HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

RISK MANAGEMENT AND ASSURANCE MAPPING FRAMEWORK

FRAMEWORK

Document Type:	**Framework**
Framework Owner:	**Head of Corporate Services**
Department:	**Corporate Services**
Framework Writer:	**Business Continuity and Risk Co-ordinator**
Version:	**1.2**
Effective Date:	**25/02/2020**
Recommended Review Date:	**25/02/2023**

Version No	Author	Changes
0.1	Section 40	Transferred from Policy format (v0.5)
0.2	Section 40	Minor amendment from Ch Supt Corporate Services
0.3	Section 40	Reference to it being a joint framework between NWP and OPCC
1.0	Section 40	Agreed at Assurance Board 24/02/2020
1.1	Section 40	Para 3.13 added re. Assurance Board Terms of Reference and ameneded reference to Risk & Business Continuity Coordinator to Risk & Business Continuity Lead throughout.
1.2	Section 40	Pic updated in 5.11 to reflect updated governance structure

CONTENTS

1. INTRODUCTION & PURPOSE 2

2. TARGET AUDIENCE 2

3. ROLES AND RESPONSIBILITIES 2

4. RISK MANAGEMENT IN NWP 3

4.1 Risk Management 3

4.2 APP Risk Principles 4

4.3 What is a Risk? 4

4.4 When Do Risks Need To Be Recorded? 4

4.5 National Decision Model (NDM) 5

4.6 Risk Appetite 6

4.7 Assurance Mapping 7

5. NWP RISK MANAGEMENT PROCESSES 8

5.1 Force Risk Register (FRR) 8

5.2 Risk Types 8

5.3 Risk Levels 8

5.4 Risk Owners 9

5.5 Risk Wording 9

5.6 Risk Actions 9

5.7 Closing risks 9

5.8 Partnership/Collaboration 9

5.9 Programme and Project Risk Management 9

5.10 Duplication 10

5.11 Risk Reports 10

5.12 Record Retention 11

5.13 Assurance Mapping 11

5.14 Process Flowcharts 12

5.14.1 New Risk Creation for the Force Risk Register 12

5.14.2 Updating Force Risks/Ongoing Force Risks on the Force Risk Register 13

5.14.3 Closing Force Risks on the Force Risk Register 14

5.14.4 Assurance Mapping 15

1. INTRODUCTION & PURPOSE

1.1 **Risk Management**

Risk Management is fundamental to any organisation's strategic management process and is a part of internal control systems.

North Wales Police (NWP) and the Office of the Police and Crime Commissioner (OPCC) have a duty to manage risk effectively to

- Maintain confidence in the force
- Safeguard public confidence and integrity
- Ensure the delivery of the police and crime plan objectives

Risk Management enables both to understand acceptable levels of risk and take a planned and systematic approach to the identification, evaluation and control of the risks that can threaten the Force.

The processes in place to manage risk within NWP:

- ensures the Force has strategic direction for risk management and seeks to achieve successful outcomes;
- provides clear and consistent standards for the management of risks that contribute to and support the Police and Crime Commissioner's (PCC) police and crime plan objectives and the efficient running of the Force;
- ensures risk management is integrated in the culture of the Force, by informing all officers and staff of their responsibilities in relation to risk management; and
- ensures the Force has up to date and live records relating to the highest risks affecting the Force.

2. TARGET AUDIENCE

2.1 This framework is a joint framework between NWP and OPCC and should therefore be used by all officers and staff of both North Wales Police and the Office of the Police and Crime Commissioner. It is vital that everyone understands the role they play in effective risk management.

3. ROLES AND RESPONSIBILITIES

3.1 The **Police and Crime Commissioner** is responsible for risk management within the OPCC; however this is delegated to the OPCC Chief Executive and Chief Finance Officer.

3.2 The **OPCC Chief Executive and Chief Finance** hold delegated responsibility for OPCC risk management.

3.3 The **Deputy Chief Constable** is responsible for NWP risk management; however this is delegated to the Risk and Business Continuity Lead. As SIRO, the DCC is responsible for providing scrutiny for information security risks.

3.4 The **Risk and Business Continuity Lead** is responsible for the administration of the risk processes which includes providing support to risk leads. The Risk and Business Continuity Lead will also provide regular reports to SMTs and Force Committees.

3.5 The **SMT / Risk Owner** will collectively own risks. They will ensure risk is a standing agenda item at all SMT Meetings and will monitor and challenge the performance of risks, ensuring they liaise with risk leads as and when necessary. The SMT/Risk Owners will consider all new/emerging risk and determine if the recording threshold is met or not. For project risks, this will be the role of the Project and Programme Boards.

3.6 The **Risk Lead** is the officer or staff member that is in the best position to actively influence the management of the risk. The Risk Lead is responsible for **allocating actions, coordinating updates and regularly reviewing and updating risks.**

3.7 **Action Owners** may differ from the Risk Lead, and may be tasked by the risk lead. There may be several different Action Owners for one risk. Action Owners are responsible for progressing any actions associated to a risk.

