Appendix 1

Authorisation to Put on Strategic Risk Register

Risk identifier		***Risk category***		***Risk source***	
Date raised			***Raised by***		
Risk owner			***Risk status***		

Risk description	

Cause	**Event**	**Effect**
.		

Proximity		**Probability**		**Impact**		**Risk rating**	

Appendix 1

Authorisation to Put on Strategic Risk Register

Risk response option	

Risk response plan	Action owner	Costs	Action status

Residual proximity	-	Residual probability	-	Residual impact	-	Residual risk rating	-

Secondary risks	

Signed ---------- Date ----------

Appendix A

<<Document Number>>	Corporate Risk Management Policy
Type of Document:	Policy
Version:	1.0
Registered Owner:	DCC Simon Torr/Kevin Dennis OPCC
Author:	Amanda Froggatt, Risk and Business Continuity Officer
Effective Date:	tbc
Review Date:	tbc
Replaces document (if applicable)	
Linked Documents:	Corporate Risk Management Procedure

Functional owner

Signed: _____ **Date:** _____

Name: _____

Post: _____

Authorised (Head of FEB/Head of OPCC)

Signed: _____ **Date:** _____

Name: _____

Post: _____

Table of Contents

SECTION 1 VERSION CONTROL 2
SECTION 2 BACKGROUND 2
SECTION 3 AIMS / OBJECTIVES 3
SECTION 4 DETAILS 3
4.1 Policy statement 3
4.2 Definitions 3
4.3 Policy scope 4
4.4 Roles and Responsibilities 4
4.5 Application of the Policy 5
4.6 Monitoring and Review of the Policy 5
SECTION 5 LEGISLATIVE COMPLIANCE 5

SECTION 1 VERSION CONTROL

Version No.	Date	Post Holder/Author	Post	Reason for Issue
1.0		Amanda Froggatt	Risk and Business Continuity Officer	Risk Management Policy recommended in line with ISO31000 risk management standard

SECTION 2 BACKGROUND

Corporate risk management is a formalised, systematic process for the identification, evaluation and response to future challenges that an organisation is likely to face.

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) published its influential Enterprise Risk Management (ERM) framework in 2004.

The International Standard for risk management (ISO 31000) was published in 2009.

Risk management is identified in the CIPFA (Chartered Institute of Public Finance and Accountancy) / SOLACE (Society of Local Authority Chief Executives) framework document Corporate Governance in Local Government as one of the 5 dimensions vital to the principles of good corporate governance.

The UK public sector risk management association, Alarm (which the Force is a member of) has produced a National Performance Model for Risk Management in Public Services which is based on ISO 31000.

The development of this Corporate Risk Management Policy and the Procedure (PD592) that supports its implementation have been based on the Alarm model and the ERM framework.

SECTION 3 AIMS / OBJECTIVES

This Policy is jointly owned by the Deputy Chief Constable (DCC) of the Force and the Chief Executive of the Nottinghamshire Office of the Police and Crime Commissioner (NOPCC). The purpose of this Policy is to clarify and communicate why and how the principles and techniques of risk management will be implemented by Nottinghamshire Police (the Force) and the Nottinghamshire Office of the Police and Crime Commissioner.

The aim of this Policy is to establish and embed within normal business practice and culture, the foundations for efficient and effective corporate risk management to improve the organisation's ability to predict and prepare for future challenges and support Nottinghamshire Police and NOPCC in the achievement of their objectives.

The specific objectives of this policy are to:

- Communicate a **policy statement** that describes Nottinghamshire Police's and the NOPCC's approach to corporate risk management
- Provide a **definition** of a corporate risk within the context of this policy
- Define the **scope** of corporate risk management, making it clear when this policy should be applied and when it should not
- Outline **roles and responsibilities** for corporate risk management within the Force and NOPCC
- Describe key stages in the **application** of this policy, linking it with the supporting Procedure

SECTION 4 DETAILS

4.1 Policy statement

Nottinghamshire Police and the NOPCC will employ a formal, structured process for the identification; evaluation and response to corporate risks which will seek to identify threats, opportunities and vulnerabilities at the earliest opportunity and then measure their likely effect on the achievement of business priorities. Wherever practicable, the Force and NOPCC will endeavour to apply a proportionate level of resources to control known risks in order to preserve the quality of service provision, whilst maintaining value for money.

The Chief Officer Team and Chief Executive will seek to obtain regular assurance that the controls put in place to mitigate risk exposure throughout the organisation are effective and proportionate. This will be enabled through the maintenance of risk registers that are reviewed and updated quarterly, and the production of an annual report on the efficiency and effectiveness of corporate risk management throughout the organisation.

