Northern Ireland Ambulance Service
Health and Social Care Trust

Title:	**Corporate Risk Management Strategy**		
Author(s):	Katrina Keating, Risk Manager		
Ownership:	Dr David McManus, Medical Director		
Date of SEMT Approval:	28.07.16	**Date of Trust Board Approval:**	06.10.16
Operational Date:	06.10.16	**Review Date:**	October 2018
Version No:	7.0	**Supercedes:**	Previous (V.6)
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 (pending), Complaints Policy, Board Assurance Framework, Information Governance Policies and Procedures, PPI Strategy, Serious Adverse Incidents (SAI) Procedure (pending), Incident Reporting Procedure (pending), Guidelines for Writing A Report/Statement (pending), Management of Medical Devices Policy, Claims Management Policy, Whistle Blowing Policy, Infection, Prevention & Control Policy & Procedures		

Version Control:			
Date:	**Version:**	**Author:**	**Comments:**
December 2006	1	Risk Manager	
September 2008	2	Risk Manager	
November 2009	3	Risk Manager	Ratified by Trust Board
October 2010	4	Risk Manager	Committee structures modified
August 2013	5	Risk Manager	Full review
November 2013	6	Risk Manager	Editorial amendments
October 2016	7	Risk Manager	Full review
October 2018	TBC	TBC	Scheduled review

1.0 INTRODUCTION:

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

1.1 Background:

The purpose of this Corporate Risk Management Strategy is to support the Northern Ireland Ambulance Service Health and Social Care Trust (NIAS) in managing its risks as effectively as possible by understanding and embedding the principles of effective risk management throughout the organisation. This ensures that NIAS meets both its moral and legal obligations, and ensures the safeguarding of patients, the public, its employees and assets as far as is reasonably practicable.

This strategy along with the Corporate Risk Management Policy, provides the framework that enables NIAS to manage its risk effectively, discharge its duties appropriately, and progress the successful delivery of both corporate and directorate aims and objectives.

This Strategy forms part of the Trust's internal control and corporate governance arrangements, is integrally linked to the Board Assurance Framework and is aligned with the Annual Business Plan and Trust Delivery Plan 2015-2016. It reflects a range of risk management standards, current guidance and best practice (AS/NZS Risk Management Standard, DHSSPS guidance, ISO 31000 Risk Management Principles and Guidelines, Risk Management Standard for Ambulance Services – NHSLA 2013-14, Institute of Risk Management ERM guidance etc.).

1.2 Aims & Objectives:

The aim of this strategy is to establish a framework for the effective and systematic management of risk; the objectives are to:

- 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 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 NIAS applies a best practice approach to risk management, which is aligned to relevant NHS risk management requirements, and which demonstrates a commitment to continual improvement.
- Support the further development of an open, honest and just (fair) culture.

1.3 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. There are no exceptions.

1.4 Risk Management Priorities & Resources:

Over the next twenty four months NIAS will enhance the risk maturity of the organisation through the implementation of this Strategy; it will review the Board Assurance Framework, implement an improved incident reporting and investigation process, refresh the risk workshop process, and identify opportunities for developing individual risk management capability.

The Trust aims to enhance its ability to record and manage risks including those that are identified externally, for example through the regional Serious Adverse Incident Procedure (SAI), RQIA and changes in legislation.

With regards to the administration and internal control of the risk management process, risks are currently recorded on an electronic Risk Management System known as DATIX by the Risk Manager. The Trust will make arrangements for risk owners to access DATIX directly; this would facilitate the removal of associated paper systems.

The Risk Manager will be responsible for both supporting and challenging risk owners on how effectively they are managing their risks, with progress being reported back to the Medical Director, as the accountable Director for Risk Management, for inclusion at Senior Executive Management Team (SEMT) meetings.

In addition to the regular presentation of risk registers, there will be an annual presentation to Trust Board on how effectively NIAS is managing its risks, and on how continual improvement will be sustained.

The Trust will continue to be substantively compliant with applicable Controls Assurance Standards such as the Risk Management and Governance Controls Assurance Standards.

Resources, including cost, will inevitably impact on what risks are managed to what extent, and how. This framework ensures that principal risks are communicated to SEMT for monitoring, further action, approval, advice and prioritisation as appropriate.

2.0 DEFINITIONS:

2.1 Risk Management:

The International Risk Management Standard ISO 31000:2009 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’.