3.8 The **Strategic Management Board** will regularly review the risk register and provide strategic oversight of all NWP 'high' and 'critical' risks. For project risks, this will be the role of the Programme Board.

3.9 The **Force Committees i.e. Ops Committee** will provide a second level of scrutiny for all recorded risks under their remit and will challenge, when appropriate, the decisions made at SMT level.

3.10 The **Joint Audit Committee** are responsible for considering the effectiveness of the PCC and the Chief Constable's risk management arrangements by regularly reviewing the risk register.

3.11 **Internal Audit** will provide independent assurance that risk management, governance and internal controls are operating effectively.

3.12 **Welsh Audit Office** will provide further independent assurance that risk management, governance and internal controls are operating effectively.

3.13 **Assurance Board** will provide a single point for managing all assurance related matters i.e. policies, risk management and business continuity management. The Board will provide the Force with reassurance that there is sufficient evidence that the right level of assurance is in place in the right areas. The Assurance Board will be the final ratification point for all policies**.**

4. RISK MANAGEMENT IN NWP

4.1 **Risk Management**

Risk management is a continuous process that runs through the whole Force and helps to reduce potential harms and risks.

Risk management is about making the most of opportunities, making the right decisions and achieving objectives once those decisions are made. A failure to manage risk effectively could result in financial losses, disruption to services, threats to public health & safety, bad publicity or claims for compensation.

There are both positive and negative aspects of risk; risk taking offers the possibility of harm but also the chance of success. As well as the threats, risk management can identify opportunities which contribute to the effectiveness of performance delivery.

Positive activity should be considered, recorded and offset against negative impacts. Positive activity, continuous improvement and lessons arising from good practise can highlight opportunities.

The below represents the 7R's and 4T's of risk management as noted in the ISO31000 and NWP risk arrangements follows this model.

4.2 **APP Risk Principles**

NWP adhere to the College of Policing's APP risk principles which should underpin all considerations of risk and can be found here.

4.3 **What is a Risk?**

A risk can be defined as an uncertain event which, should it occur, will have an effect on the achievement of the Police and Crime Plan objectives. A risk can be either a threat or an opportunity.

Risks should be highlighted where they will affect the Forces' capacity or capability to achieve the Police and Crime Plan objectives.

4.4 **When Do Risks Need To Be Recorded?**

Across the organisation officers and staff are managing risk effectively as part of their day to day activities; this framework does not impact on that activity. Whilst the general principles outlined in this document may support that activity, the processes outlined at section 5 only applies to those risks that meet the threshold (see table below).

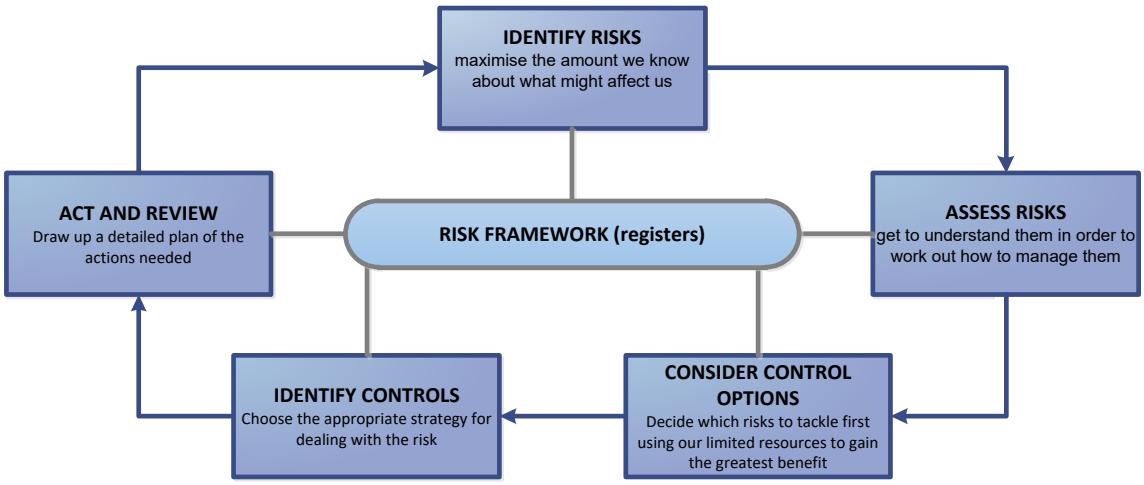
The PESTELOM model (source: College of Policing) identifies areas that support identification of risks and should be considered when applying the threshold below

- Political
- Economic
- Social
- Technological
- Environmental
- Legal
- Organisational
- Media

