pose a threat to corporate objectives, and the Head of Department's limit of authority has been reached. Each business area/department is supported by a Single Point of Contact (SPOC) who is responsible for collating risk information and maintaining the departmental risk register.

Risk, Policy and review Officer (RPRO)

The RPRO co-ordinates the force's risk management process on behalf of the DCC and offers guidance and support to departments and SMTs in following the process. The RPRO also:

- Facilitates the identification of new risks.
- Presents to the Risk Management Board:
  1) risks requiring their attention and action including,
  2) any recommended new risks,
  3) changes to risk scores,
  4) risks with no movement and not within tolerance.
- Assists in the maintenance of force-level risks through continued monitoring and reviewing the overall administration of the force and departmental risk registers.
- Develops and embeds risk management across the force.
- Conducts horizon scanning in order to identify new and emerging risks.
- Reviews implemented controls for force risks that are scored 8 and above on a monthly basis. Ad-hoc audits will also be conducted into the effectiveness of controls in place to mitigate any other risk, implementing an assurance frame work for risk management.

Strategic Partner

Recognising that the appointment of a Strategic Partner to provide a number of mid and back office functions changes the dynamic of risk management in these areas, a two pronged approach to risk management has been taken.

The senior management of each service within the Strategic Partnership is required to review business area risks, determine the suitability of new risks for inclusion on risk registers and assign risk owners, actions and controls to those risks in the same way that Force Managers are for their departments.

Secondly the Force lead in service provision (normally the Commercial Partnership Team) will consider risks associated with the service delivery by the Strategic Partner for inclusion on their Departmental and Force Risk Registers.

Not Protectively Marked

SECTION 5: THE RISK MANAGEMENT PROCESS

The risk management process provides a standardised framework for the whole life management of risk within the force and details the steps needed to form and maintain a risk register.

The force will follow ISO 31000 standard as the basis of our work.

Essentially it is a process used to assess all areas of work in identifying what could go wrong or what could prevent the achievement of objectives.

There are four key steps to the risk management process which are shown in the flow chart below.

All managers and staff should follow this process to ensure that the force maintains a consistent approach to the management of risk.

This will provide assurance that all risk registers contain a standard assessment of risk across the Force.

A detailed process map can be found at **Appendix B.**

Risk Identification

The initial step of the risk management process is to identify any potential risks facing a department, business area or the force that would reduce or remove the likelihood of achieving its objectives.

Risks can be identified by any member of staff working for Lincolnshire Police and should be formally raised through the correct channels, feeding into the risk management process at the appropriate risk level: Force, Department/Business Area, Programme/Project or Operational.

What is the difference between a risk and an issue?

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

On the surface, it's quite clear:

- an **issue** is a problem **today**
- A **risk** *may* become a problem in the **future.**

In practice it's not ALWAYS that simple to understand the difference between a risk and an issue. Many people struggle with the question *Is this an issue or is it a risk?*

A **risk** is 'a future event' that *may* have an impact on organisational objectives. It may happen or it may not. We can plan for risk based on its likelihood and potential impact – risks can be avoided completely, minimized, transferred to another party, or we can meet them head on with strategies to deal with their effects.

An **issue** is 'a present problem or concern influencing organisational objectives'. In other words, an issue is raised when something has gone or is going wrong and will affect the organisation.

A risk can become an issue, but an issue is not a risk because it has already happened.

When does a risk become an issue?

The answer to this question is not as simple as it seems. The short answer is – 'when you can no longer stop the impact, it is an issue'. This means that it doesn't actually have to impact to become an issue.

For example:

Suppose you are planning a holiday. You are going to fly to Italy, rent a car for two weeks, travel a bit and then return. You heard that your airline might go on strike. This is a risk! You know that it might happen and you now have a chance to manage the risk.

You might decide to minimize the risk by investigating ferry timetable, train timetables or other airlines, if a strike occurs, you can still go and achieve your objective of having a good holiday.

Now suppose you fly to Italy as planned and the airline go on strike before you can return. You now have an issue that you must resolve.