NIAS risk management covers a wide spectrum including clinical care, finances, assets, health and safety, business continuity, public image (reputation), legal compliance, procurement, contractual agreements, etc. See Appendix 6 for the DHSSPS Regional Matrix which depicts the suggested domains for risk management.

Effective risk management is a continual process that must be embedded in our ways of working at both strategic and operational levels, including business planning, project management, partnerships, SLA’s, target and objective setting, and service plans.

Existing NIAS good practice, such as effective clinical care, good health & safety management, and efficient procurement practices are all examples of effective risk management. These must be sustained, with relevant lessons shared, and regularly reviewed with a view to continual improvement

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.

2.2 Risk Registers:

Risk Registers are logs of identified and evaluated risks, maintained at a corporate and directorate (and where necessary operational) 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.

2.3 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 6 for full HSC Regional Tables).

2.4 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.

2.5 Risk Appetite:

Risk appetite is the amount of risk the organisation is willing to accept. This is difficult to define as the risk appetite will vary depending on each individual risk. No system can be risk free and this strategy is focused on the effective management of risk so as to support efficient service delivery.

Trust Board provides due governance of the level of risk appetite adopted by NIAS and the DHSSPS has developed HCS Regional Matrix (Appendix 6) in order to direct HSC Trusts in the management of risk. The principles applied by NIAS in deciding its risk appetite are listed in Section 7.

3.0 BENEFITS OF SUCCESSFUL RISK MANAGEMENT:

Effective risk management in NIAS will ensure the following:

- Compliance with relevant legal and regulatory requirements.
- Resources are used effectively and efficiently (staff, financial resources etc.).
- Risk to reputation is minimised (including a reduced risk of misinterpretation by the media).
- There is clear evidence of robust decision making and action planning relating to risk management.
- A high quality service is delivered (including a reduction in service disruptions).
- Service performance is improved and relevant KPIs are met.
- The Annual Business Plan and Trust Delivery Plan 2015-2016 is supported, with objective met on time and to the required standards.
- Opportunities are exploited and innovation is supported.
- Change is effectively managed.
- There are fewer 'surprises'.

4.0 APPROVAL, CONSULTATION, IMPLEMENTATION & REVIEW:

NIAS employs both a 'top down' and 'bottom up' approach to the implementation of this Corporate Risk Management Strategy. This Corporate Risk Management Strategy (and the Corporate Risk Management Policy) has been:

- Drafted in consultation with the Chief Executive, Directors and Assistant Directors.
- Ratified by SEMT for presentation to Assurance Committee.
- Considered by the Trust's Assurance Committee.
- Approved by Trust Board on recommendation by the Assurance Committee.

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

- Issued to all Board Members, Chairman, 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.

In addition:

- Risks are discussed at Directorate/management/team meetings.
- Regular review meetings and annual risk management workshops are arranged for those required to attend.

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

5.0 ROLES AND RESPONSIBILITIES:

This strategy incorporates a Responsibility, Accountability and Support (RAS) matrix at Appendix 4 to define the key roles and responsibilities for corporate risk management across NIAS, based on the following descriptors:

R	Responsible	This identifies who has overall responsibility for each key risk management function, and should generally be allocated to one individual, though it can be allocated to a team i.e. a Senior Management Team
A	Accountable	This identifies those who are accountable to the responsible person for the effective delivery of each risk management function, and can comprise several people and/or teams
S	Support	This identifies those who can provide technical/expert support to the responsible and/or accountable persons as appropriate, including policies, procedures, etc.

The corporate level RAS matrix at Appendix 4 can be supported by the development and implementation of directorate/service level RAS matrices as required.

5.1 All Employees:

In addition to such RAS matrices it must be emphasised that 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 patients, 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.
- 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.

5.2 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 Medical Director or an alternative Director in his absence. 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 also holds the position of DATIX Administrator and is therefore responsible for the upkeep of the Risk Management System. The Risk Manager 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 complaints and claims sections, with a regular meeting structures in place.

5.3 Service Users / Members of the Public:

It must also be noted that we expect our 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.

6.0 GOVERNANCE:

Due governance of NIAS risk management is provided through several assurance functions, including:

6.1 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.
- Reviewing and approving the Corporate Risk Management Policy and Strategy (including the risk appetite statement).
- 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 not less than 3 times a year.
- Supporting the CEO and SEMT 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.