DETERMINING RISK LEVEL AND MANAGEMENT ROUTE		Probability (consider the period within which the risk is likely to occur e.g. highly likely to occur in the next year; and how often, on average, has the risk occurred already)				
		Negligible Rare, **may** occur in exceptional circumstances. No or little experience for a similar failure;	**Low** **Might** occur at some point in time. Conditions do exist for this to occur, but controls exist and are effective.	**Medium** **Could** occur, this is possible. Measures to reduce likelihood exist, but may not be fully effective.	**High** **Will** probably occur, measures may or may not exist to reduce likelihood.	**Critical** Is **expected** to occur, almost certain.
Impact	**Critical** May cause key objectives to fail. Very **significant** impact on organisational goals. A major effect on the organisation /communities.	**Medium** SMT*/PB (*If cannot be managed by single SMT should be escalated to Force Risk Register)	**Medium** SMT*/PB (*If cannot be managed by single SMT should be escalated to Force Risk Register)	**High** Force Risk Register, reported to SMT/PB and Force Committee	**Critical** Force Risk Register, reported to SMT/PB, Force Committee and SPB	**Critical** Force Risk Register, reported to SMT/PB, Force Committee and SPB
	High Risk factor may lead to significant delays or non-achievement of objectives. An event which has a high impact on the organisation and / or a serious effect on a Service Area or Department.	**Low** Managed by individual or team; if necessary may be referred to SMT/PB for management at that level	**Medium** SMT*/PB (*If cannot be managed by single SMT should be escalated to Force Risk Register)	**High** Force Risk Register, reported to SMT/PB and Force Committee	**High** Force Risk Register, reported to SMT/PB and Force Committee	**Critical** Force Risk Register, reported to SMT/PB, Force Committee and SPB
	Medium **Moderate** effect. Risk factor may lead to delays or increase in cost. An event that has an overall medium effect on the organisation or the outcome of which significantly affects a unit or section	**Low** Managed by individual or team; if necessary may be referred to SMT/PB for management at that level	**Low** Managed by individual or team; if necessary may be referred to SMT/PB for management at that level	**Medium** SMT*/PB (*If cannot be managed by single SMT should be escalated to Force Risk Register)	**High** Force Risk Register, reported to SMT/PB and Force Committee	**High** Force Risk Register, reported to SMT/PB and Force Committee
	Low Some impact of the risk, **fairly minor**. An event that has an overall minor effect on the organisation but the outcome effects individual or unit level only.	**Negligible** Managed by individual/team	**Low** Managed by individual or team; if necessary may be referred to SMT/PB for management at that level	**Low** Managed by individual or team; if necessary may be referred to SMT/PB for management at that level	**Medium** SMT*/PB (*If cannot be managed by single SMT should be escalated to Force Risk Register)	**Medium** SMT*/PB (*If cannot be managed by single SMT should be escalated to Force Risk Register)
	Negligible Some impact of the risk, **but negligible**. The outcome effects individual or small unit only.	**Negligible** Managed by individual/team	**Negligible** Managed by individual/team	**Low** Managed by individual or team; if necessary may be referred to SMT/PB for management at that level	**Low** Managed by individual or team; if necessary may be referred to SMT/PB for management at that level	**Medium** SMT*/PB (*If cannot be managed by single SMT should be escalated to Force Risk Register)

4.5 National Decision Model (NDM)

The following diagram illustrates how the NDM can be used to support an objective approach to risk management. Further information on the NDM can be found here.



4.6 **Risk Appetite**

NWP's risk appetite has been determined as 'Open'; the Chief Constable is willing to consider all options and choose the one that is most likely to result in successful delivery, minimising residual risk as far as possible, while also providing an acceptable level of business benefit. This position falls satisfactorily within the overarching aim of Making North Wales the Safest Place in the UK.

The chart below reinforces NWP's risk appetite on certain risk areas.

While the diagrams at 4.5 and 5.9 illustrate the agreed triggers for escalation; de-escalation and reporting, it is accepted that the risk appetite below may change in response to particular circumstances or the general operating environment.

Risk Area	Risk Level	Context/Narrative
Public Safety	Averse	We will take action to avoid or mitigate risks that impact on public safety.
Staff/officers – Fraud and corruption	Averse	We have no appetite for any fraud or corruption perpetrated by our officers or staff
IT security	Minimalist	We have a very low appetite for risks to the network and availability of systems that support our critical functions; we have a very low appetite for threats to our assets arising from external malicious attacks We will support and enable staff to work effectively in today's digital environment and are prepared to accept some risk to achieve this.
Finance	Cautious	We need to ensure that resources are aligned to strategic objectives, that we have a balanced and sustainable budget and provide VFM in delivering services.
Compliance (Legal / HO / IOPCC / HMIC)	Cautious	We will always operate within the law. We will give due consideration to guidance, recommendations and non-statutory regulations taking into account local circumstances and the needs of the public of North Wales when making our decisions. Compliance is enhanced by our positive attitude towards Social Value.
Staff and Officer wellbeing	Cautious	The health and safety of our staff is important to the delivery of effective and efficient policing in North Wales. We will provide the tools (risk assessments; dynamic risk assessment; training; and equipment) for staff to take managed and acceptable risks.
Public Experience / satisfaction	Cautious	Public experience/satisfaction is very important to us; in a changing environment we are prepared to be innovative and forward-thinking we are prepared to take some risks providing there is an operational/financial imperative

