Northern Ireland Ambulance Service
Health and Social Care Trust

Title:	**Corporate Risk Management Strategy & Procedures**		
Author(s):	Katrina Keating, Risk Manager		
Ownership:	Maxine Paterson, Director of Planning, Performance & Corporate Services		
Date of SMT Approval:	5th April 2022	**Date of ARAC Approval:**	14th April 2022
Operational Date:	14th April 2022	**Review Date:**	April 2025
Version No:	9.0	**Supercedes:**	V.8
Key Words:	Risk Management, Governance, Accountability, Responsibility, Assurance, Risk Matrix, Likelihood, Impact, Risk Appetite, Risk Assessment, Mitigation, Action Plan		
Other Relevant Policies / Procedures:	Health and Safety Policy and Procedures, Risk Assessment Procedure, Complaints Policy, Board Assurance Framework, Information Governance Policies and Procedures, PPI Strategy, Serious Adverse Incidents (SAI) Procedure, Incident Reporting Procedure, Management of Medical Devices Policy, Claims Management Policy, Whistle Blowing Policy, Infection, Prevention & Control Policy & Procedures		

Version Control:			
Date:	**Version:**	**Author:**	**Comments:**
April 2022	9	Risk Manager	Scheduled review and the inclusion of new governance arrangements / revised appetite
April 2019	8	Risk Manager	Scheduled review
October 2016	7	Risk Manager	Full review
November 2013	6	Risk Manager	Editorial amendments
August 2013	5	Risk Manager	Full review
October 2010	4	Risk Manager	Committee structures modified
November 2009	3	Risk Manager	Ratified by Trust Board
September 2008	2	Risk Manager	
December 2006	1	Risk Manager	

1.0 INTRODUCTION:

How we manage risk directly impacts on how effective we are as an organisation.

1.1 Background:

This Corporate Risk Management Strategy has been developed to provide the Northern Ireland Ambulance Service Health and Social Care Trust (NIAS) with a suitable risk management framework to enhance strategic planning and prioritisation, assist in achieving objectives and strengthen the ability to be agile to respond to the challenges faced. NIAS intends to meet its objectives successfully, improve the delivery of its services and achieve value for money. This Risk Management Strategy will ensure that corporate risk management is an essential and integral part of business planning and decision-making.

This Strategy forms part of the Trust's corporate governance arrangements. It is integrally linked to the Board Assurance Framework (BAF), is aligned with the Strategy to Transform 2020-2026 and associated Corporate / Directorate / Service Area Plans. It reflects a range of risk management standards, current guidance and best practice (ISO 31000 Risk Management Principles and Guidelines, HM Treasury Orange Book etc.). See Appendix 5 for further information on ISO 31000.

Whilst risk practices have improved over time across the public sector, the volatility, complexity and ambiguity of the operating environment has increased, as have demands for greater transparency and accountability for managing the impact of risks. Public sector organisations cannot be risk averse and be successful[1].

1.2 Purpose:

The purpose of this Risk Management Strategy is to establish a framework for the effective and systematic management of risk. It has been developed to enable NIAS to manage its risk effectively, discharge its duties appropriately, and progress the successful delivery of both corporate and directorate aims and objectives (note incident reporting remains a separate process).

1.3 Objectives:

- Define risk management and set out the benefits of managing it effectively.
- Identify accountability and responsibility for the management of risk across NIAS.
- Provide a clearly understandable, structured framework that drives a consistent and continually improving approach to risk management and its implementation.
- Ensure that significant, existing and emerging risks to NIAS are effectively identified, assessed and controlled to an acceptable level, taking into account costs and resource requirements, whilst also supporting the identification of opportunities.
- Ensure that all such significant risks and controls are accurately recorded, monitored and reported, that relevant NIAS staff and Trust Board are kept informed, as appropriate, and relevant risk information is included in the Board Assurance Framework, Governance Statements etc.
- Ensure that risk management is embedded within business planning and performance management processes, and that NIAS applies a best practice approach to risk management (aligned to relevant NHS risk management requirements).

[1] The Orange Book (publishing.service.gov.uk)

- Reduce injury, damage, loss and inconvenience to patients / clients / service users arising from or connected with the delivery of services.
- Contribute to compliance with relevant legal and regulatory requirements.
- Effective use of resources (staff, financial resources etc.).
- Reduce risk to reputation (including a reduced risk of misinterpretation by the media).
- A reduction in service disruptions.
- Opportunities are exploited and innovation is supported.
- That there are fewer 'surprises'.

2.0 SCOPE:

This Strategy applies to all those working within, providing services to or acting on behalf of the Northern Ireland Ambulance Service Health and Social Care Trust (NIAS). There are no exceptions.

3.0 ROLES AND RESPONSIBILITIES:

3.1 The Chief Executive as accounting officer is responsible for:

- Demonstrating leadership and continual commitment to risk management.
- Periodically assessing whether the organisational values, leadership style, opportunities for debate and learning, and human resource policies support the desired risk culture, incentivise expected behaviours and sanction inappropriate behaviours.
- Ensuring that expected values and behaviours are communicated and embedded at all levels to support the appropriate risk culture.
- Ensuring that an overall approach to risk management is in place, along with an effective risk management framework.
- Ensuring that that roles and responsibilities are communicated, understood and embedded at all levels.
- Designating an individual officer responsible for leading the risk management approach.
- Ensure the appropriate allocation of support and resources for risk management.
- Ensuring that there is a clear process for bringing significant issues to the attention of senior management / Trust Board.

3.2 Director of Planning, Performance & Corporate Services:

As the Director responsible for risk management, the Director of Planning, Performance & Corporate Services is responsible for:

- Ensuring risk is effectively managed across NIAS through suitable policies, processes, procedures and accountabilities, and that internal governance procedures provide adequate assurance that they are suitable and sufficient.
- Deputising for the Chief Executive with regards to risk management; leading on the implementation of the Corporate Risk Management Policy and Strategy across NIAS; and ensuring the policy, strategy and procedures are regularly reviewed, based on continual improvement.
- Regular reporting to Trust Board and Audit and Risk Assurance Committee.

3.3 Trust Board:

Overall responsibility for risk management and governance across NIAS, including:

- Providing visible leadership for effective risk management, promoting an open and non-judgemental approach, and encouraging the identification of opportunities for improvement as well as managing risks to the organisation/service delivery.
- Ensuring that the Trust has in place a fully functioning committee structure.
- Monitoring progress against the risk management strategy, ensuring that risk management is suitably resourced, risks are at least adequately controlled, and opportunities for continual improvement are identified.
- Reviewing the Corporate Risk Register (principal risks) and any critical risks, and identifying / approving relevant action plans. This must be formally carried out at least annually.
- Supporting the Chief Executive and SMT in managing any significant risks that require additional / external resources to control to an acceptable level.
- Ensuring risk management is integrated into the Trust Board decision making process as appropriate, including all relevant strategy papers, contracts, partnerships and projects submitted to Trust Board.
- Informing the Governance Statement.
- Approval of the Board Assurance Framework.
- The appointment of a Non-Executive Director at Board level with responsibility for Risk and Governance (Internal Audit review of Board Secretariat arrangements).

3.4 <u>The Audit, Risk & Assurance Committee (ARAC) is responsible for:</u>

- Contributing to the establishment, review and maintenance of an effective system of integrated governance, risk management and internal control that supports the achievement of the organisation's objectives.
- Reviewing the findings of other significant assurance functions, both internal and external to the organisation, and monitor compliance with any work programmes as necessary.
- Reviewing and approving the Corporate Risk Management Policy and Strategy (including the risk appetite statement).
- Critically challenging risk assurance arrangements / frameworks for risks across the organisation including programmes and partnerships. See Appendix 7 – Risk Management Assurance Mapping.
- Critically challenging risk assurance arrangements / frameworks for <u>all</u> of the other board committees (Safety, Quality, Experience and Performance Committee, People, Finance and Organisational Development Committee and Remuneration Committee).
- Critically challenging assurance over the risk and control environment for services outsourced to external providers, including shared service arrangements.
- Reviewing and constructively challenging the Corporate Risk Register not less than twice per year, and that directorate / service area / programme / project risk registers are highlighted as necessary.
- Providing advice and guidance regarding 'acceptable' risks.
- Reviewing hot topics and emerging risks as necessary.
- Scrutinising action plans, reports etc. from statutory authorities such as RQIA and HSENI.
- Considering assurance from areas across the Trust to inform governance statements, including Controls Assurance Standards (CAS) and / or any replacement processes.
- Monitoring of the Board Assurance Framework not less than twice a year, and Directorate / service area / programme / project assurance frameworks as necessary.
- Communicating matters to Trust Board as necessary.

3.5 Directors & Assistant Directors are responsible for:

- Implementing the Corporate Risk Management process across their area of responsibility.
- Participating in Trust business planning and performance arrangements, taking into account the Strategy to Transform and relevant business plans, maintaining accurate risk registers and reporting as directed.
- The timely (immediate) escalation of relevant (critical) risks to SMT.
- Effective communication on risk management to all relevant staff.
- The provision and maintenance of appropriate training and resources within departments to support required competencies and effective risk management.
- Ensuring arrangements are in place for the identification of critical and common risks to NIAS, and / or common controls, with the aim of identifying actions that maximise effectiveness, make the most efficient use of NIAS resources, and ensure all relevant lessons and opportunities for improvement are shared.
- Formally reviewing all risks / risk registers on a monthly basis (agendas / minutes must be made available for the Risk Manager as appropriate).
- Ensuring that SMART based action plans are applied to risks requiring additional control measures.
- Arranging a half day workshop (at least annually), led by the Risk Manager / Performance Directorate as appropriate in order to refresh skills and fully review all risks.
- Ensuring arrangements are in place for line managers and staff to raise risks for formal scrutiny and review.
- Monitoring incidents, complaints, claims, SAIs, internal audit reports, involvement with regulators, advisory bodies etc. and escalating risks as appropriate.

3.6 All Employees:

Every NIAS employee, of every grade, in every role, and at every location, has a role to play in ensuring that the risks to our service users, our people and our organisation are minimised, so that the efficiency of the invaluable service we provide to society is maximised. This includes:

- Complying with all relevant policies and procedures (HCPC standards of proficiency and conduct apply to registrants).
- Applying a risk assessment methodology to all relevant ways of working, including both formal and dynamic approaches.
- Reporting risks perceived as not being effectively managed for review and the identification of additional/improved controls if required (note incident reporting remains a separate process).
- Exchanging best practice with other organisations/divisions/stations etc. where possible.
- Supporting each other, at all levels, in identifying ways that we can continually improve the management of risk across the organisation, so improving service efficiency.
- Following the Corporate Risk Management Policy and Strategy with regards to partnerships, contracted services, programmes and projects.