4.2 Definitions

For the purposes of this Policy the following definition of a **corporate risk** will be applied:

> A corporate risk is an uncertain future event that may affect the achievement of the organisation's objectives

In this context, what is "uncertain" could be the likelihood of the event occurring, and/or the degree of impact it may have.

4.3 Policy scope

This policy applies to the management of the Force Strategic Risk Register, the NOPCC Risk Register, the Information Risk Register and thematic and individual departmental risk registers.

Corporate programmes and projects will maintain their own risk registers, utilising the same scoring matrix and terminology as that used for Corporate Risk Management.

Other areas of business that employ aspects of risk assessment, such as public protection and health and safety, are outside the scope of this policy.

This policy does not apply to risks that are managed by collaborative policing units or statutory partnerships. However, the risk that a key service delivery partnership or collaborative agreement may fail, or fail to achieve its agreed objectives, will form part of the Strategic Risk Register.

4.4 Roles and Responsibilities

The **Deputy Chief Constable (DCC)** and the **Chief Executive** of the NOPCC, as the joint owners of the Corporate Risk Management Policy, are responsible for,

- Defining the risk management approach through the Corporate Risk Management Policy.
- Providing assurance to the Chief Constable and Commissioner that the Corporate Risk Management Policy is effective and being applied consistently and appropriately throughout the Force and NOPCC.
- Reporting on strategic risks to the Joint Audit and Scrutiny Panel.
- Ensuring that appropriate risk registers are in place for their respective areas of accountability and that are communicated to relevant stakeholders.

The **Chief Officers** are responsible for:

- Contributing to the development of risk management strategies within their areas of accountability and expertise.
- Owning strategic risks (where appropriate) within their areas of accountability, applying the process of escalation and delegation in accordance with the relevant risk management strategy.
- Delegating the management of specific risks (where appropriate) to thematic leads, heads of department or senior managers.

Thematic Leads and Heads of Departments are responsible for managing their own risk registers, allocating responsibility for individual risks to members of their **Senior Management Team**, and escalating potential strategic risks to **their respective Chief Officer.**

Senior Managers are responsible for:

- Managing risks assigned to them by a Chief Officer, Thematic Lead or Head of Department.
- Participating in the identification and assessment of risks and risk response within their area of expertise.

The **Risk and Business Continuity Officer**, is responsible for providing professional advice and guidance on all aspects of the Corporate Risk Management Policy and Procedure, facilitating full risk reviews and maintaining the Strategic Risk Register.

Individual **project managers** are responsible for the identification and management of risks to their activities within the Nottinghamshire Police Project Management Methodology.

4.5 Application of the Policy

The process for identifying and evaluating risks, implementing a risk control strategy and conducting and reporting on a quarterly review of corporate risks, is described in the Corporate Risk Management Procedure (PD592).

4.6 Monitoring and Review of the Policy

The Governance and Business Planning team will review the application of the Force's Corporate Risk Management Policy against the Alarm model and prepare a summary report as part of the Annual Governance Statement.

Independent review of corporate risk management will also be conducted by the internal auditors, Mazars, as part of their audit strategy.

SECTION 5 LEGISLATIVE COMPLIANCE

This document has been drafted to comply with the general and specific duties in the Race Relations (Amendment) Act 2000, Data Protection, Freedom of Information Act, European Convention of Human Rights and other legislation relevant to the area of policing such as, Employment Act 2002, Disability Discrimination Act 1995, Sex Discrimination Act 1975 and Employment Relations Act 1999.

Appendix B

<<Document Number>>	Corporate Risk Management Procedure
Type of Document:	Procedure
Version:	1.0
Registered Owner:	DCC Simon Torr/Kevin Dennis OPCC
Author:	Amanda Froggatt, Risk and Business Continuity Officer
Effective Date:	tbc
Review Date:	tbc
Replaces document (if applicable)	
Linked Documents:	Corporate Risk Management Policy

Functional owner

Signed: _____ **Date:** _____

Name: _____

Post: _____

Authorised (Head of FEB/OPCC)

Signed: _____ **Date:** _____

Name: _____

Post: _____

Table of Contents

SECTION 1 VERSION CONTROL 2
SECTION 2 BACKGROUND 2
SECTION 3 AIMS / OBJECTIVES 2
SECTION 4 DETAILS 3
4.1 Risk management structure 3
4.2 Risk review process 3
4.2.1 Risk identification 4
4.2.2 Risk analysis 4
4.2.3 Risk control 7
4.2.4 Risk monitoring 8
4.3 Monitoring and review of the procedure 9
SECTION 5 LEGISLATIVE COMPLIANCE 9

SECTION 1 VERSION CONTROL

Version No.	Date	Post Holder/Author	Post	Reason for Issue
1.0	October 2016	Amanda Froggatt	Risk and Business Continuity Officer	New Process

SECTION 2 BACKGROUND

Corporate risk management is a formalised, systematic process for the identification, evaluation and response to future challenges that an organisation is likely to face.