Risk Area	Risk Level	Context/Narrative
Staff/officers - Unethical behaviour	Cautious	Where appropriate we will educate and advise staff/officers whose behaviour falls short of the high standards expected.
Reputation	Open	We are willing to accept some risks to reputation if there is clear potential for the benefits to outweigh the risks. Our willingness to take risks is limited to those situations where there is little chance of significant repercussions for the force should there be a failure. Our reputation is enhanced by our positive attitude towards Social Value and our risk appetite in other areas
Partnerships / collaborations	Open	We are willing to take risks in pursuit of partnership/collaboration development that have the potential to deliver higher benefits.
Business Change	Open	We are open to taking some risk in order to ensure we remain focussed on the future. Business change can be achieved by developing new and innovative ways of managing our services and includes investment in new technologies and IT development.

The Forces' appetite for financial risk is also set out in detail, in the Treasury Management Strategy and the Medium Term Financial Plan which sets out the Forces' budgets for the next five years and is updated annually.

4.7 **Assurance Mapping**

Assurance Mapping compliments the Force's risk management approach as an evidence gathering exercise considering risks that could have a critical impact on the Force. The evidence is structured on the three lines of defence model below.

1st Line of Defence	2nd Line of Defence	3rd Line of Defence
Operational or tactical evidence i.e. procedures, business level monitoring by local management.	Corporate or strategic oversight i.e. Force meetings which oversee and challenge or provide guidance and direction.	External assurance providers i.e. TIAA, Welsh Audit, HMIC who monitor compliance and provide independent challenge and assurance.

Assurance Mapping provides an improved ability to understand and confirm that there are assurances in place over key controls. It also highlights where control gaps exist and therefore allows the Force to address those gaps.

Assurance is fundamental to ensuring a robust governance approach. Assurance aims to provide confidence and evidence and a degree of certainty that the Force knows what is reality. Assurance also enables our regulators and auditors to have confidence that NWP knows where there are vulnerabilities and are therefore able to direct activity appropriately. Assurance provides confidence, evidence and certainty.

Assurance Mapping feeds into governance, policy management and performance management. By managing long term risks which are controlled, through assurance

mapping, it allows the Force to focus time and effort on the live management of dynamic risks.

5. NWP RISK MANAGEMENT PROCESSES

5.1 **Force Risk Register (FRR)**

All risks that meet the threshold will be recorded on a standard template and entered onto the Force Risk Register which is managed by Corporate Services and viewed via the Risk Management SharePoint Site.

Risks that do not meet the threshold, may be recorded in registers held locally however, that is not mandatory. Business Areas intending to establish a local register are encouraged to use an abbreviated version of the Force Risk Register which is available from the Force Risk and Business Continuity Lead on request.

5.2 **Risk Types**

Risks can be agreed by SMTs as being either

- Dynamic or
- Static

Dynamic risks should be recorded on the Force Risk Register and reviewed monthly as a minimum.

Static risks should be recorded on the Force Risk Register and reviewed quarterly as a minimum unless there is rationale for reviewing it on a less frequent basis, and in that case, would likely to be better being recorded on the relevant business areas assurance map.

This will enable attention to be focussed where it is most productive at that time.

5.3 **Risk Levels**

Risk level is derived from the potential impact a risk might have combined with the probability that the risk might become reality.

Three risk levels will be recorded for each risk

- Before controls – the exposure arising from a specific risk before any action has been taken to manage it. If action has already been taken to manage a risk it should be discounted in arriving at the risk level 'before controls'. This will ensure that assumptions about the effectiveness of actions taken to date are scrutinised and tested. This risk level will tend to remain static throughout the life of the risk though it may be reassessed in light of new information.

- Current – the risk level that exists now, this is a product of the risk level 'before controls' and any actions that have been taken to manage the risk.

- Target – this is the level that the risk is to be managed to, the level deemed acceptable for the Force.

It is the risk level before controls that determines if the risk should be added to the Force Risk Register and the reporting route for that risk. So, if a risk is considered 'high'

before controls but has already been managed to 'medium' it will continue to be reported as a 'high' risk throughout its lifetime.

5.4 **Risk Owners**

Force risks will be owned by Senior Management Teams. Project risks will be owned by Project Boards. This will ensure that risks are discussed and assessed collectively and do not represent an individual's viewpoint. It will also reduce the impacts of prolonged absence of individual senior staff.

Where the ownership of a risk is unclear Service Leads will normally be able to discuss and resolve the situation. If that is not possible for any reason then the matter can be referred to the DCC for a decision.