3.7 Risk Manager:

The Risk Manager is the subject expert and is responsible for the development and review of the Corporate Risk Management Policy and Strategy and associated documentation. The Risk Manager must ensure that up to date documentation is available and training /

workshops are carried out as necessary. The Risk Manager acts as risk management coordinator across the organisation, providing the framework, tools and techniques that ensure consistency (the Risk Manager is also the subject expert for Health and Safety).

The Risk Manager will liaise with Directors and Assistant Directors to ensure that Risk Registers are populated appropriately and are being effectively managed. The Risk Manager should bring any concerns / gaps / irregularities to the attention of the lead Director. The Risk Manager is there to assist and provide advice, but individuals must take ownership of the risks relevant to their areas of responsibility.

The Risk Manager is responsible for the upkeep of the Risk Management System (DATIX) and will compile risk information and prepare reports for committees.

The Risk Manager will benchmark both regionally and nationally and will maintain a close relationship with the Safety, Quality and Experience Directorate with a regular meeting structures in place.

3.8 Service Users / Members of the Public:

It must also be noted that we expect our service users / patients / clients / carers and members of the public to co-operate with us in ensuring we manage risks effectively to provide an efficient service and, whilst also recognising that we have limited control over such external influences, we will do everything reasonably practicable to work with them to achieve this.

3.9 Internal Audit:

Responsibility for formally reviewing Trust risk management arrangements as part of third line assurance arrangements, with the aim of providing objective commentary on their effectiveness and identifying opportunities for improvement. Undertakes audits to monitor compliance with assurance frameworks, reviews, self-assessments etc.

4.0 KEY PRINCIPLES:

4.1 Risk Management Definitions:

4.1.1 Risk Management:

The International Risk Management Standard ISO 31000:2018 defines risk as being 'the effect of uncertainly on objectives'. Risk Management is defined as 'coordinated activities to direct and control an organisation with regards to risk'. Risk management is about making the most of opportunities (making the right decisions) and about achieving objectives once those decisions are made. This is achieved through transferring risks, controlling risks and living with risks.

4.1.2 Risk Registers:

Risk Registers are records of identified and evaluated risks, maintained at a corporate and directorate (and where necessary service / programme / project) level. They are used to ensure all significant risks are visible, that the effectiveness of controls are monitored, that risks are prioritised, and that action plans are initiated where required. Within NIAS, Risk Registers are held electronically on the DATIX Risk Management System (each risk is

assigned a unique reference number (the Trust is in the process of making arrangements for risk owners to access DATIX directly; this will facilitate the complete removal of associated paper systems).

4.1.3 Risk, Hazard, Likelihood & Impact:

A hazard is anything with the potential to cause harm or loss, and a risk is measured by the combination of the likelihood (sometimes known as probability, frequency or chance) of an actual or perceived hazard occurring and the level of its impact on objectives, i.e. what harm would result should the hazard be realised.

NIAS uses the HSC Regional Matrix for the purposes of risk evaluation. The HSC matrix applies both numerical values and descriptors to both the impact of the consequences, and the likelihood of the event occurring (see Appendix 8 for full HSC Regional Tables).

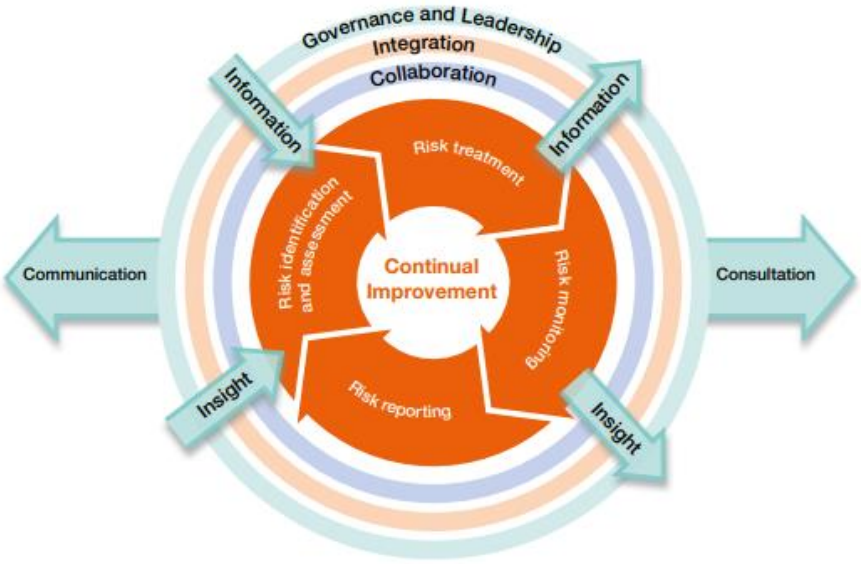
4.1.4 Control Measures:

A control measure is a measure that reduces the level of risk, either by reducing the likelihood of the risk actually occurring, or by reducing the adverse impact if it does occur. Control measures can be applied at the planning stage, throughout operations, following an incident etc. can take many forms including physical measures, procedures, training etc. Good control measures will normally comprise a combination of some or all of these, and will be subject to continual improvement.

Further definitions can be found in Appendix 11 – Risk Terminology.

4.2 Risk Management Framework:

The Trust risk management framework supports the consistent and robust identification and management of opportunities and risks within desired levels across an organisation, supporting openness, challenge, innovation and excellence in the achievement of objectives and mirrors best practice, i.e. ISO 31000 Risk Management Principles and Guidelines and HM Treasury Orange Book[2].



[2] The Orange Book (publishing.service.gov.uk)

Risk management is:

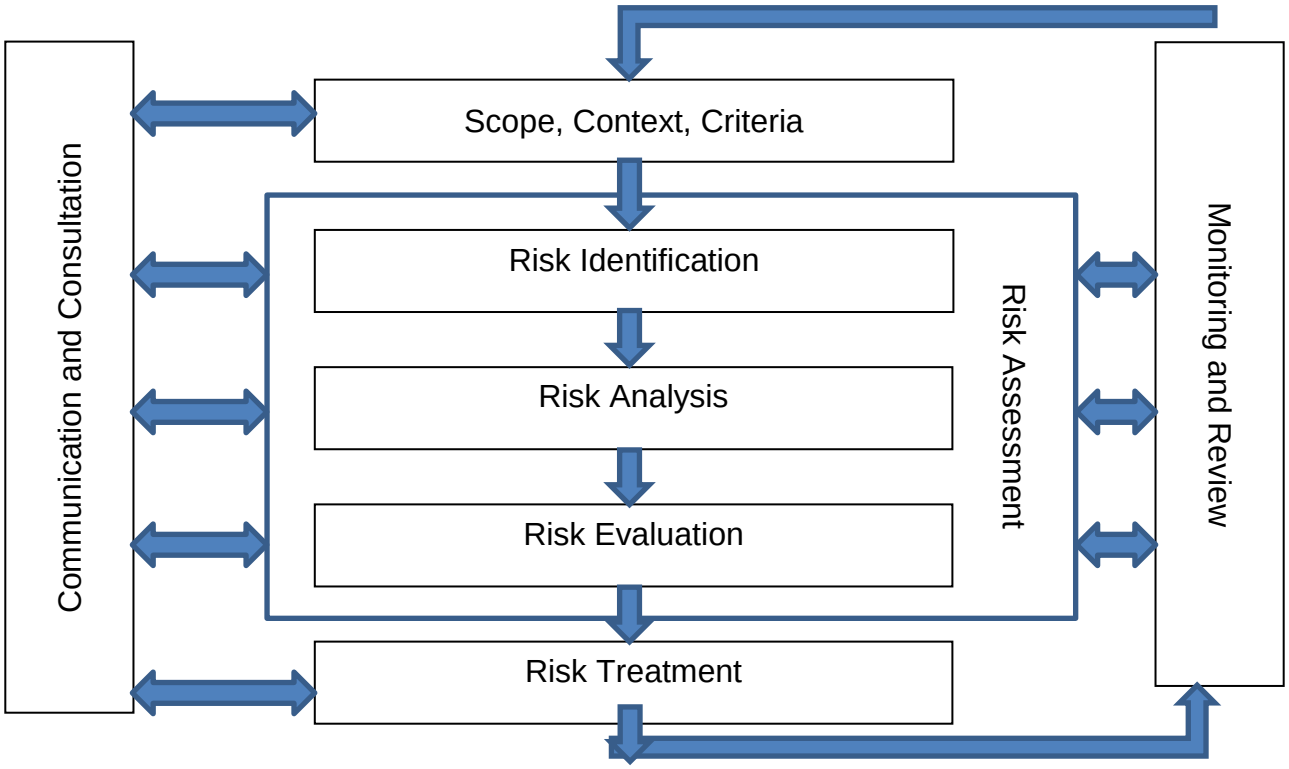
A. An essential part of governance and leadership, and fundamental to how the organisation is directed, managed and controlled at all levels.
B. An integral part of all organisational activities to support decision-making in achieving objectives.
C. Collaborative and informed by the best available information and expertise.
D. Structured to include:
    - risk identification and assessment to determine and prioritise how the risks should be managed;
    - the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
    - the design and operation of integrated, insightful and informative risk monitoring; and
    - timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

E. Continually improved through learning and experience.

4.3 Risk Management Process:

An effective Risk Management Process (based on ISO 31000) is summarised below:

Risk Rating = Impact / Likelihood



4.3.1 Establish Context & Identify Risks:

The Trust will employ a methodical approach to risk identification taking into account:

- Risks that might affect the achievement of objectives, i.e. risks linked to corporate objectives and operational risks linked to service provision need.

- Relevant business plans, project plans, KPIs, best practice, audit reports, clinical audit documentation, self-assessments, regulators, media reports, FOIs, complaints, performance reports, incident reports including SAIs etc.
- NIAS experience and the experiences of others, including those in other Ambulance Services, other Trusts, and relevant lessons from historical events / activities / incidents.
- Both external and internal factors, the actual or potential failure to exploit / manage opportunities and any cross cutting risks, i.e. whether any activity creates a risk to another part of the organisation.
- The cause / root cause of risk, i.e. what could trigger the risk, how is NIAS vulnerable etc.
- The frequency of the risk related tasks, who may be harmed, number of people who may be harmed, potential consequences etc.

The Risk Register Development Tool in Appendix 6 and the table of Risk Categories in Appendix 9 can be used to identify risks.

4.3.2 Risk Descriptions:

Risks will be described in a way that they can be understood by everyone. Each significant risk will be recorded separately to enable the accurate allocation of risk ratings, appropriate controls, grading and actions. Risk descriptions will comprise three elements:

A. Risk Cause – the source of the risk, the event/situation that gives rise to the risk.
B. Risk Event – the area of uncertainty, what will happen if the risk occurs (may or might terminology is often used).
C. Risk Effect – the impact the risk would have on the organisational activity.

Please see Appendix 10 for a risk description example.