The potential impact on your objectives of the original risk didn't eventuate: you were able to fly to Italy and have a good holiday. However, you now have the issue of getting home.

Where an issue is identified then it is dealt with by the department or part of the force which is responsible or in the case of projects included on an Issues register and monitored by the project board.

Analysis of the risk

At this stage of the process, an assessment of the risk should be carried out by completing the Initial Risk Assessment form, which can be found on the intranet following this link Intranet - Risk assessment form .This will assist in developing a concise and clear account of the risk, its consequences and the level at which will be monitored.

Risk analysis helps us to determine the severity of the risks our organisation faces by analysing the likelihood of the risk materialising together with the severity of the impact on the organisation.

Risk analysis focuses in particular on the two dimensions of risk analysis, which are risk likelihood and risk impact.

When scoring risk a consistent method is used across the force, which is also aligned with our regional forces and the Office of Police and Crime Commissioner.

The impact and probability score allocated to a risk will be between 1 and 4 and based on the criteria set out in **Appendix C.** The score will be determined by multiplying the highest impact score against the probability.

Evaluate the risk

We now move on to the final element of risk assessment, risk evaluation. The central idea behind risk evaluation is that after analysing a risk analysis to estimate its severity, we then have to decide whether to:

• respond to the risk in some form in order to reduce our exposure (hazard risk), reduce the level uncertainty (control risk), or modify the investment (opportunity risk); or

• simply tolerate the level of risk that we have estimated without any further action.
So risk evaluation is, in effect, a decision point in which we decide whether to respond or not to respond to the risk.

Treat/respond to the risk Plan the response

Having set our objectives (at strategic, tactical and operational levels), and then identified and analysed our risks to determine their severity, the next stage logically is to respond to, treat or control the identified risks.

When planning the risk response, the level of ownership and controls must be ascertained before deciding on a suitable response to the risk.

Standard risk management practice requires organisations to set a risk 'appetite'.

Risk controls and Appetite

Risk appetite is described as *"An organisation's unique attitude towards risk taking, which in turn dictates the amount of risk that it considers acceptable"*[2]. Essentially, this refers to the level of risk that can be tolerated if the correct levels of controls have been applied.

If the force's risk appetite is set incorrectly, it could result in an inappropriate risk response and mitigating actions being taken.

The matrix in Figure 1 sets out the force's level of appetite for risk along with the level of controls and ownership that are to be applied. Risks scored between 1 and 6 can be

[2] Office of Government Commerce: Management of Risk: Guidance for Practitioners

tolerated if the correct level of controls have been applied, and any risks scored 8 and above will require necessary action with frequent monitoring and reporting.

(Figure 1: Risk Appetite and Control)

← Risk Probability →				
VERY HIGH	**Green 4** **Senior/ Line Manager** Cost effective controls. Regular monitoring & reporting. Sporadic action & contingency plans not essential	**Amber 8** **Senior Manager** Comprehensive controls. Frequent monitoring & reporting. Necessary action & comprehensive contingency plans.	**Red 12** **Dept Head** Comprehensive controls. Frequent monitoring & reporting. Immediate action & comprehensive contingency plans	**Red 16** **Dept Head** Comprehensive controls. Frequent monitoring & reporting. Immediate action & comprehensive contingency plans
HIGH	**Green 3** **Senior/Line Manager** Cost effective controls. Regular monitoring & reporting. Sporadic action & contingency plans not essential.	**Amber 6** **Senior Manager** Cost effective controls. Regular monitoring & reporting. Necessary action & Outline contingency plans.	**Amber 9** **Senior Manager** Comprehensive controls. Frequent monitoring & reporting. Necessary action & comprehensive contingency plans	**Red 12** **Dept Head** Comprehensive controls. Frequent monitoring & reporting. Immediate action & comprehensive contingency plans
MEDIUM	**Green 2** **Senior/ Line Manager** Low cost controls. Occasional monitoring & reporting. Sporadic action & contingency plans not essential.	**Green 4** **Senior/ Line Manager** Cost effective controls. Regular monitoring & reporting. Sporadic action & contingency plans not essential	**Amber 6** **Senior Manager** Cost effective controls. Regular monitoring & reporting. Necessary action & Outline contingency plans.	**Amber 8** **Senior Manager** Comprehensive controls. Frequent monitoring & reporting. Necessary action & comprehensive contingency plans
LOW	**Green 1** **Senior/ Line Manager** Low cost controls. Occasional monitoring & reporting. Sporadic action & contingency plans not essential.	**Green 2** **Senior/ Line Manager** Low cost controls. Occasional monitoring & reporting. Sporadic action & contingency plans not essential.	**Green 3** **Senior/ Line Manager** Cost effective controls. Regular monitoring & reporting. Sporadic action & contingency plans not essential	**Green 4** **Senior/ Line Manager** Cost effective controls. Regular monitoring & reporting. Sporadic action & contingency plans not essential
	LOW	**MEDIUM**	**HIGH**	**VERY HIGH**