5.5 **Risk Wording**

Risks should be clear, specific and as brief as possible. The nature of the risk needs to be understood by people who don't have direct knowledge of the subject matter. The model below is not prescriptive but is simple and can be adapted to most risks that will be recorded.

If (EVENT), then (CONSEQUENCE)

E.g. ***If*** *policies and procedures are not updated and maintained as required* ***then*** *officers/staff may act on incorrect or out of date information giving rise to complaints and legal action*

5.6 **Risk Actions**

Adding a risk to the Force Risk Register is not an end in itself, the actions to be taken to mitigate the risk and progress in completing them must be clearly articulated.

5.7 **Closing risks**

When a risk has been managed to an acceptable level (usually the target level) or the circumstances around it have improved it may be closed. Assurance (evidence to support the closure) must be articulated in the risk template. The SMT or Project Board that own the risk must approve closure and allocate an action to the Risk Lead to ensure the risk is updated and removed from the Force Risk Register.

Where there are open risks at the point that a project closes then the risks will be referred to the relevant SMT for decisions on the future management of that/those risk(s).

Closed risks will not be reopened. If a risk becomes active again it must be recorded as a new risk.

5.8 **Partnership/Collaboration**

Where risks relate to projects or programmes that are being undertaken in collaboration either with other forces or other organisations then there is no obligation to record risks on the NWP Force Risk Register; there is an expectation that those risks will be managed on an independent register.

Risks recorded and managed on this basis can be transferred to the NWP Force Risk Register if the circumstances warrant it. Alternatively such a risk can be rewritten to capture the particular risks that are posed for the Force.

5.9 **Programme and Project Risk Management**

All risks relating to programmes and projects are managed by the Portfolio Management Office as detailed in their Issue and Risk Management Framework. Risks deemed to impact the Force's ability to meet its' objectives by the SRO will be escalated and added to the Force Risk Register. This will be a decision made at the Project or Programme Board.

5.10 **Duplication**

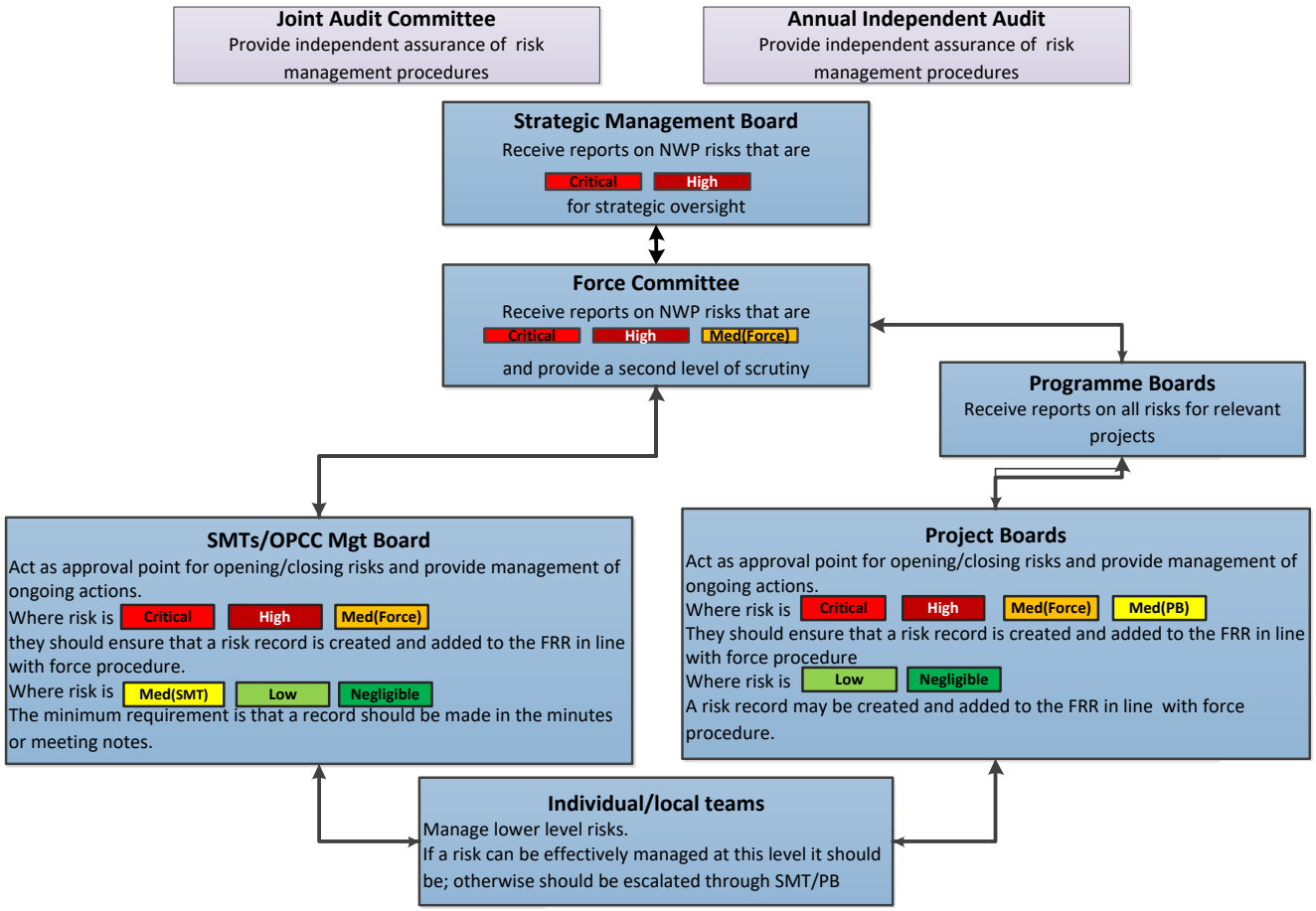
Where there is a legal or business requirement to record and maintain risks elsewhere there will generally not be a requirement to duplicate them in the Force Risk Register, as an example the Treasury Management Strategy and the Medium Term Financial Plan include detailed financial risk analysis which is not replicated on the Force Risk Register.