4.3.3 Risk Analysis, Evaluation & Prioritisation:

The HSC Regional Risk Matrix at Appendix 8 is used to objectively analyse, evaluate and prioritise risks across NIAS, and ensure a consistent and comparable methodology across the HSC Trusts.

This simple methodology uses qualitative descriptors to identify quantitative scores for both the potential impact of a risk and the likelihood of it occurring. These ratings are then plotted on a final matrix which incorporates a traffic light system to determine whether the risk is evaluated as 'Low, Medium, High or Extreme', so facilitating prioritisation of action and application of the Trust escalation process (see Appendix 3).

4.3.4 Risk Appetite:

A key part of effective risk management is the setting of a Trust risk appetite. Risk appetite is the amount of risk the organisation is willing to accept. Risk appetite takes into consideration risk tolerance and risk capacity:

- *Risk tolerance* – is the amount of risk that the Trust is willing to tolerate. This is often used as a synonym to risk appetite, it is quite different, tolerances are more commonly quantitative in nature. They are thresholds that should guide staff when they are considering risks, so that they understand the levels that should not be exceeded, or those thresholds that if breached require further mitigation and monitoring.

- *Risk capacity* – is the level of impact that we can bear in the event of the risk occurring.

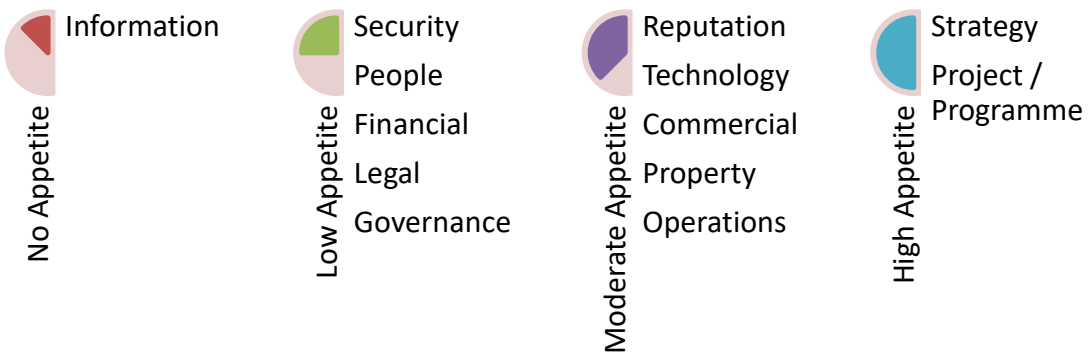
Each significant risk is assessed individually when deciding whether it is within our risk appetite (tolerable), or whether additional controls (terminate, treat or transfer) are required. Trust risk appetite is as follows:

Risk Appetite	What This Means
Extreme Risk – No Appetite	We are not prepared to accept uncertainly of outcomes for this type of risk.
High Risk – Low Appetite	We accept that a low level of uncertainly exists but expect that risks are managed to a level that may not substantially impede the ability to achieve objectives.
Moderate Risk – Moderate Appetite	We accept a moderate level of uncertainly but expect that risks are managed to a level that may only delay or disrupt achievement of objectives, but will not stop their progress.
Low Risk - High Appetite	We accept a high level of uncertainly and expect that risks many only be managed to a level that may significantly impede the ability to achieve objectives.
Low Risk - High Appetite	Will be recorded on risk register and reported to Emergency Planning Team

See Appendix 12 for an example of Risk Appetite Levels. Trust Risk Appetite has been included in HSC Matrix as follows:

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	**Insignificant(1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	**Medium / Moderate Appetite**	**Medium / Moderate Appetite**	**High / Low Appetite**	**Extreme / No Appetite**	**Extreme / No Appetite**
Likely (4)	**Low / High Appetite**	**Medium / Moderate Appetite**	**Medium / Moderate Appetite**	**High / Low Appetite**	**Extreme / No Appetite**
Possible (3)	**Low / High Appetite**	**Low / High Appetite**	**Medium / Moderate Appetite**	**High / Low Appetite**	**Extreme / No Appetite**
Unlikely (2)	**Low / High Appetite**	**Low / High Appetite**	**Medium / Moderate Appetite**	**High / Low Appetite**	**High / Low Appetite**
Rare (1)	**Low / High Appetite**	**Low / High Appetite**	**Medium / Moderate Appetite**	**High / Low Appetite**	**High / Low Appetite**

In addition, the following risk appetite principles are applied within NIAS listed by category (see Appendix 9 for further information on Risk Categories):



4.3.5 Existing Controls:

The risk analysis, evaluation and prioritisation process will then take into account any existing controls in order to ensure the risk rating score is accurate. Any such controls i.e. policies, procedures, training, devices, staffing, etc. that influence the likelihood of a risk occurring, or the impact should it occur, will be taken into account when identifying the relevant quantitative scores, whilst also considering the strengths or weaknesses of such controls, and whether there are opportunities for improvement.

4.3.6 Risk Treatment & Control:

Following risk analysis, evaluation and prioritisation, taking into account existing controls, the need for any further control action(s) must be identified and captured in action plans, which must be properly recorded to demonstrate both the assessment and decision making process.

Risk controls can be grouped into 4 main types:

- Terminate: Eliminate the risk i.e. remove the device, chemical; ban the practice, etc.

- Treat: Introduce control measures that will reduce the likelihood of the risk occurring and/or reduce the impact if it does incur.

- Transfer: Outsource the activity; take out insurance; engage contractors, etc. to reduce the risk exposure, bearing mind that residual risks may remain i.e. reputational risk

- Tolerate: Accept the risk. The risk may not be sufficiently significant; other priorities may apply; the cost of controlling the risk may be disproportionate to the benefits; control options may be very limited, etc.

Action plans must incorporate SMART principles:

S Specific – clearly defined actions to be completed, with clearly defined owners (both name and designation)
M Measurable – how will implementation and effectiveness be measured
A Aligned – actions and action plans must be aligned with relevant policies and procedures and agreed by relevant action owners
R Realistic – actions must be achievable, with sufficient resources, within agreed timescales
T Time bound – both target and actual completion dates should be captured

4.3.7 Revised Risk Rating:

Where a requirement for further risk control action is identified, and action plans initiated, the relevant risk rating must be revised to demonstrate how these actions will influence the risk rating score.

This is achieved by repeating the risk analysis; evaluation and prioritisation process i.e. applying the risk matrices at Appendix 8, and should result in a lower overall risk rating. If it does not result in a lower risk rating then the effectiveness/value of the additional controls should be challenged to ensure they justify implementation.

4.3.8 Monitoring & Review:

Risk registers should be continually monitored and subject to formal review on a regular basis:

a. Risk registers must be formally reviewed by relevant risk owners at least monthly.
b. Risk registers should be reviewed following the identification of new or emerging risks, or following relevant incidents including Serious Adverse Incidents (SAIs).
c. Reviewing of principle risks and risk registers at SMT meetings on a monthly basis.
d. Risk management summary reporting at ARAC & Trust Board.

Risk management action plans must also be continually monitored and reviewed on a regular basis, including:

- Inclusion in Directorate / management / team meeting agendas, with risk action owners providing updates.
- Ensuring controls are being progressed as agreed or, if not, identifying why not and what further action is required.
- Ensuring controls are being effective i.e. impacting on (reducing) risk ratings as anticipated.
- Any opportunities for continual improvement and identification of lessons worth sharing (positive or negative).
- Updating of risk registers, action plans, any other relevant documents/registers, and DATIX as applicable

Actions must stay open, and be formally tracked, until they are fully closed out, and it must be remembered that the main focus should be on the achievement of objectives, rather than the risk management process itself.

4.3.9 Escalation Process:

The risk analysis and evaluation will enable risks to be categorised in accordance with Appendix 9. The following table defines appropriate action/escalation requirements:

Risk Level	Action	Remedial Action	Decision to Accept	Risk Register	Action / Review
Extreme (Red)	Immediately refer to Director. Director to investigate, agree and oversee implementation of action plan. Director to consider requirement to escalate to Chief Executive and/or SMT and if necessary Trust Board Risk Manager informed ASAP.	Chief Executive or Director responsible	Senior Executive Management Team (SMT). Report to Trust Board if necessary.	Corporate (principal risk)	**Action immediately, review daily / weekly depending on particular requirements.** **Review at least monthly**
High (Amber)	Immediately refer to Director. Director / Assistant Director to	Director responsible or delegated	Director. Report to SMT and at	Corporate or Directorate (depending on organisational	**Action within one month.** **Review monthly**

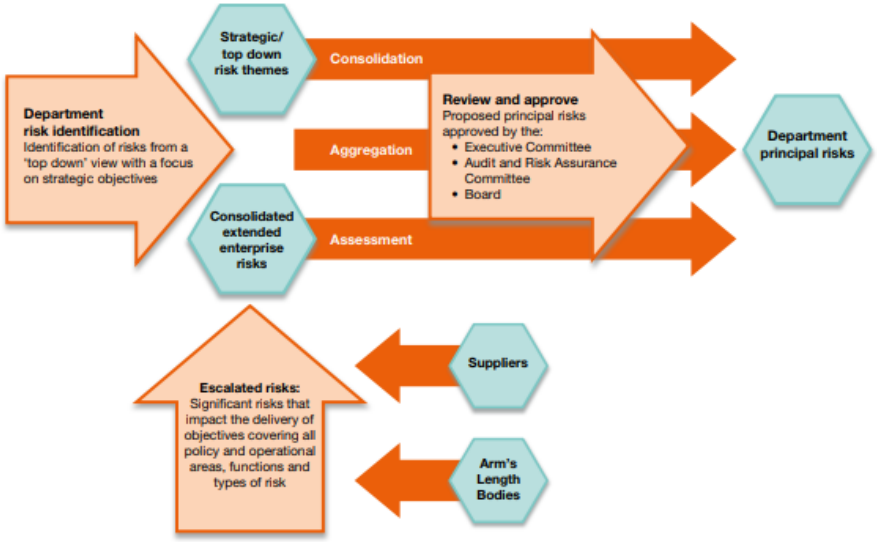
Risk Level	Action	Remedial Action	Decision to Accept	Risk Register	Action / Review
	investigate, agree and oversee implementation of action plan. Risk Manager informed.	Assistant Director	Directorate Meetings.	impact and action plan)	
Medium (Yellow)	Action and monitor within area by Assistant Director / Area Manager / equivalent local manager. Risk Manager kept informed.	Assistant Director / Area Manager or delegated Station Officer or equivalent	Assistant Director. Report at Directorate Meetings.	Directorate / Service Area	**Action within three to six months (depending on organisational impact and action plan).** **Review monthly**
Low (Green)	Monitored and reviewed regularly to ensure controls remain in place. Assistant Director and Risk Manager kept informed.	Station Officer / Supervisor or equivalent	Area Manager or delegated Station Officer Report at Directorate Meetings.	Directorate / Service Area as appropriate	**Accept risk and/or carry out any actions within nine – twelve months.** **Review monthly**

The Risk Manager will monitor the escalation and de-escalation process. See Appendix 1 for the Risk Management Communication Structure. See Appendix 3 Recording and Escalating Risks and Appendix 4 De-escalation and Closure of Risks (Flow Charts).