← Risk Impact →

Risk Controls

The nature of controls implemented will be dependent on the Responsible Owners discretion; however, the matrix above provides guidance on the appropriate controls that should be applied.

The Responsible Owner will also be accountable for ensuring any controls they choose to implement are considerate of wider requirements such as cost, legislation, and corporate responsibilities in relation to threat to life and duty of care, amongst others. They will also maintain responsibility for reviewing and monitoring the risk and the controls applied to it.

Risk Responses

Risk management terminology describes four main ways of responding to risk which are widely used across the Force and also form the recommendations at the Risk Management Board.

Tolerate – the risk will be accepted within agreed limits and will depend on the nature of the risk. It will also be dependent on the force's appetite for risk and what level it is prepared to tolerate.

Treat – the risk will be reduced from its current level with the application of appropriate controls.

Transfer – the risk can be transferred, either to another department, or the Force risk register.

Terminate – Also known as avoidance the organisation eliminates the risk if it is too great for the organisation to bear or if the ways to reduce it are impractical or too expensive.

Implementation

The primary goal of the implementation stage of the process is to ensure that the planned risk management response is implemented and monitored as to its effectiveness, and corrective action is taken where responses do not match expectations.

Monitoring and Review

The active monitoring and reviewing of departmental risk will be carried out by departmental heads as well as the Risk, Policy and Review Officer. The departmental risks will be reviewed on a monthly basis by the Senior Management Team to ensure that the necessary controls have been applied, the risk is scored appropriately and that the department's limit of authority to manage the risk has not been reached. If this is the case the risk can then be put forward for the Risk Management Board to consider as a force risk.

The Risk Management Board will monitor and review risks not within tolerance levels and scored 8 or above quarterly in addition to any others raised by Heads of Department or the Risk, Policy and Review Officer.

Strategic risks scored between 1 and 6 can be tolerated if the correct level of controls have been applied and will be managed and actively monitored by the departmental heads responsible for the business area concerned.

The Chief Officer Group will review any risks presented to them at the discretion of the Deputy Chief Constable that require their attention and action.

The Joint Independent Audit Committee are presented with the Force Risk Register and a summary report outlining risk processes, new risks, and changes to risk scores and directions direction of travel.

Making sense of risk scoring

Genuine risks have a **definite cause**, an **uncertain outcome**, and an **impact on objectives**, which can be measured or at least estimated.

We need to look at - What can go wrong, how it could do so, what the impact could be.

If a **definite cause** cannot be identified the item should not be on the risk register.

Risks referring to events that have already happened i.e. incidents. **Incidents** are not risks. The purpose of risk management is to identify risks that can impact on the achievement of objectives and to manage down the likelihood of their occurrence and/or the impact if they materialise, within levels that the organisation can tolerate.

Current risk score - it scores the position at the time the risk is identified taking account of any mitigating controls currently in place

Target risk score - The score after allowing for both mitigating controls in place AND planned actions i.e. where the organisation expects to end up after all mitigating actions are implemented.

Investing effort in agreeing and embedding a common vocabulary will be rewarded by more meaningful risk scores, allowing senior management to focus effort in the right places.