However, there is nothing to prevent such risks, with SMT approval, from being transferred to or duplicated in the Force Risk Register when appropriate.

5.11 **Risk Reports**

Risks will be reported on to a variety of meetings and committees. The reporting process detailed below allows for the effectiveness of the risk management framework and processes and the risk portfolio content to be reviewed. It also provides reassurance that NWP have robust risk management arrangements in place.

Risk must be a standing agenda item at SMT and Strategic Committee meetings. Programme and Project risks will be considered at dedicated Programme and Project Board meetings.



5.12 **Record Retention**

Risk records – full version history will be retained while a risk is open. When a risk is closed only the last version will be archived, all other versions will be disposed of. The archived final version will be held for two years from the date the risk is closed.

Risk Register - the register does not hold original information; a full version history will be retained for twelve months, any version more than twelve months old will be disposed of.

Project Risks – full version history will be retained while a risk is open. When a risk is closed only the last version will be archived, all other versions will be disposed of. The final version of project risks will be retained for the same period as final project documentation, normally five years.

5.13 **Assurance Mapping**

Each business area should have a completed assurance map (appendix A) and accompanying action plan (appendix B), if necessary.

The Assurance Team will be responsible for creating the assurance map with Business Area SMTs. Assurance maps will record details of the risk, controls in place to mitigate the risk and evidence to demonstrate that the controls are effective. The Assurance maps will also highlight any risks with cross cutting themes by using the following tags

- Reputation
- Health & Safety
- Finance
- IT
- Information Security
- Training

This will ensure any cross cutting themes are identified and reported to the most relevant meetings.

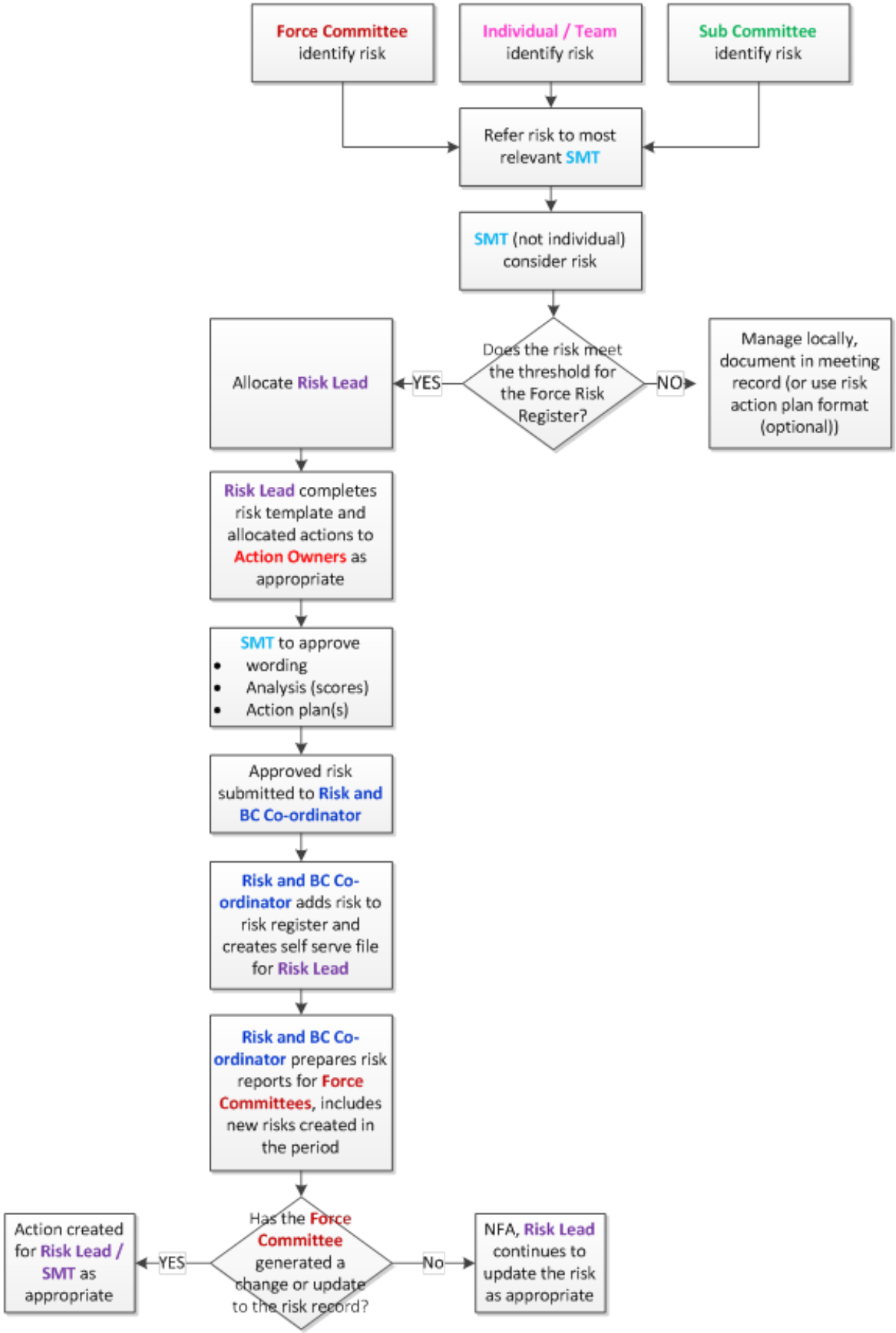
Any areas of weakness identified during the assurance map exercise will be addressed by an accompanying action plan.