SECTION 3 AIMS / OBJECTIVES

The aim of this Corporate Risk Management Procedure is to establish a framework for providing assurance to the Chief Officer Team, Nottinghamshire Office of Police and Crime Commissioner (OPCC), stakeholders and members of the public that the Force is using its resources proactively and proportionately to manage risk in line with its Policy and in support of its objectives.

The specific objectives of this Procedure are to:

- Prescribe a formal **structure** for managing corporate risk throughout the organisation
- Establish a clear **process** and consistent set of criteria to enable the identification, analysis, control and monitoring of corporate risk as part of a structured, evidence-based approach to decision making

SECTION 4 DETAILS

4.1 Risk management structure

A **risk register** is a document used to record, manage and monitor identified risks. Nottinghamshire Police will adopt a hierarchy of risk registers to enable the management of corporate risks.

The following risk registers will be set up and maintained within the Corporate Development Department:

Strategic Risk Register
Strategic Risks are those risks that could have an impact on the achievement of the organisation's objectives. The Chief Officer Team will determine and manage strategic risks, and the Strategic Risk Register will be administered by the Risk and Business Continuity Officer, with Corporate Development.

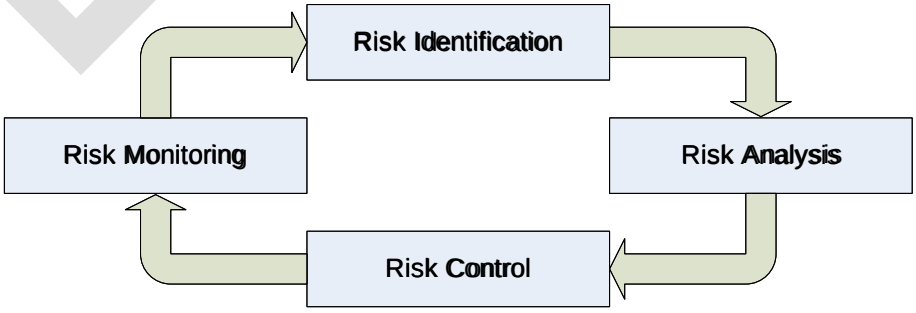
NOPCC Risk Register
NOPCC risks are those risks which could have an impact on the achievement of the Commissioner's objectives. The Senior Management Team will determine and manage these risks, with the register being maintained by the Risk and Business Continuity Officer, with Corporate Development.

Information Risk Register
Information Risks are those risks which are specific to the Force's information systems, security or management. The Force Information Assurance Board (FIAB) chaired by the DCC, will determine and manage information risks, and the Information Risk Register will be administered by the Information Security team.

Thematic and Departmental Risk Registers
Risks which are anticipated to have an effect on the objectives of only one thematic area or department are managed using the respective thematic and departmental risk registers. Each Senior Management Team (SMT) will determine and manage thematic and departmental risks, supported by the Risk and Business Continuity Officer.

4.2 Risk review process

There are 4 distinct stages in the risk review process, as shown in the following diagram:



Each of these stages is described in more detail below.

4.2.1 Risk identification

The risk registers are populated with a broad range of generic risks which are kept under regular review as new threats and opportunities appear on the horizon and organisational vulnerabilities are revealed. The purpose of these risk registers is to provide a comprehensive overview of the ever-present potential risks that the organisation faces, as a focus for regular review and evaluation and to provide the necessary level of assurance to senior management. However, from time to time it is possible that new risks may be identified that are not included on any risk register.

In order to be considered for inclusion on a risk register a potential new risk must be raised at the appropriate management meeting for consideration:

- Strategic risks - Chief Officer Team, or Force Performance Board.
- NOPCC risks – Senior Management Team.
- Information risks – Chief Officer Team, or Information Assurance Board.
- Thematic or department risks - Senior Management Team meeting.