Before a risk assessment is **reduced**, or a **risk closed**, there should be **evidence that the mitigation action is working**, for example through audits or performance monitoring data. A change in the way something is done does not necessarily reduce the risk. The key issue is whether there is evidence that objectives are now more likely to be met, than they were before the mitigation was put in place.

SECTION 6: OPERATIONAL RISK

Although the focus of this strategy is around ‘business’ or ‘strategic’ risks, operational risk is an important factor in the day-to-day business of policing, and should be considered alongside business and strategic risk.

Operational risk and threat is identified in line with the Joint 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.

However, where appropriate, operational risk relating to business area risk should be recorded under department risk registers in line with the scoring and assessment outlined in this strategy, and escalated through the risk management process when there is a potential for it to effect the organisation.

The National Decision Model

The police service adopted a single National Decision Model (NDM) in April 2012.

This model encourages everybody to make risk based decisions taking into account the ACPO 10 Principles of Risk and the new service wide Statement of Mission and Values.

Although the model relates closely to operational risk the NDM can be applied to any situation whether it be a planned operation, spontaneous incident, by an individual or team, and also to both operational and non-operational situations.

An Aide Memoir of the model is contained within **Appendix D** of this strategy and an e-learning package can be completed on NCALT (National Centre for Applied Learning Technologies).

ACPO 10 Principles of Risk

Lincolnshire Police's operational and force risk management processes seek to operate in accordance with the ACPO 10 Principles of Risk which are:

1. The willingness to make decisions in conditions of uncertainty (i.e. risk taking) is a core professional requirement of all members of the Police Service.

2. Maintaining or achieving the safety and well-being of individuals and communities is a primary consideration in risk decision making.

3. Risk taking involves judgement and balance, with decision makers required to consider the value and likelihood of the possible benefits of a particular decision against the seriousness and likelihood of the possible harms.

4. Harm can never be totally prevented. Risk decisions, should, therefore, be judged by the quality of the decision making, not by the outcome.

5. Making risk decisions, and reviewing others' risk decision making, is difficult. This needs to take into account whether they involved dilemmas or emergencies, were part of a sequence of decisions or might appropriately be taken by other agencies.

6. The standard expected and required of members of the Police Service is that their risk decisions should be consistent with those a body of officers of similar rank, specialism or experience would have taken in the same circumstances.

7. Whether to record a decision is a risk decision in itself which should be left to professional judgement. The decision whether or not to make a record, and the extent of that record, should be made after considering the likelihood of harm occurring and its seriousness.

8. To reduce risk aversion and improve decision making, policing needs a culture that learns from successes as well as failures. Good risk taking should be identified, recognised and shared.

9. Since good risk taking depends upon quality information, the Police Service will work with partner agencies and others to share relevant information about those who pose risk or those who are vulnerable to the risk of harm.

10. Members of the Police Service who make decisions consistent with these principles should receive the encouragement, approval and support of their organisation.

SECTION 7: PARTNERS AND REGIONAL COLLABORATION

To ensure that risks and risk management processes are effectively shared and that the force risk management processes sit within a wider realm, the force will continue to be actively involved in Regional Risk Management Groups and other partnerships within this area. This includes the Local Resilience Forum who produces the Community Risk Register as required by the Civil Contingencies Act 2004 and the Greater Lincolnshire Risk Management Group, which has representation from the Lincolnshire County Council, District Councils, and Fire and Rescue.

Participation in Regional Risk Management Groups allow for the sharing of risks which enables common risks to be identified and considered for regional attention, or mitigation through mutual aid agreements.

Whilst staff from the Strategic Development Department will be involved in these ‘risk specific’ groups, all members of the force will be encouraged to feed into and receive feedback from other groups which may improve the force’s risk management process.

SECTION 8: ADDITIONAL INFORMATION AND GUIDANCE

APPENDIX A: RISK MANAGEMENT BOARD

Terms of Reference

This strategy should be read in conjunction with the Force Risk Management Policy which is available on the force intranet.

Further guidance on risk management can be gained from the team Continuous Improvement Unit within Strategic Development.

1 Purpose of the Board

The Role of the Risk Management Board (RMB) is:

1.1 To ensure a co-ordinated approach to identifying, assessing, controlling and monitoring organisational risks with the implementation of the force's Risk Management Process.