4.3.10 Risk Escalation, Consolidation & Aggregation:

NIAS risk management framework has been designed to be collaborative and informed by the best available information and expertise. Risk management processes will be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of experts and stakeholders.

NIAS employs both a 'top down' and 'bottom up' approach to the implementation of this Corporate Risk Management Strategy as set out in best practice guidance, HM Treasury Orange Book[3].



[3] The Orange Book (publishing.service.gov.uk)

4.3.11 Corporate Risk Register (Principal Risks):

The Corporate Risk Register details the principle (key) risks to the organisation, it will normally comprise more than one of the following:

- Has been evaluated as a High or Extreme risk.
- The risk will have an adverse and significant impact on the achievement of strategic objectives
- The risk has implications beyond the immediate area of control and/or cannot be managed within the immediate area of control.
- Existing standards and guidance ignore or contribute to the risk.
- The risk requires escalation to another HSC body and/or needs the involvement of Commissioner(s).

Although captured in the Corporate Risk Register such risks can also be included in directorate risk registers, and will generally still be owned by a relevant director and/or a specific committee or subcommittee.

4.4 Risk Management in Partnerships & Contracted Services:

The Audit Commission defines partnership working as “an agreement between two or more independent bodies to work collectively to achieve an objective”. Whilst there are opportunities, there are risks associated with partnerships and contracting services. This can be complex, create confusion and weaken accountability; the principles of accountability remain.

For each of the Trust’s key partnerships, a detailed joint risk assessment should be undertaken. Questions should be asked about the risk management process within the partner/contracted organisation and arrangements for risk management should be agreed. Procedures should be in place to ensure that key risks are adequately reported, assessed, controlled and monitored. Risk management is the shared responsibility of the partner/contractor and NIAS, and registers should be reviewed as part of the ongoing contract management meetings. Some of the risks which might be encountered include:

- Contract requirements are not delivered.
- Contractor failure during the term of the contract.
- Capital investment ‘squandered’ on non-productive schemes.
- Changing organisational priorities.
- Front line efficiencies are not captured.
- Imposition of targets rather than negotiation of manageable targets.
- Loss of control over staff and the service but with retention of accountability.
- No ownership by local delivery agents.

Directors must ensure that risks have been considered in any partnerships and contracts. This includes suitable arrangements for the use of contractors and agency staff, including suitable procedures for professional, clinical registration checks, reporting, monitoring and review. As part of these arrangements; Directors should assure themselves of the arrangements for the training of responders and volunteers not directly employed by NIAS and ensure that the appropriate scope of practice is set out for all. Appropriate risk management arrangements must also be put in place for work with charities.

4.5 Risk Management in Projects / Programmes:

Directors must ensure that corporate arrangements for risk management are followed for project / programmes risks. All projects/programmes / service developments must incorporate and be supported by the appropriate risk management documentation and entered into DATIX. HSC Matrix must be used.

4.6 Risk Management Training:

All staff will attend training appropriate to their responsibility. Risk Management training will be delivered as part of induction and as part of the Trust's continuing professional development for all staff. Everyone should receive specific risk management training as follows:

- At induction.
- Upon promotion, where the level of risk management authority is to increase.
- On appointment at Board Level / Committee level.
- As part of the Trusts statutory / mandatory training program (every three years).
- As part of specialist training for example fire safety, IPC, moving and handling etc.

Training will be delivered using a variety of methods, for example face to face, learning packs, workshops, observation in practice. A risk management eLearning package is available. Records will be held by the Risk Management Team via HRPTS.

5.0 IMPLEMENTATION OF PROCEDURE:

5.1 Dissemination:

With regards to dissemination this Corporate Risk Management Strategy (and the Corporate Risk Management Policy) has been:

- Issued to all Board Members, Chair, Non-Executive Directors, Chief Executive, Directors and Assistant Directors.
- Disseminated to all staff by Assistant Directors.
- Made available on the Internet, Intranet and SharePoint so that all employees and members of the public/stakeholders can easily have access.
- Posted on the notice boards in all operational areas.
- Discussed in Corporate Induction, Employee Resource Packs and Workbooks.

5.2 Resources:

Training on the application of this procedure for relevant managers and staff will be facilitated / delivered by the Risk Management Team

.

5.3 Exceptions:

This Strategy applies to all those working within, providing services to or acting on behalf of the Northern Ireland Ambulance Service Health and Social Care Trust. There are no exceptions.

6.0 MONITORING:

It is the responsibility of Trust Board and the Audit and Risk Assurance Committee to monitor the implementation of and assess the level of compliance with this procedure.

7.0 EVIDENCE BASE/REFERENCES:

- The Orange Book – Management of Risk – Principles & Concepts. HM Government.
- ISO 31000 Risk Management Principles and Guidelines.
- Risk Management Standard for Ambulance Services – NHSLA 2013-14.
- Enterprise Risk Management – Institute of Risk Management.
- Corporate governance code for central government departments. HM Government.
- The Principles of Managing Risks to the Public. HM Government.

8.0 CONSULTATION PROCESS:

This Corporate Risk Management Strategy (and the Corporate Risk Management Policy) has been:

- Drafted in consultation with the Director of Planning, Performance and Corporate Services, Finance Director, Chief Executive, Directors and Assistant Directors.
- Ratified by SMT for presentation to Audit and Risk Assurance Committee.
- Approved by the Trust's Audit and Risk Assurance Committee.

The Corporate Risk Management Policy and Strategy will be reviewed every three years.

9.0 APPENDICES:

Appendix 1 – Risk Management Communication Structure.
Appendix 2 – Committee Structure.
Appendix 3 – Recording & Escalating Risks.
Appendix 4 – De-escalation & Closure of Risks.
Appendix 5 – ISO 31000 2018 Risk Management Standard:
Appendix 6 – Developing Your Risk For The Risk Register.
Appendix 7 – Risk Management Assurance Mapping.
Appendix 8 – Regional HSC Risk Management Matrix.
Appendix 9 – Risk Categories.
Appendix 10 – Risk Descriptions.
Appendix 11 – Risk Terminology.
Appendix 12 – Example Appetite Levels Defined By Risk Categories

10.0 EQUALITY STATEMENT:

10.1 In line with duties under Section 75 of the Northern Ireland Act 1998; Targeting Social Need Initiative; Disability Discrimination Act 1995 and the Human Rights Act 1998, an initial screening exercise, to ascertain if this policy should be subject to a full impact assessment, has been carried out.

10.2 The outcome of the equality screening for this procedure undertaken on the 1st April 2022 is:

Major impact ☐

Minor impact ☐

No impact. ✓

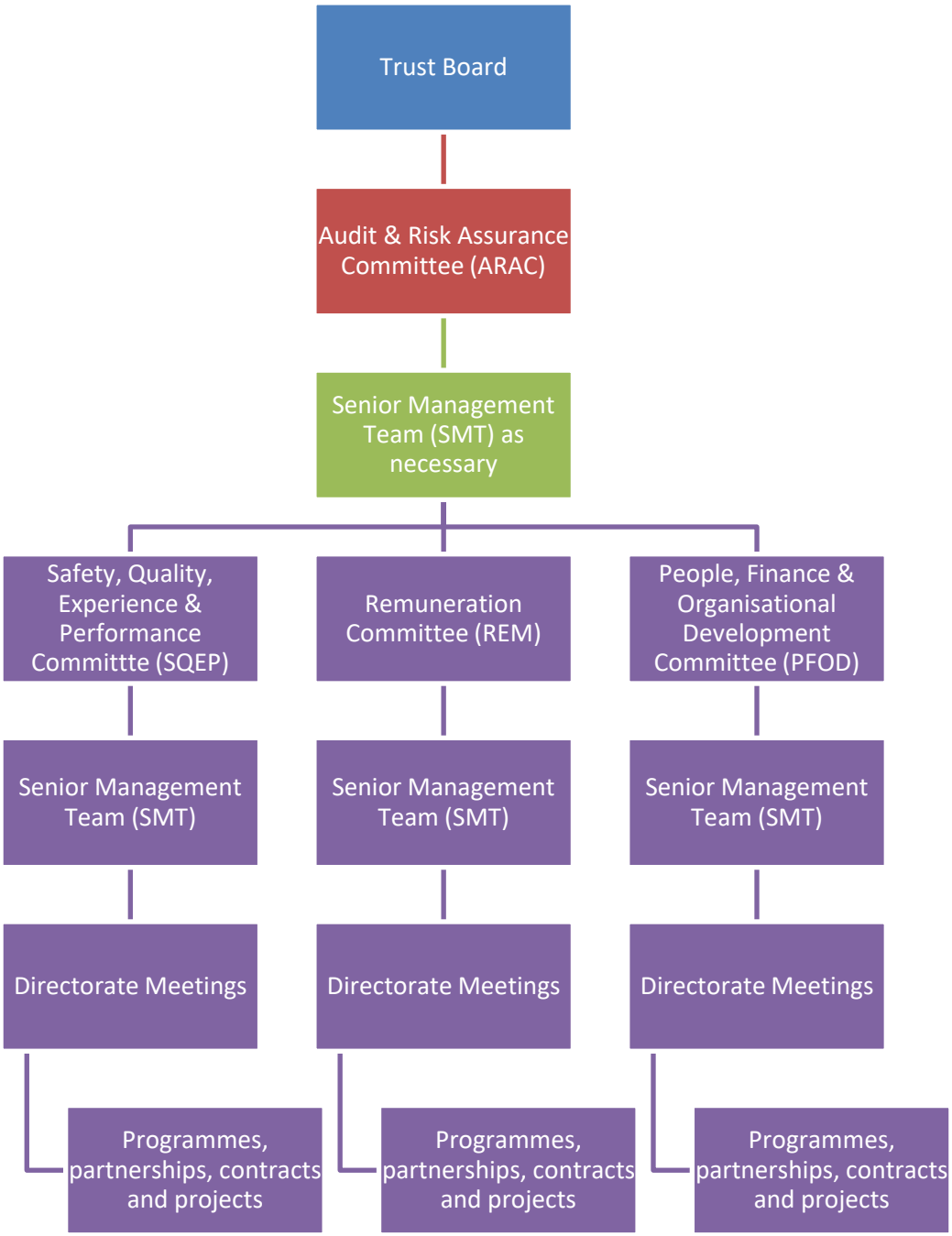
10.0 SIGNATORIES:

Katrina Keating **Date: 14th April 2022**
Lead Author

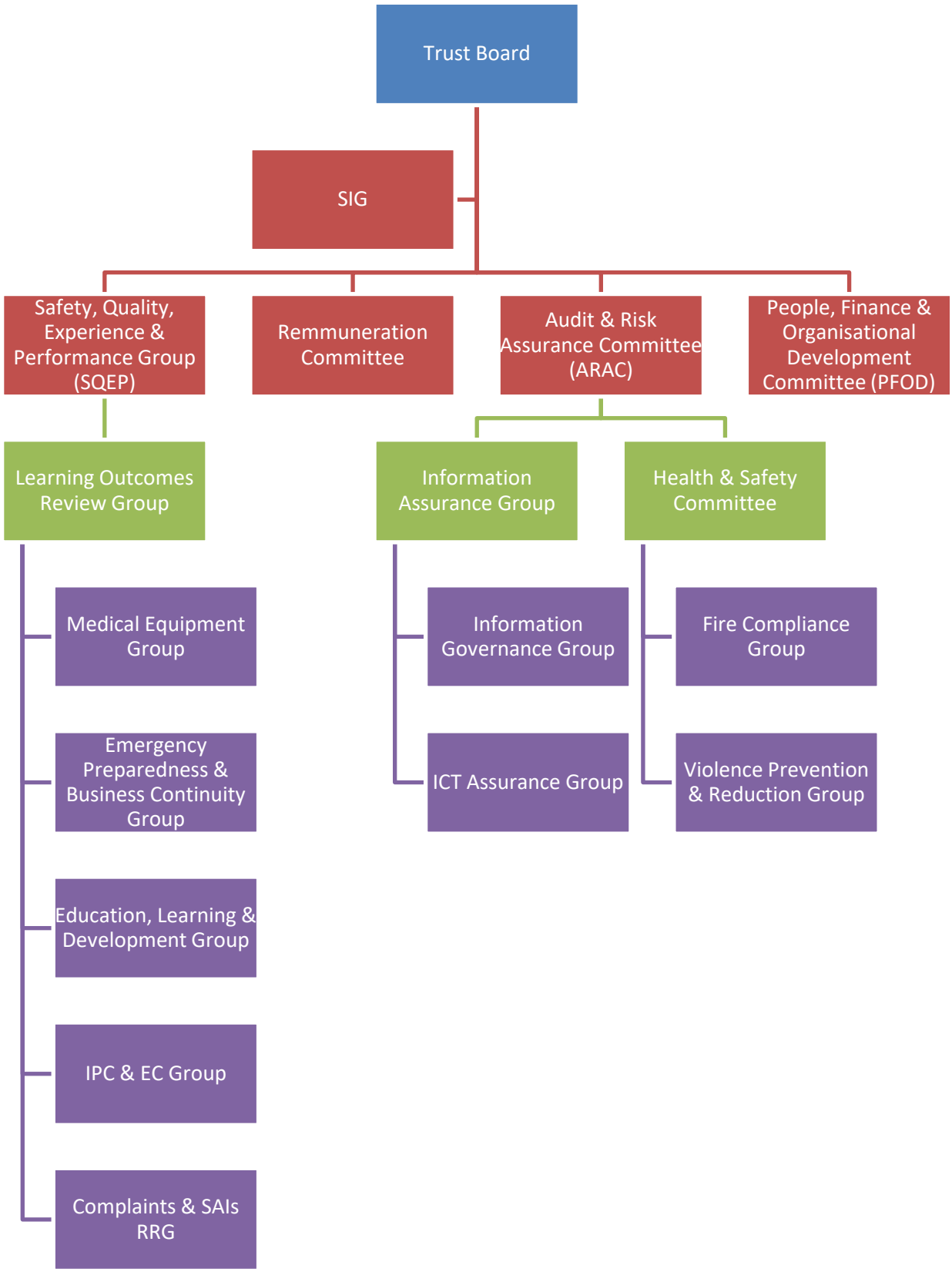
Maxine Paterson **Date: 14th April 2022**
Lead Director

APPENDIX 1 – RISK MANAGEMENT COMMUNICATION STRUCTURE:

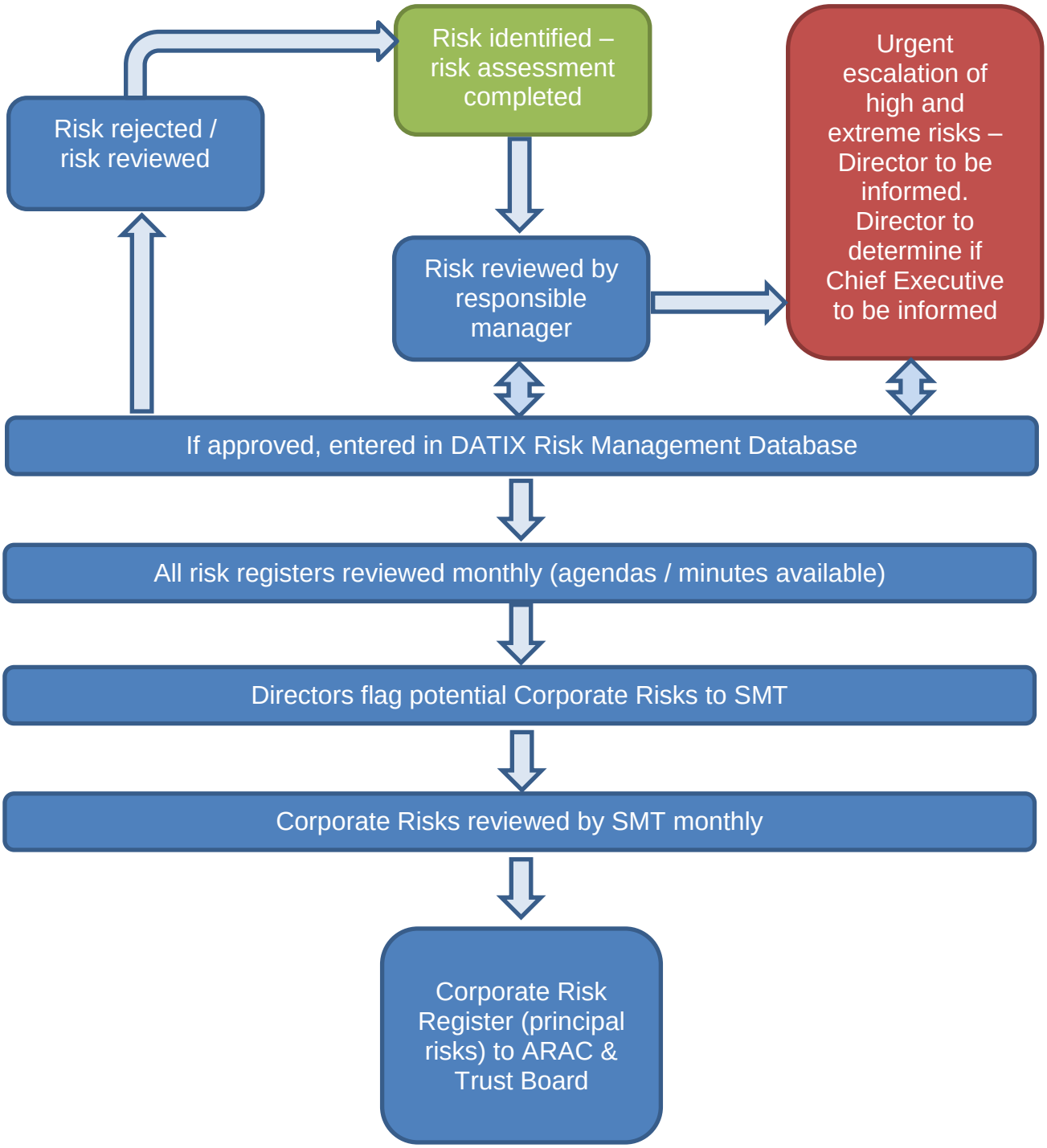
This structure identifies the lines of communications for identification, management and escalation of risks throughout NIAS.



APPENDIX 2 – COMMITTEE STRUCTURE (INCORPORATING WORKING GROUPS THAT SUPPORT THE COMMITTEES) – NOTE UNDER REVIEW:



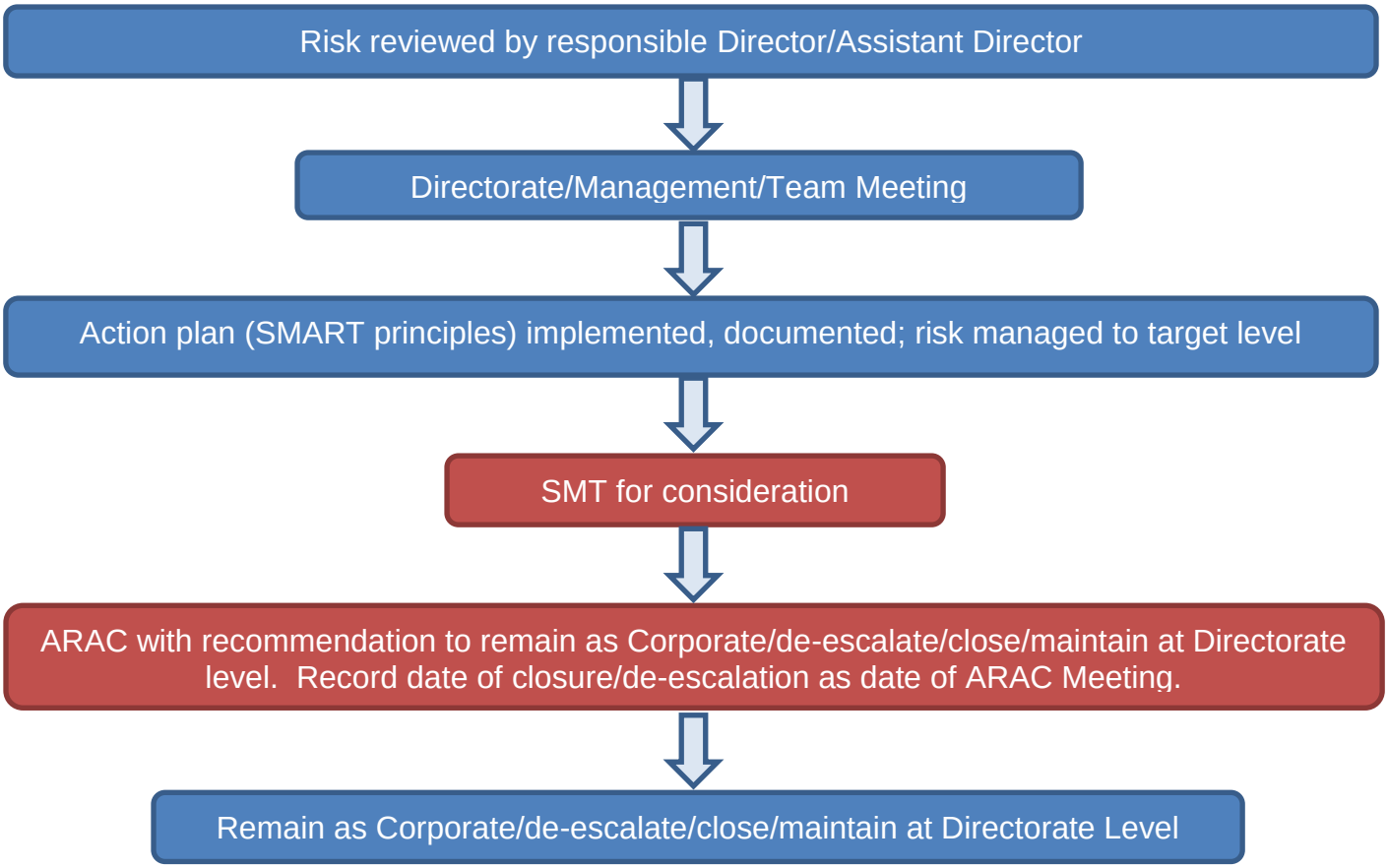
APPENDIX 3 – RECORDING & ESCALATING RISKS:



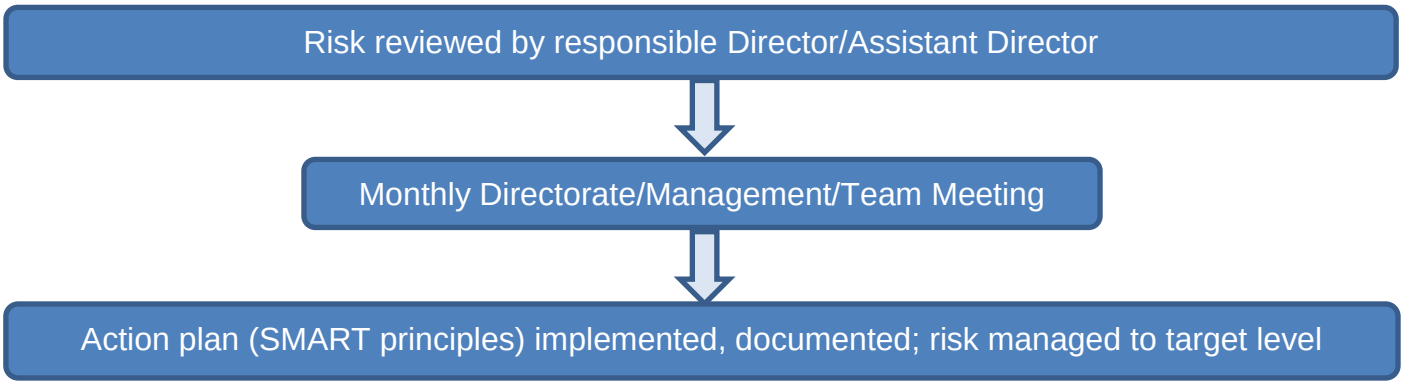
NOTE: Risk Owners are responsible for contacting the Risk Manager to arrange regular workshops and keeping risks / DATIX up to date at all times

APPENDIX 4 – DE-ESCALATION & CLOSURE OF RISKS:

CORPORATE / PRINCIPLE RISKS

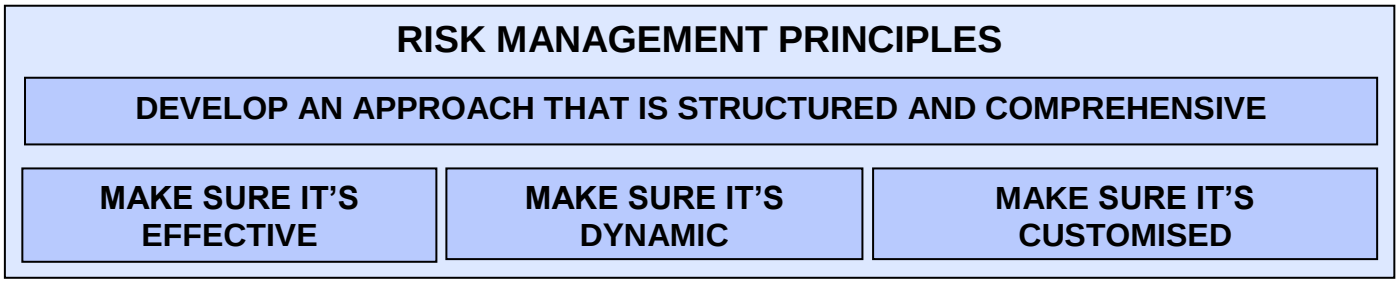


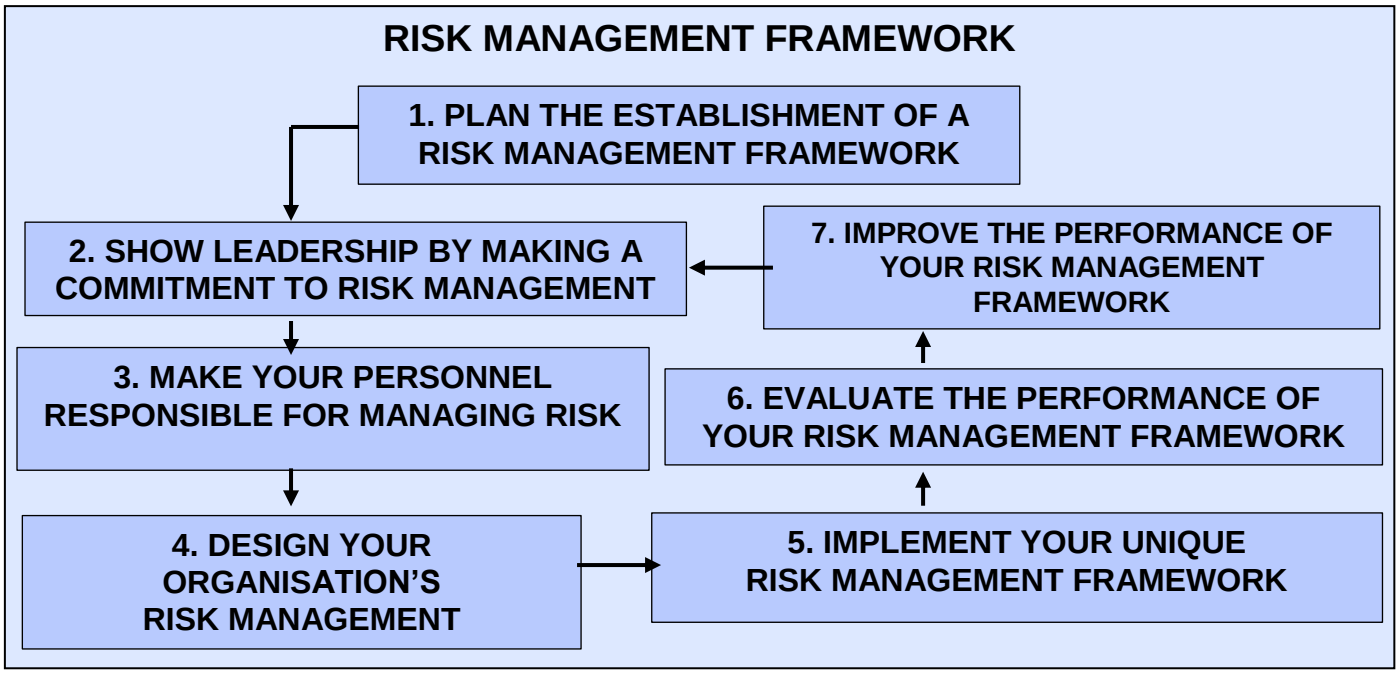
DIRECTORATE RISKS

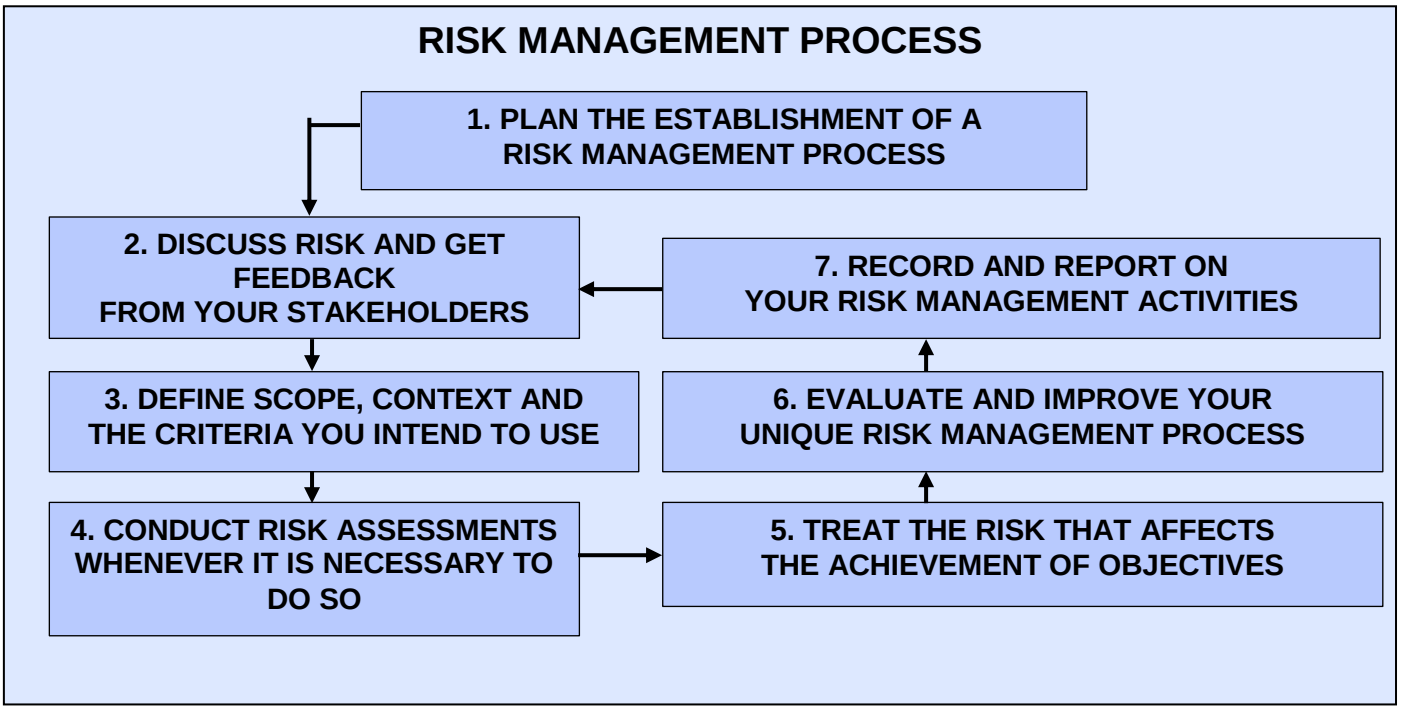


NOTE risks / DATIX must be kept up to date at all stages

APPENDIX 5 – ISO 31000 2018 RISK MANAGEMENT STANDARD:







APPENDIX 6

RISK REGISTER DEVELOPMENT TOOL

Key Themes *(please tick the one most relevant)*			
Motivated & Engaged Workforce		Clinical Excellence at Our Heart	
Right Resources to Patients Quickly		Recognised for Innovation	
Improving Experience & Outcomes for Patients		Effective, Ethical, Collective Leadership	

Risk Description: *Cause/event/effect (see Appendix 9 of the Risk Management Strategy for further information)*	**DATIX ID**	

Controls				
Existing Controls	**Further Action To Control Risk**	**Person Responsible**	**Target Date**	**Date Completed**

Risk Rating *(see Appendix 8 of the Risk Management Strategy for further information)*								
Initial (Without Control Measures)			**Current (With Existing Control Measures)**			**Target Rating**		
Impact	**Likelihood**	**Rating**	**Impact**	**Likelihood**	**Rating**	**Impact**	**Likelihood**	**Rating**

Assurances On Controls (where we gain evidence that our controls are effective). Assurance Mapping Tool can be used to assist.	
Positive Assurances	**Gaps In Assurance**

Risk Category (✓)							
Strategy		Property		People		Security	
Governance		Financial		Technology		Project / Programme	
Operations		Commercial		Information		Reputation	
Legal							

Accountable Director:		**Directorate:**		**Date:**	
Person Responsible:		**Directorate:**		**Date:**	

Agreed Directorate Meeting (✓)	**Yes**		**No**		**Comment:**		**Date:**	
Entered onto DATIX	**Yes**		**No**		**Comment:**		**Date:**	

APPENDIX 7 – RISK MANAGEMENT ASSURANCE MAPPING:

Assurance Mapping										
Sources of Assurance										
Risk / Key Process / Significant Change etc.	**Owner**	**1st Line of Defence (Business Management)**	**Level**	**2nd Line of Defence (Corporate Oversight)**	**Level**	**3rd Line of Defence (Independent Assurance)**	**Level**	**Sufficient?**	**Gaps**	**Improvement Actions**
Management of Risk	Director of Planning, Performance & Corporate Services Risk Manager	• Risk Management Policy & Strategy, i.e. identify, assess, own and manage risks, effective internal control measures, monitor / address deficiencies. • Annual Risk Management Workshops. • DATIX authorisations. • Monthly review of all registers at team meetings. • Incident reporting and learning.	**A**	• Agreed assurance Framework. • Monthly review of Corporate Risk Register by SMT. • Receipt of assurance by Audit and Risk Assurance Committee (annual report). • Corporate Risk Register to ARAC twice a year and Trust Board Annually.	**A**	BSO Internal Audit.	**A**	Yes	1. Revised policy.	1. Ongoing consultation and tabling at ARAC

Low Assurance	**Red**
Medium Assurance	**Amber**
High Assurance	**Green**

HSC Regional Impact Table – with effect from April 2013 (updated)					
APPENDIX 8	**IMPACT (CONSEQUENCE) LEVELS [can be used for both actual and potential]**				
DOMAIN	**INSIGNIFICANT (1)**	**MINOR (2)**	**MODERATE (3)**	**MAJOR (4)**	**CATASTROPHIC (5)**
PEOPLE *(Impact on the Health/Safety/Welfare of any person affected: e.g. Patient/Service User, Staff, Visitor, Contractor)*	• Near miss, no injury or harm.	• Short-term injury/minor harm requiring first aid/medical treatment. • Any patient safety incident that required extra observation or minor treatment e.g. first aid • Non-permanent harm lasting less than one month • Admission to hospital for observation or extended stay (1-4 days duration) • Emotional distress (recovery expected within days or weeks).	• Semi-permanent harm/disability (physical/emotional injuries/trauma) (Recovery expected within one year). • Admission/readmission to hospital or extended length of hospital stay/care provision (5-14 days). • Any patient safety incident that resulted in a moderate increase in treatment e.g. surgery required	• Long-term permanent harm/disability (physical/emotional injuries/trauma). • Increase in length of hospital stay/care provision by >14 days.	• Permanent harm/disability (physical/ emotional trauma) to more than one person. • Incident leading to death.
QUALITY & PROFESSIONAL STANDARDS/ GUIDELINES *(Meeting quality/ professional standards/ statutory functions/ responsibilities and Audit Inspections)*	• Minor non-compliance with internal standards professional standards, policy or protocol. • Audit / Inspection – small number of recommendations which focus on minor quality improvements issues.	• Single failure to meet internal professional standard or follow protocol. • Audit/Inspection – recommendations can be addressed by low level management action.	• Repeated failure to meet internal professional standards or follow protocols. • Audit / Inspection – challenging recommendations that can be addressed by action plan.	• Repeated failure to meet regional/ national standards. • Repeated failure to meet professional standards or failure to meet statutory functions/ responsibilities. • Audit / Inspection – Critical Report.	• Gross failure to meet external/national standards. • Gross failure to meet professional standards or statutory functions/ responsibilities. • Audit / Inspection – Severely Critical Report.
REPUTATION *(Adverse publicity, enquiries from public representatives/media Legal/Statutory Requirements)*	• Local public/political concern. • Local press < 1day coverage. • Informal contact / Potential intervention by Enforcing Authority (e.g. HSENI/NIFRS).	• Local public/political concern. • Extended local press < 7 day coverage with minor effect on public confidence. • Advisory letter from enforcing authority/increased inspection by regulatory authority.	• Regional public/political concern. • Regional/National press < 3 days coverage. Significant effect on public confidence. • Improvement notice/failure to comply notice.	• MLA concern (Questions in Assembly). • Regional / National Media interest >3 days < 7days. Public confidence in the organisation undermined. • Criminal Prosecution. • Prohibition Notice. • Executive Officer dismissed. • External Investigation or Independent Review (e.g., Ombudsman). • Major Public Enquiry.	• Full Public Enquiry/Critical PAC Hearing. • Regional and National adverse media publicity > 7 days. • Criminal prosecution – Corporate Manslaughter Act. • Executive Officer fined or imprisoned. • Judicial Review/Public Enquiry.
FINANCE, INFORMATION & ASSETS *(Protect assets of the organisation and avoid loss)*	• Commissioning costs (£) <1m. • Loss of assets due to damage to premises/property. • Loss – £1K to £10K. • Minor loss of non-personal information.	• Commissioning costs (£) 1m – 2m. • Loss of assets due to minor damage to premises/ property. • Loss – £10K to £100K. • Loss of information. • Impact to service immediately containable, medium financial loss	• Commissioning costs (£) 2m – 5m. • Loss of assets due to moderate damage to premises/ property. • Loss – £100K to £250K. • Loss of or unauthorised access to sensitive / business critical information • Impact on service contained with assistance, high financial loss	• Commissioning costs (£) 5m – 10m. • Loss of assets due to major damage to premises/property. • Loss – £250K to £2m. • Loss of or corruption of sensitive / business critical information. • Loss of ability to provide services, major financial loss	• Commissioning costs (£) > 10m. • Loss of assets due to severe organisation wide damage to property/premises. • Loss – > £2m. • Permanent loss of or corruption of sensitive/business critical information. • Collapse of service, huge financial loss
RESOURCES *(Service and Business interruption, problems with service provision, including staffing (number and competence), premises and equipment)*	• Loss/ interruption < 8 hour resulting in insignificant damage or loss/impact on service. • No impact on public health social care. • Insignificant unmet need. • Minimal disruption to routine activities of staff and organisation.	• Loss/interruption or access to systems denied 8 – 24 hours resulting in minor damage or loss/ impact on service. • Short term impact on public health social care. • Minor unmet need. • Minor impact on staff, service delivery and organisation, rapidly absorbed.	• Loss/ interruption 1-7 days resulting in moderate damage or loss/impact on service. • Moderate impact on public health and social care. • Moderate unmet need. • Moderate impact on staff, service delivery and organisation absorbed with significant level of intervention. • Access to systems denied and incident expected to last more than 1 day.	• Loss/ interruption 8-31 days resulting in major damage or loss/impact on service. • Major impact on public health and social care. • Major unmet need. • Major impact on staff, service delivery and organisation - absorbed with some formal intervention with other organisations.	• Loss/ interruption >31 days resulting in catastrophic damage or loss/impact on service. • Catastrophic impact on public health and social care. • Catastrophic unmet need. • Catastrophic impact on staff, service delivery and organisation - absorbed with significant formal intervention with other organisations.
ENVIRONMENTAL *(Air, Land, Water, Waste management)*	• Nuisance release.	• On site release contained by organisation.	• Moderate on site release contained by organisation. • Moderate off site release contained by organisation.	• Major release affecting minimal off-site area requiring external assistance (fire brigade, radiation, protection service etc.).	• Toxic release affecting off-site with detrimental effect requiring outside assistance.

HSC REGIONAL RISK MATRIX – WITH EFFECT FROM APRIL 2013 (Updated)

Risk Likelihood Scoring Table			
Likelihood Scoring Descriptors	Score	**Frequency (How often might it/does it happen?)**	**Time framed Descriptions of Frequency**
Almost certain	5	Will undoubtedly happen/recur on a frequent basis	Expected to occur at least daily
Likely	4	Will probably happen/recur, but it is not a persisting issue/circumstances	Expected to occur at least weekly
Possible	3	Might happen or recur occasionally	Expected to occur at least monthly
Unlikely	2	Do not expect it to happen/recur but it may do so	Expected to occur at least annually
Rare	1	This will probably never happen/recur	Not expected to occur for years

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	**Insignificant(1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Likely (4)	**Low**	**Medium**	**Medium**	**High**	**Extreme**
Possible (3)	**Low**	**Low**	**Medium**	**High**	**Extreme**
Unlikely (2)	**Low**	**Low**	**Medium**	**High**	**High**
Rare (1)	**Low**	**Low**	**Medium**	**High**	**High**

APPENDIX 9 – RISK CATEGORIES – The following table lists potential sources of risk. The examples given are neither prescriptive nor exhaustive, but rather provide a useful framework for identifying and categorising a broad range of risks facing the organisation.

Strategy	Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).
Governance	Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
Operations	Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money
Legal	Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).
Property	Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public
Financial	Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.
Commercial	Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.
People	Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.
Technology	Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
Information	Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.
Security	Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.
Project / Programme	Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
Reputation	Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

APPENDIX 10 – RISK DESCRIPTIONS:

Risks must be described in a way that they can be understood by everyone. Each significant risk should be recorded separately to enable the accurate allocation of risk ratings, appropriate controls, grading and actions.

Risk descriptions should comprise three elements:

A. Risk Cause – the source of the risk, the event/situation that gives rise to the risk.
B. Risk Event – the area of uncertainty, what will have if the risk occurs (may or might terminology is often used).
C. Risk Effect – the impact the risk would have on the organisational activity.