Once a potential new risk has been identified at the appropriate meeting and accepted by the Chair as requiring a formal evaluation, the risk must be assigned to a Responsible Officer, who has overall responsibility for managing the risk. The Responsible Officer may at any time designate a Risk Co-Ordinator, who acts on their behalf to evaluate and review the risk.

4.2.2 Risk analysis

The Responsible Officer (or Risk Co-ordinator) must carry out a full risk analysis for all newly identified risks, and when completing a formal risk review. This process will be supported by a member of the Planning & Policy team, using a standard corporate template (Appendix 1), and involves consideration of three distinct elements within each risk:

- Cause – the organisational vulnerability which may be exposed by the risk
- Event – the uncertain future occurrence which may trigger the risk
- Effect – the anticipated impact of the risk on the organisation

Organisational vulnerabilities (**causes**) may be identified through formal audit or inspection of the Force's systems and processes, or emerge more organically as part of a process of organisational learning and review.

Potential **events** which may have an effect on a risk can be identified through horizon scanning, a process which considers the extent to which future developments may affect the organisation and represent a significant threat or opportunity. Horizon scanning can take many forms, including:

- Tracking forthcoming changes to national or local government policy
- Performance analysis (predicted trends)
- Intelligence analysis (emerging threats)
- Anticipating technological developments
- Academic studies, research papers and "Think tank" reports

All risks are categorised and scored according to the area of business they are likely to have the biggest **effect** on, drawn from the following list:

- Strategic direction
- Community harm
- Performance / Service delivery
- Confidence / reputation
- Finance / efficiency
- Health & safety
- Environment

The first stage in the risk analysis is to describe the risk clearly and concisely according to its cause, event and effect. This also includes linking the risk to one of the Force's priorities:

1 Cut crime and keep you safe.
2 Earn your trust and confidence.
3 Spend your money wisely.

Once the risk has been described it should be scored, taking account of any controls that are already in place to either reduce the likelihood or mitigate the impact. This will produce the **initial risk score**.

Risk scoring is achieved through an evaluation of the chance that the risk will occur, based on an understanding of the likely cause and event (**likelihood**), and the potential effect it will have (**impact**). In order to evaluate Likelihood and Impact, consideration should be given to relevant **key risk indicators**. These indicators will provide the evidence base for both initial and periodic risk analysis.

Typical sources of key risk indicators include:

- Performance analysis
- Forecasting
- Audit or inspection
- Peer review
- Consultation
- Benchmarking
- Research

The Likelihood of a risk occurring is scored according to the following criteria:

Likelihood	**Description**	**Score**
Very High	>75% chance, almost certain to occur	4
High	51-75% chance, more likely to occur than not	3
Medium	26-50% chance, fairly likely to occur	2
Low	<25% chance, unlikely to occur	1

The Impact of a risk is scored according to the following criteria:

	Impact score			
Impact category	**Low (1)**	**Medium (2)**	**High (3)**	**Very High (4)**
Performance / Service Delivery	Minor, brief disruption to service delivery. Minor impact on performance indicators.	Significant, sustained disruption to service delivery. Noticeable impact on performance indictors.	Serious, protracted disruption to service delivery. Substantial impact on performance indicators.	Major, long term disruption to service delivery. Major impact on performance indicators.
Finance / Efficiency	Force: <£50,000 Business Area: <£10,000	Force: £51,000 -£250,000 Business Area: £11,000 -£40,000	Force: £251,000 - £1,000,000 Business Area: £41,000 - £150,000	Force: >£1,000,000 Business Area: >£150,000
Confidence / Reputation	Complaints from individuals. Little or no noticeable local media coverage.	Significant public concerns / investigations. Significant reputational damage / adverse local media coverage.	Substantial stakeholder / public concerns / investigations. Substantial reputational damage / adverse national media coverage < 7 days	Major stakeholder / public concerns / investigations. Major reputational damage / adverse national media coverage >7 days
Community impact	Minor impact on a specific section of the community	Significant impact on a specific section of the community. Minor impact on the wider community.	Substantial, prolonged, impact on a specific section of the community. Significant impact on the wider community.	Major, prolonged impact on the wider community.
Health & Safety	An injury or illness involving no treatment or minor first aid / care with no time off work	An injury or illness requiring hospital / professional medical attention and / or between one day and three days off work, with full recovery	An injury or illness requiring over 24 hrs hospitalisation and / or more than 3 days off work, or a major injury as defined by the RIDDOR Regulations	Death, or a life changing injury or illness.
Environment	Little or no noticeable natural resources used, pollution produced, or biodiversity affected.	Moderate amount of natural resources used, pollution produced, or biodiversity affected.	Substantial amount of natural resources used, pollution produced, or biodiversity affected.	Major amount of natural resources used, pollution produced, or biodiversity affected.
Strategic direction	Little or no noticeable change to one strategic objective.	Noticeable change to one or more strategic objectives.	Substantial changes to one or more strategic objectives.	Complete change to strategic direction.