1.2 This co-ordinated approach will enable the force to achieve successful risk management and realise benefits in support of the force's strategic objectives.

1.3 The Board will review organisational risks, assign risk owners and monitor organisational risks to the force.

1.4 The Board will focus on:

- Maintaining a clear and cohesive approach of the organisational risk management process.
- Co-ordination of all Risks within the organisational Risk Process and their interdependencies with Lincolnshire Police Force Objectives in order to:
  - Reduce Crime
  - A fair deal for the people of Lincolnshire
  - Policing and services that are there when you need them.

1.5 This will be done, whilst taking into account:

- Key national and local drivers
- Force capacity and capability to deliver
- Impact upon force's performance
- Compliance with Force Security, Data Protection, Health and Safety, and other organisational responsibilities
- Equality and Diversity Issues
- Impact on public confidence, perception and reputation of the force.
- Impact on partners, the community and victims of crime.

2 Specific Responsibilities

2.1 The specific responsibilities of the Board will include:

- Determining if risks are organisational.
- Managing and developing the Risk Management Process.
- Review risk assessments of potential organisational risks.
- Monitor red and amber risks on a quarterly basis.
- Assigning Risk Owners to a risk depending on the risk scoring.
- Providing visible leadership and commitment to the organisational risks and Risk Management Process throughout the organisation.
- Ensuring Programme and Project assurance.
- Ensuring that any agreed actions are completed on time and that timescales are set ensuring when actions should be completed.

3 Frequency

3.1 The Risk Management Board will meet quarterly during the year.

4 Leadership

4.1 The Risk Management Board will display leadership by ensuring that the following key principles are progressed:

4.2 Displaying visible commitment and authority with membership sufficiently senior to:

- Ensure appropriate resources are available to the organisational risks.
- Influence and engage with stakeholders and risk owners.

4.3 Ensuring that skills and experience within the Board provide active management of:

- The cultural and people issues involved in risk.
- The risk costs and the inevitable conflicting demands on resources.
- Organisational risk identification, evaluation and management.

4.4 To enable empowered decision-making, giving individuals the autonomy to fulfil their roles effectively.

4.5 In order to achieve these principles the membership of the Risk Management Board will consist of:

- The Deputy Chief Constable
- The Assistant Chief Constable
- The Assistant Chief Officer
- Force CFO

Not Protectively Marked

- Head of Strategic development
- Head of IMU
- Head of Human Resources
- Head of ICT
- Research and Performance Officer (OPCC)
- Risk, Policy and Review Officer

5 Technical and Specialist Support

5.1 The Board may also invite employees and specialists to the meeting ‘as required’ or as the agenda dictates to provide technical and specialist support.

APPENDIX B: RISK MANAGEMENT PROCESS 2016-2019

Not Protectively Marked

APPENDIX C: RISK SCORING MATRIX

The tables below show how each risk should be assessed to determine its potential impact and probability.