Completed assurance maps and accompanying action plans should be reviewed at SMT meetings on a monthly basis. They should also be reported to the Strategic Management Board on a quarterly basis so progress against action plans can be monitored.

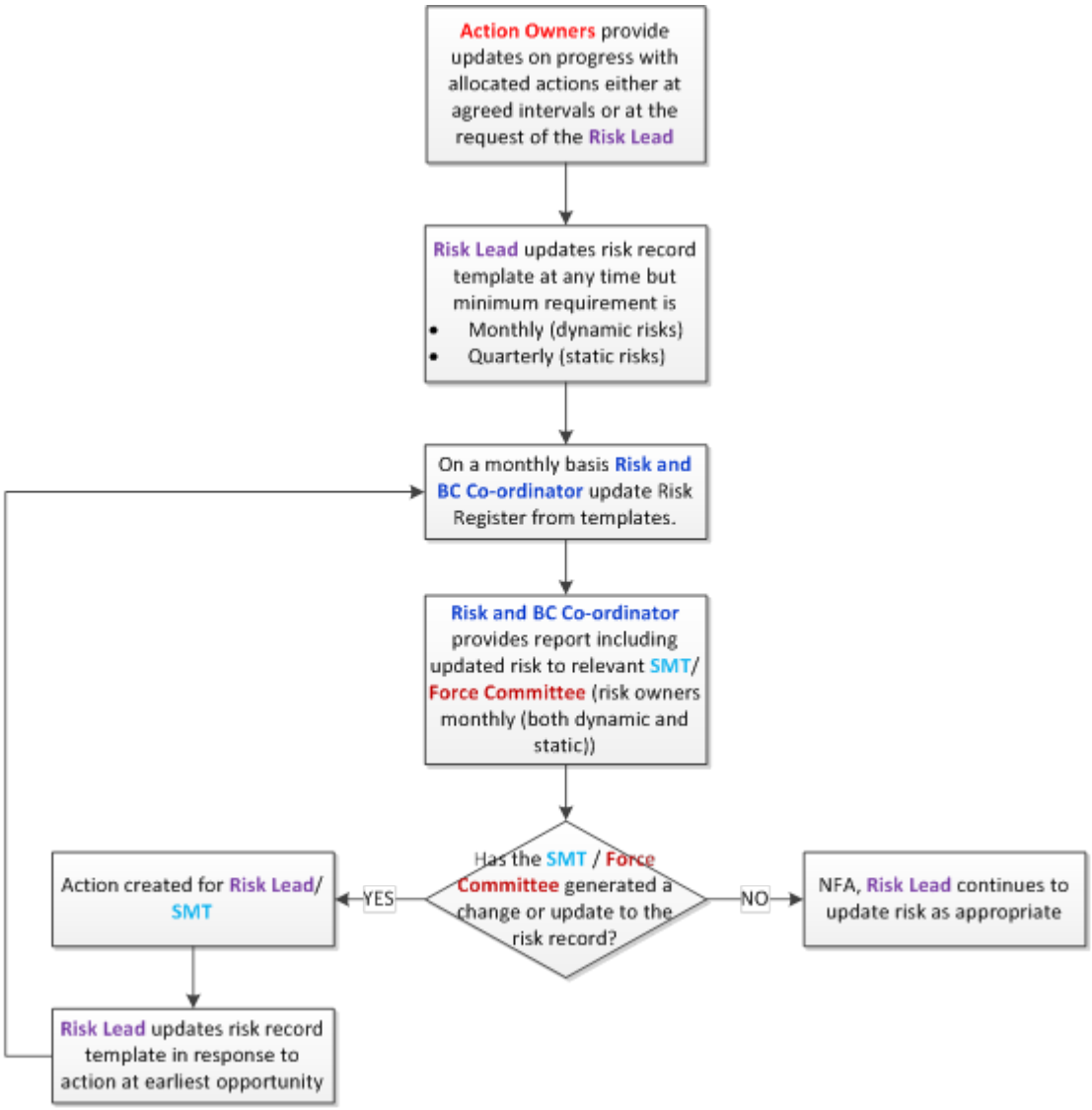
Assurance maps should be working documents, which can be added to as and when risks are identified.