The overall **Risk Score** is arrived at by multiplying the Likelihood by the Impact to give a result between 1 (Low) and 16 (High). The full range of possible risk scores, and the Red (High) / Amber (Medium) / Green (Low) **risk rating**, is shown on the following table:

Impact	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
		Likelihood			

4.2.3 Risk control

Once a risk has been analysed and scored, a basic **risk strategy** should be determined by the Responsible Officer. The chosen strategy should fall into one of the following four categories, typically referred to as the 4Ts:

- Treat – Take action to reduce the likelihood or mitigate the impact of the risk
- Tolerate – Accept the risk and take no further action at this time
- Transfer – Make someone else responsible for the risk, such as through contracting out, a service level agreement, or an insurance policy
- Terminate – Withdraw from the activity that is at risk

If the chosen risk strategy is to **treat** the risk, then consideration must be given to the **risk controls** that already exist and those which would need to be put in place in order to reduce the likelihood of the risk occurring, or mitigate its impact should it occur.

Typical examples of risk controls include:

- Policies, procedures, protocols and guides
- Governance and scrutiny arrangements
- Financial plans (such as insurance or use of reserves)
- Workforce plans (such as recruitment or training)
- Improvement plans and strategies
- Communication strategies
- Contingency or business continuity plans
- Partnership or collaboration agreements
- Mutual aid agreements
- Security arrangements

The effectiveness of existing risk controls can be evaluated through internal audit and review or performance management, and the degree of assurance they provide should be recorded against each control. Any actions necessary to enhance existing controls or implement new controls should be managed through the Force Action Plan.

Once all existing and planned controls have been identified, the **risk appetite** should be set. Risk appetite is the highest level of risk which the organisation is prepared to accept before it feels compelled to take further action. Put another way, it is the target level for reducing individual risk scores. The Responsible Officer should determine their risk appetite on an individual risk basis, taking account of any potential benefits or opportunities which may arise should the risk be left unchecked and the relative cost and feasibility of attempting to control the risk, so that the Force response is proportionate. Once the risk appetite has been reached the risk strategy should be reset to **tolerate**.

4.2.4 Risk monitoring

Effective risk management requires a structured monitoring and review process to provide assurance that necessary controls are in place and to enable correct prioritisation where additional action is required. This process will be supported by the Risk and Business Continuity Officer, with the exception of the Information Risk Register where support will be provided by the Information Security team.

There are two distinct types of risk review:

- A **full risk review** involves the completion of all stages described in section 4.2.2 above (supported by the Risk and Business Continuity Officer)
- An **interim risk review** should provide assurance that controls are still effective, that no new vulnerabilities have been exposed since the last review and that there are no significant events on the horizon (supported by the Risk and Business Continuity Officer).

The level of risk review required is determined by the current **risk rating**, as follows:

- All High (Red) risks should receive a full risk review every quarter
- All Medium (Amber) risks should receive a full risk review every 6 months and an interim risk review every quarter
- All Low (Green) risks should receive a full risk review every 12 months and an interim risk review every quarter

In addition, should an interim risk review identify significant changes to the nature of the risk, a full risk review is required.

All risks on the Force's strategic and thematic or department risk registers will be reviewed on a quarterly basis by the Responsible Officer or Risk Co-ordinator[1]. Thematic and department risk registers are then presented to their SMT meeting.

All strategic risks, along with thematic or department risks within their portfolio are then reported to the Performance Board (or, in the case of the DCC, to them in person) by the Planning and Policy team. This will enable the Chief Officer to scrutinise the management of corporate risk within their area of responsibility and provide an opportunity for thematic or department risks to be considered for escalation to the strategic level.

The Planning and Policy team will then present the complete Strategic Risk Register, along with High thematic and departmental risks to the DCC for approval.