	Score	Performance/ Service Delivery (A)	Finance /Efficiency £ (B)	Confidence/ Reputation (C)	Health & Safety (D)	Environment (E)	Strategic Direction (F)
Very High	**4**	**(A4)** Major disruption to service delivery Major impact on performance indicators noticeable by stakeholders	**(B4)** Force >1,000,000 Business Area >150,000	**(C4)** Major stakeholder /public concerns/ investigations Major reputational damage adverse national media coverage > 7 days	**(D4)** Life threatening. Fatality.	**(E4)** Very high negative environmental impact (high amount of natural resources used, pollution produced, biodiversity affected)	**(F4)** Major impact on the ability to fulfil strategic objective
High	**3**	**(A3)** Serious disruption to service delivery Serious impact on performance indicators noticeable by stakeholders	**(B3)** Force 251,000-1,000,000 Business Area 41,000-150,000	**(C3)** Serious stakeholder/ public concerns/ investigations Serious reputational damage adverse national media coverage < 7 days	**(D3)** Permanent Injury/damage. Critical impact on care. Major injury (reportable to HSE).	**(E3)** High negative environmental impact (medium amount of natural resources used, pollution produced, biodiversity affected)	**(F3)** Serious impact on the ability to fulfil strategic objective
Medium	**2**	**(A2)** Moderate disruption to service delivery Noticeable impact on performance indictors	**(B2)** Force 51,000-250,000 Business Area 11,000-40,000	**(C2)** Moderate public concerns/ investigations Moderate reputational damage adverse local media coverage	**(D2)** Semi-permanent injury/damage. Moderate impact on care. > 3 days absence (reportable to HSE).	**(E2)** Medium negative environmental impact (low amount of natural resources used, pollution produced, biodiversity affected)	**(F2)** Moderate impact on the ability to fulfil strategic objective
Low	**1**	**(A1)** Minor disruption to service delivery Minor impact on performance indictors	**(B1)** Force <50,000 Business Area <10,000	**(C1)** Complaints from individuals	**(D1)** Short-term injury/damage. Cuts/Bruises. < 3 days absence.	**(E1)** Low negative environmental impact (limited amount of natural resources used, pollution produced, biodiversity affected)	**(F1)** Minor impact on the ability to fulfil strategic objective

PROBABILITY			
	Score	**Description**	**Likelihood of the risk occurring**
Very High	4	**Extremely likely** to happen within the next 6 months.	Very likely to happen/occur, possibly frequently
High	3	**Likely to** happen in the next 6-12 months.	Will probably happen/occur, but it is not a persisting issue/ circumstances
Medium	2	**Likely to** happen in the next 1-2 years.	Possible – Might happen or occur occasionally
Low	1	**Unlikely** to happen within the next 2 years.	Do not expect it to happen/occur but it is possible it may do so
Rare	0		This will probably never happen/occur

The force risk score = impact score x probability score. This can be illustrated by the risk matrix below:

IMPACT LEVEL	**Very High**	**4**	**8**	**12**	**16**
	High	**3**	**6**	**9**	**12**
	Medium	**2**	**4**	**6**	**8**
	Low	**1**	**2**	**3**	**4**
		Low	**Medium**	**High**	**Very High**
		PROBABILITY (must be evidence based)			

LOW **1,2,3,4**	***MEDIUM*** **6,8,9**	***HIGH*** **12,16**

APPENDIX D: NATIONAL DECISION MODEL: AIDE MEMOIR

ASSOCIATION OF
CHIEF POLICE OFFICERS

The National Decision Model

VALUES PENTAGON – Statement of Mission and Values

- Is what I'm considering consistent with the Statement of Mission and Values?
- What would the Police Service, any victim, the affected community and the wider public expect of me?

1. INFORMATION – Gather Information and Intelligence

- What is happening?
- What do I know so far?

2. ASSESSMENT – Assess Threat and Risk and Develop a Working Strategy

- Do I need to take action immediately?
- What could happen? Likelihood? Impact?
- Should I seek more information?
- Is this a situation for the police alone to deal with?

Develop a **working strategy:** What am I trying to achieve?

3. POWERS AND POLICY – Consider Powers and Policy

- What police powers might be required?
- Is there any national guidance
- Are there any local policies or guidelines?
- What legislation might apply?

As long as there is a good rationale for doing so, it may be reasonable to act outside policy.

4. OPTIONS – Identify Options and Contingencies

- What options are open to me? Consider the immediacy of any threat; the limits of information to hand; the amount of time available; available resources and support; your own knowledge, experience and skills; the impact of potential actions on the situation and the public.
- Is my preferred option proportionate, legitimate, necessary and ethical?
- What will I do if things don't happen as I anticipate?

5. ACTION AND REVIEW – Take Action and Review What Happened

Respond:
- Implement the option you have selected
- Does anyone else need to know what you have decided?

Record:
- If appropriate, record what you did and why (proportionate record only)

Monitor:
- What happened as a result of your decision?
- Was it what you wanted or expected to happen?

If the incident is continuing, keep using the NDM.
If the incident is over, **review your decisions.**

- What lessons can you take from how things turned out?
- What might you do differently next time?

Not Protectively Marked