5.14 Process Flowcharts

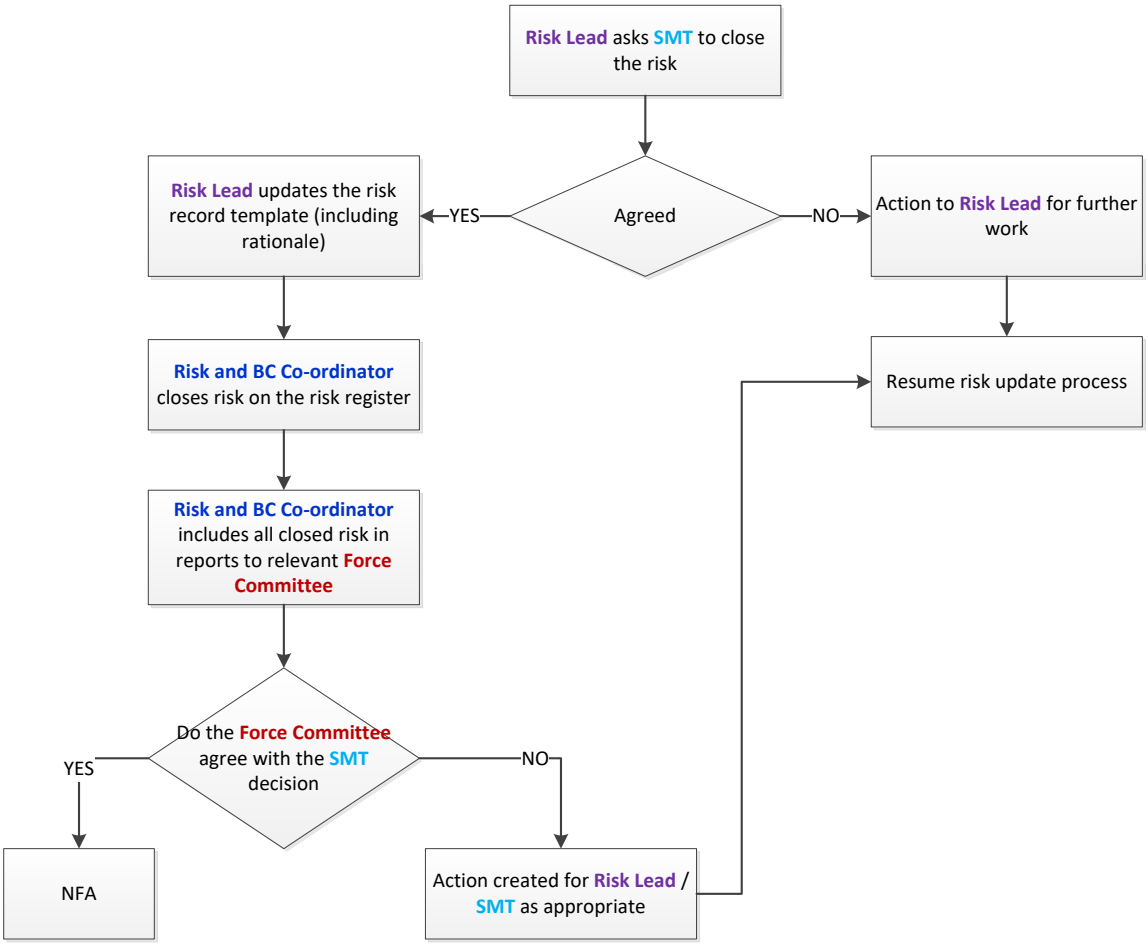
5.14.1 New Risk Creation for the Force Risk Register



5.14.2 **Updating Force Risks/Ongoing Force Risks on the Force Risk Register**



5.14.3 **Closing Force Risks on the Force Risk Register**



5.14.4 **Assurance Mapping**