[1] The reporting timetable for the Information Risk Register will be determined by the Force Information Assurance Board (FIAB)

4.3 Monitoring and review of the procedure

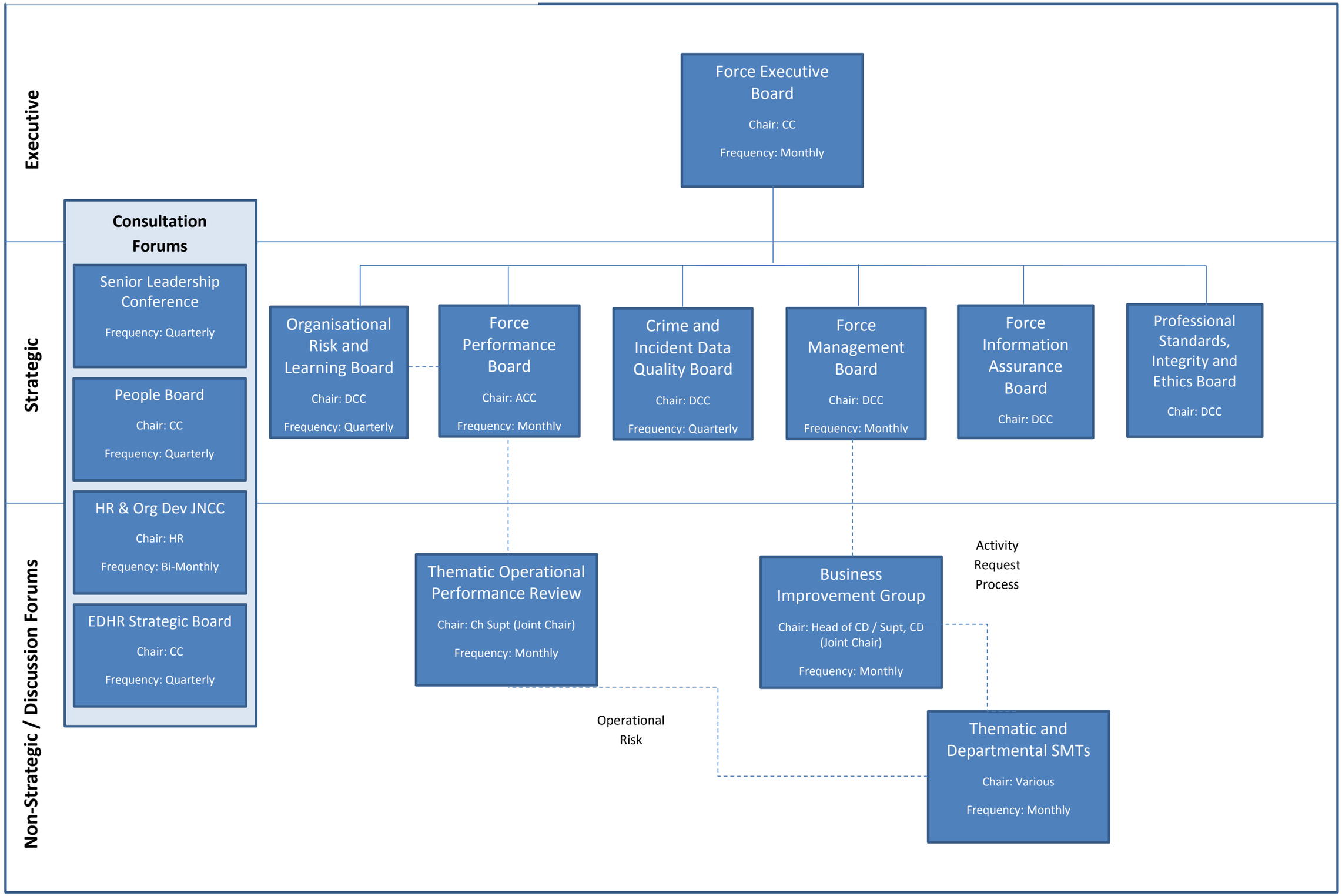
The Joint Corporate Risk Management Procedure will be routinely monitored and reviewed alongside the Policy, by the Risk and Business Continuity Officer and by the Force's internal auditors.

SECTION 5 LEGISLATIVE COMPLIANCE

This document has been drafted to comply with the general and specific duties in the Race Relations (Amendment) Act 2000, Data Protection, Freedom of Information Act, European Convention of Human Rights and other legislation relevant to the area of policing such as, Employment Act 2002, Disability Discrimination Act 1995, Sex Discrimination Act 1975 and Employment Relations Act 1999.