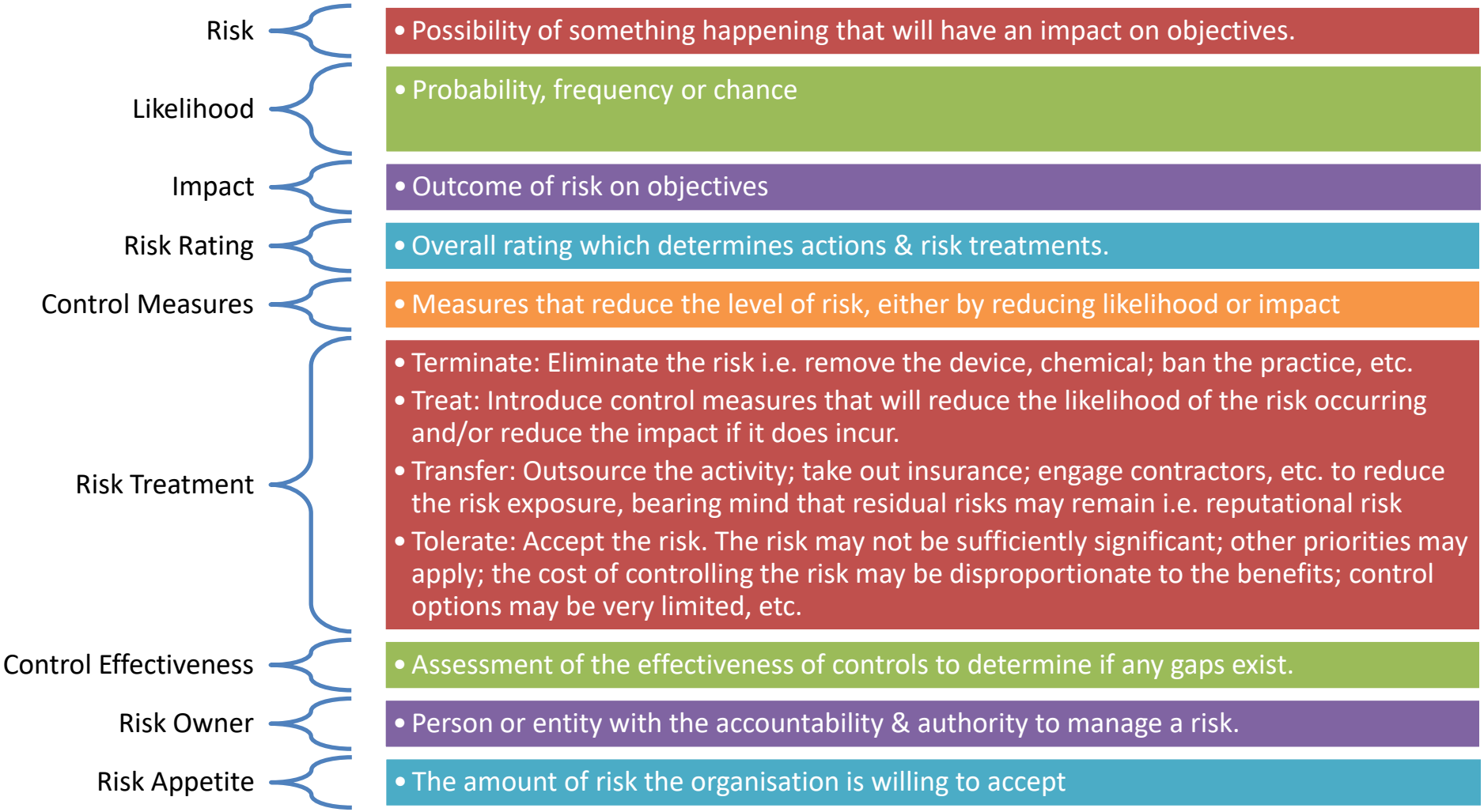
Applying this approach ensures clarity of understanding and, importantly, supports the identification of a range of potential controls which may be applied at the cause, event of effect stage, or any combination thereof.

For example…If the fixed electrical installation is not maintained (risk cause) this may result in a fire in the control room (risk event) which would lead to the inability to answer 999 calls (risk effect). See table below for risk and control measures:

Risk Element	Risk Descriptor	Possible Control Measures
Risk Cause	'If the fixed electrical installation is not maintained……..	• Formal maintenance plan (planned preventative maintenance). • Rewiring if required. • Regular inspections (internal and external). • Priority response to any faults.
Risk Event	..this may result in a fire in the control room…..	• Fire suppression systems and alarms. • Firefighting equipment and training for staff. • Fire safety procedures i.e. PAT testing, close fire doors etc. • Staff awareness and reporting systems
Risk Effect	….which would lead to the inability to answer 999 calls'	• Business continuity plans i.e. alternative premises/systems • Testing of alternative premises/systems

If risks are not properly described they can create more questions than answers and, in the worst case scenario, can lead to the wrong control measures being identified. For example, if a risk is described simply as 'no qualified staff' the immediate question is 'why?' Is it down to recruitment, retention, training, or what? However, if described as 'an inability to recruit suitably qualified medical staff (cause) may lead to a shortage of clinical staff (event) and a failure to deliver critical services (effect)' all aspects of the risk are clearly identified, readily understood, and the identification of suitable control measures facilitated.

APPENDIX 11 – RISK TERMINOLOGY:



APPENDIX 12 – EXAMPLE APPETITE LEVELS DEFINED BY RISK CATEGORIES[4]:

	Averse	Minimal	Cautious	Open	Eager
Strategy	Guiding principles or rules in place that limit risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 5+ year intervals	Guiding principles or rules in place that minimise risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 4-5 year intervals	Guiding principles or rules in place that allow considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 3-4 year intervals	Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2-3 year intervals	Guiding principles or rules in place that welcome considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 1-2 year intervals
Governance	Avoid actions with associated risk. No decisions are taken outside of processes and oversight / monitoring arrangements. Organisational controls minimise risk of fraud, with significant levels of resource focused on detection and prevention.	Willing to consider low risk actions which support delivery of priorities and objectives. Processes, and oversight / monitoring arrangements enable limited risk taking. Organisational controls maximise fraud prevention, detection and deterrence through robust controls and sanctions.	Willing to consider actions where benefits outweigh risks. Processes, and oversight / monitoring arrangements enable cautious risk taking. Controls enable fraud prevention, detection and deterrence by maintaining appropriate controls and sanctions.	Receptive to taking difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements enable considered risk taking. Levels of fraud controls are varied to reflect scale of risks with costs.	Ready to take difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements support informed risk taking. Levels of fraud controls are varied to reflect scale of risk with costs.
Operations	Defensive approach to operational delivery - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority.	Innovations largely avoided unless essential. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with clear demonstration of benefit / improvement in management control. Responsibility for non / critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.
Legal	Play safe and avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge.	Want to be reasonably sure we would win any challenge.	Challenge will be problematic; we are likely to win, and the gain will outweigh the adverse impact.	Chances of losing are high but exceptional benefits could be realised.
Property	Obligation to comply with strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Recommendation to follow strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Requirement to adopt arrange of agreed solutions for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Consider benefits of agreed solutions for purchase, rental, disposal, construction, and refurbishment that meeting organisational requirements.	Application of dynamic solutions for purchase, rental, disposal, construction, and refurbishment that ensures meeting organisational requirements.
Financial	Avoidance of any financial impact or loss, is a key objective.	Only prepared to accept the possibility of very limited financial impact if essential to delivery.	Seek safe delivery options with little residual financial loss only if it could yield upside opportunities.	Prepared to invest for benefit and to minimise the possibility of financial loss by managing the risks to tolerable levels.	Prepared to invest for best possible benefit and accept possibility of financial loss (controls must be in place).
Commercial	Zero appetite for untested commercial agreements. Priority for close management controls and oversight with limited devolved authority.	Appetite for risk taking limited to low scale procurement activity. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with demonstration of benefit / improvement in service delivery. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.

[4] Risk Appetite Guidance Note (publishing.service.gov.uk)

People	Priority to maintain close management control & oversight. Limited devolved authority. Limited flexibility in relation to working practices. Development investment in standard practices only	Decision making authority held by senior management. Development investment generally in standard practices.	Seek safe and standard people policy. Decision making authority generally held by senior management.	Prepared to invest in our people to create innovative mix of skills environment. Responsibility for noncritical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control.
Technology	General avoidance of systems / technology developments.	Only essential systems / technology developments to protect current operations.	Consideration given to adoption of established / mature systems and technology improvements. Agile principles are considered.	Systems / technology developments considered to enable improved delivery. Agile principles may be followed.	New technologies viewed as a key enabler of operational delivery. Agile principles are embraced.
Information	Lock down data & information. Access tightly controlled, high levels of monitoring.	Minimise level of risk due to potential damage from disclosure.	Accept need for operational effectiveness with risk mitigated through careful management limiting distribution.	Accept need for operational effectiveness in distribution and information sharing.	Level of controls minimised with data and information openly shared.
Security	No tolerance for security risks causing loss or damage to property, assets, information or people. Stringent measures in place, including: • Adherence to FCDO travel restrictions • Staff vetting maintained at highest appropriate level. • Controls limiting staff and visitor access to information, assets and estate. • Access to staff personal devices restricted in official sites	Risk of loss or damage to HMG property, assets, information or people minimised through stringent security measures, including: • Adherence to FCDO travel restrictions • All staff vetted levels defined by role requirements. • Controls limiting staff and visitor access to information, assets and estate. • Staff personal devices permitted, but may not be used for official tasks.	Limited security risks accepted to support business need, with appropriate checks and balances in place: • Adherence to FCDO travel restrictions •Vetting levels may flex within teams, as required •Controls managing staff and limiting visitor access to information, assets and estate. •Staff personal devices may be used for limited official tasks with appropriate permissions.	Considered security risk accepted to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes • Permission may be sought for travel within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices may be used for official tasks with appropriate permissions.	Organisational willing to accept security risk to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes • Travel permitted within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices permitted for official tasks
Project / Programme	Defensive approach to transformational activity - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority. Benefits led plans fully aligned with strategic priorities, functional standards.	Innovations avoided unless essential. Decision making authority held by senior management. Benefits led plans aligned with strategic priorities, functional standards.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Plans aligned with strategic priorities, functional standards.	Innovation supported, with demonstration of commensurate improvements in management control. Responsibility for noncritical decisions may be devolved. Plans aligned with functional standards and organisational governance.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control. Plans aligned with organisational governance.
Reputation	Zero appetite for any decisions with high chance of repercussion for organisations' reputation.	Appetite for risk taking limited to those events where there is no chance of any significant repercussion for the organisation.	Appetite for risk taking limited to those events where there is little chance of any significant repercussion for the organisation.	Appetite to take decisions with potential to expose organisation to additional scrutiny, but only where appropriate steps are taken to minimise exposure.	Appetite to take decisions which are likely to bring additional Governmental / organisational scrutiny only where potential benefits outweigh risks.