Appendix C

Force Meeting Structure, November 2016



Appendix D

RISK MANAGEMENT PROPOSALS

Force Performance Board –
Frequency -Monthly

Board which analyses and prioritises Strategic Risks

Escalated

Operational Performance Board –
Frequency -Monthly

Board which analyses Crime Performance Related Risks

Organisational Risk & Learning Board –
Frequency - Quarterly

Board which provides strategic governance to advance organisational wide learning. To include Force Gold Groups, Corporate Comms Reporting Issues, ACPO Integrity Model, Serious Case Reviews, Domestic Abuse Homicide Reviews, Public Complaints and Misconducts, Grievances, Employment Tribunals, FOI Requests, Civil Claims, HMIC Inspections

Escalated

Force Executive Board –
Frequency - Quarterly

Reported

Joint Audit & Scrutiny Panel –
Frequency – Bi-annually

Reported

Strategic Risk Register

Force Risk Register

Operations and Planning Command Risk Register

- Community Protection
- City/County Neighbourhood
- Response
- Contact Management
- Local Investigations

Investigations and Intelligence Command Risk Register

- Serious Investigations and Organised Crime
- Intelligence
- Archives and Exhibits
- Public Protection
- Complex Investigations

Risk Identification – Categories – Performance/Service Delivery, Finance/Efficiency, Confidence/Reputation,

Community Impact, Health and Safety, Environment, Strategic Direction

Appendix E

RISK MANAGEMENT PROPOSALS

Force Performance Board –
Frequency -Monthly

Board which analyses and prioritises Strategic Risks

Organisational Risk & Learning Board –
Frequency -Quarterly

Board which provides strategic governance to advance organisational wide learning. To include Force Gold Groups, Corporate Comms Reporting Issues, ACPO Integrity Model, Serious Case Reviews, Domestic Abuse Homicide Reviews, Public Complaints and Misconducts, Grievances, Employments Tribunals, FOI Requests, Civil Claims, HMIC Inspections

Escalated

Force Executive Board –
Frequency - Quarterly

Reported

Joint Audit & Scrutiny Panel –
Frequency – Bi-annually

Reported

Strategic Risk Register

Force Risk Register

EMPLS

EMSCU

EMCHRS-L&D

EMCHRS-OHU

EMSOU

Estates

Corporate Communications

Finance

EMOpSS

Information Services

Human Resources

Professional Standards

Corporate Development

EMCJS

Risk Identification – Categories – Performance/Service Delivery, Finance/Efficiency, Confidence/Reputation,

Community Impact, Health and Safety, Environment, Strategic Direction

Terms of Reference: Force Performance Board

1. Purpose:

Provide an organisational-wide forum for thematic leads and heads of departments to discuss key areas of performance, and identify any emerging strategic opportunities and risks.

2. Objectives:

- Identification and capturing of current and emerging risks, to ensure mitigation is identified and appropriately applied.
- Reviewing of risk responses in an open forum with the aim of advancing organisational understanding and learning.
- Recommend to the Force Executive Board risks that require a strategic response or which require additional resources.
- Identify and review any exceptional performance against Priorities of the Police and Crime Plan
- Escalate where necessary these exceptions to the Force Executive Board.
- Delegate actions in regard to exceptional performance to the departmental/thematic Operational Performance Review meetings

3. Scope:

Within these objectives, the Force Performance Board will consider the following areas:-

- Thematic/Departmental Risk Registers
- Priorities of the Police and Crime Plan
- Priorities of the Strategic Intelligence Assessment

4. Frequency:

Monthly.

5. Core Membership:

- Assistance Chief Constable (Chair)
- Head of Professional Standards
- Head of Finance
- Representative from EMSOU
- Head of EMoPS
- Head of Custody

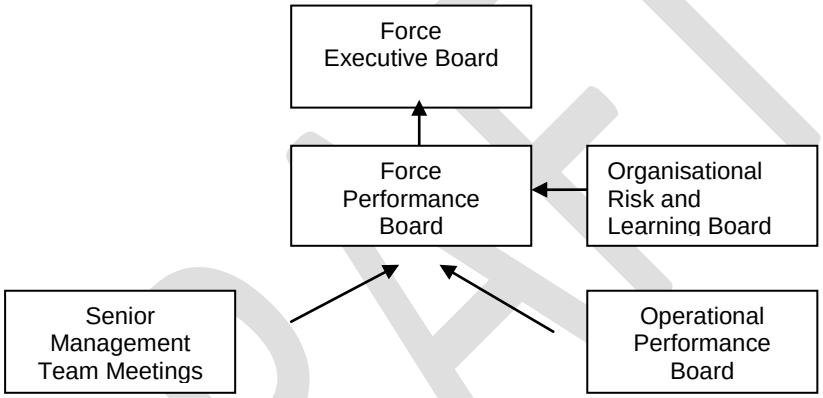
- Chief Superintendent Investigations and Intelligence
- Chief Superintendent, Operations and Planning
- Superintendent, Corporate Development
- Head of Corporate Communications
- Head of Human Resources
- Representative from Office of Police and Crime Commissioner

If a core member is unable to attend, they must send someone to deputise who is able to provide information and make decisions on behalf of the core member. Guest speakers will be invited to attend for specific agenda items as and when appropriate.

6. Administration:

Business Support Officer to record key actions and decisions.
All papers to be submitted within five working days of the meeting.

7. Governance of Force activity:



8. Key Information Sources:

- Thematic/Departmental Risk Registers
- Priorities of the Police and Crime Plan
- Priorities of the Strategic Intelligence Assessment

9. Quality Assurance Review:

All meetings will be subject to an annual quality assurance review by a member of the Corporate Governance and Business Planning Team.

Terms of Reference: Organisational Risk & Learning Board

1. Purpose:

Provide an organisational-wide forum for thematic leads and heads of departments to discuss key areas of learning, and identify any emerging strategic opportunities and risks.

2. Objectives:

- Identification and provision of strategic governance to advance organisational wide learning and address potential blame culture.
- Provision of strategic leadership, direction and governance, ensuring integrity and transparency across the organisation.
- Identification and the appropriate management of organisational wide strategic, tactical and operational matters, which require change and improvement.
- Identification and the capture of emerging strategic risks, ensuring that controls are identified and appropriately applied.

3. Scope:

Within these objectives, the Organisational Risk and Learning Board will consider the following areas:-

- On-going Force Gold Groups
- Current Corporate Communications Reporting Issues
- ACPO Integrity Model
- Serious Case Reviews, Serious Adult Reviews and Domestic Violence Homicide Reviews.
- EMSOU Regional Review Unit Recommendations
- Public Complaints and Misconduct Matters
- Grievances
- Employment Tribunals
- FOI Requests
- Civil Claims
- External Inspection Regimes, eg HMIC
- Learning from other Forces or Agencies

4. Frequency:

Quarterly subject to requirements

5. Core Membership:

- Deputy Chief Constable (Chair)
- Assistance Chief Constable

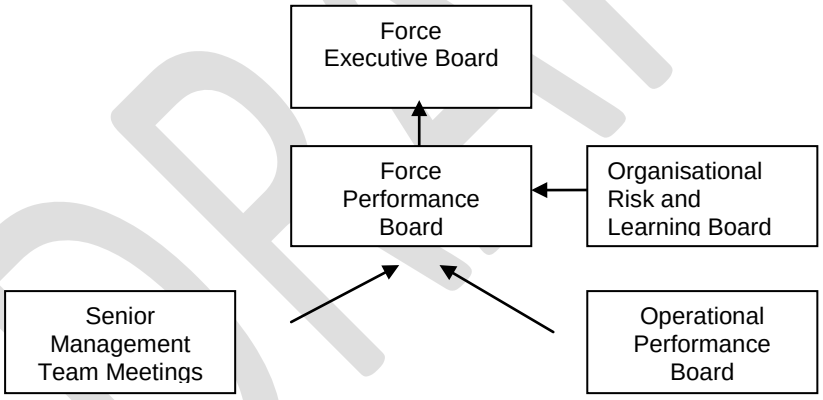
- Head of Professional Standards
- Head of Public Protection
- Representative from Regional Review Unit
- Head of Information Management
- Representative from Legal Services
- Chief Superintendent Investigations and Intelligence
- Chief Superintendent, Operations and Planning
- Superintendent, Corporate Development
- Head of Corporate Communications
- Head of Finance
- Head of Human Resources
- Representative from Office of Police and Crime Commissioner
- Risk and Business Continuity Officer

If a core member is unable to attend, they must send someone to deputise who is able to provide information and make decisions on behalf of the core member. Guest speakers will be invited to attend for specific agenda items as and when appropriate.

5. Administration:

Business Support Officer to record key actions and decisions.
All papers to be submitted within five working days of the meeting.

6. Governance of Force activity:



7. Key Information Sources:

- ACPO Integrity Model
- Serious Case Reviews, Serious Adult Reviews and Domestic Violence Homicide Review Recommendations
- EMSOU Regional Review Unit Recommendations
- Public Complaints and Misconduct Matters
- Grievances
- Employment Tribunals
- FOI Requests
- Civil Claims
- External/Internal Inspection Recommendations, eg HMIC/Mazars

8. Quality Assurance Review:

All meetings will be subject to an annual quality assurance review by a member of the Corporate Governance and Business Planning Team.