6.2 Assurance Committee:

Chaired by a Non-Executive Director, and meeting not less than 3 times a year, this committee is responsible for providing assurance to the Board that NIAS risk management is fit for purpose and supporting the organisation in meeting its objectives, including:

- Approving any revisions to the Risk Management Policy and Strategy.
- Monitoring Sub-Committees, i.e. ensuring terms of reference are up to date, risk issues are appropriately reviewed and escalated, action plans are prepared and submitted,

minutes are prepared and circulated and any reports are available (see Committee Structure at Appendix 2).
- Reviewing and constructively challenging risk registers from one directorate per meeting (including any program and project risks registers within that directorate).
- 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.
- Receiving and reviewing reports of all of the Trust's incidents; monitoring trends, reviewing all Trust Serious Adverse Incidents (SAIs). Ensuring systems are in place for organisational learning.
- Receiving and reviewing reports from Internal Audit regarding Controls Assurance Standards (CAS).
- Receiving and reviewing other standing items including Coroner's reports and letters, medical device alerts, PHA Safety & Quality Information (including national and regional guidance), Pharmacy and Medicines Management Updates (see any Assurance Committee agenda for further information).
- Monitoring of the Board Assurance Framework.
- Communicating matters to Trust Board as necessary.

6.3 Audit Committee:

Whilst the Audit Committee's primary responsibility is to provide independent assurance to the Trust Board on the effectiveness of internal financial controls the Committee has some specific responsibilities in the area of risk management and corporate governance which include the following:

- The Committee shall contribute to the establishment, review and maintenance of an effective system of integrated governance, risk management and internal control, across the whole of the organisation's activities (both clinical and non-clinical) that supports the achievement of the organisation's objectives.

- The Committee shall review the findings of other significant assurance functions, both internal and external to the organisation, and consider the implications for the governance of the organisation.

A full description of the responsibilities of the Audit Committee is included in the Terms of Reference.

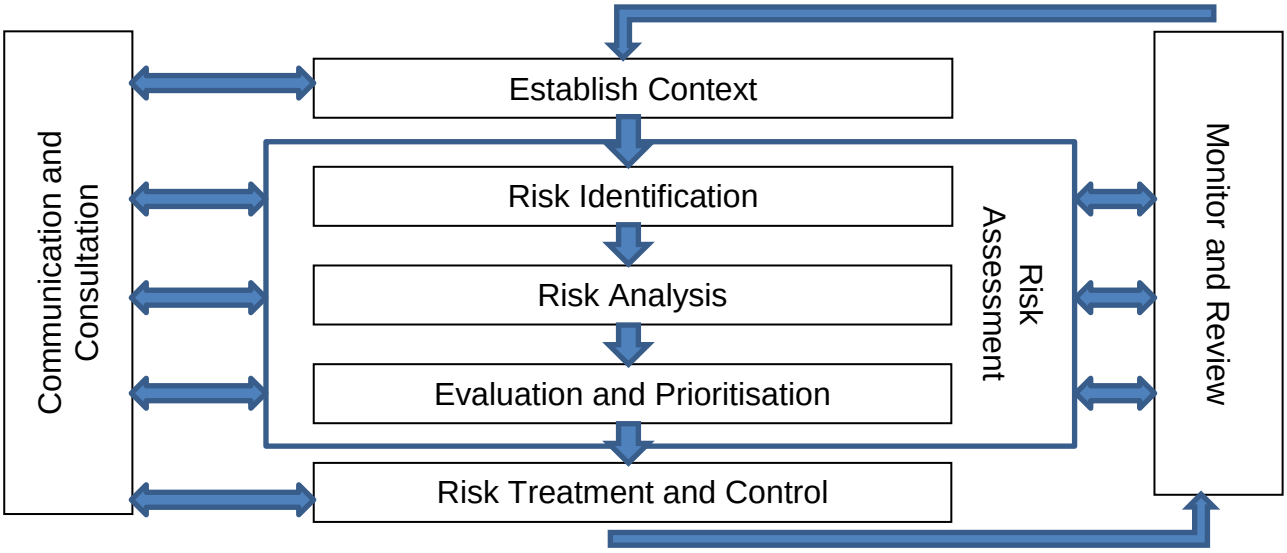
6.4 Internal Audit:

Responsibility for formally reviewing the risk management process with the aim of providing objective commentary on its effectiveness and identifying opportunities for improvement. Undertakes Controls Assurance Standards (CAS) audits, review, self assessments etc.

7.0 RISK MANAGEMENT PROCESS:

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

Risk Rating = Impact / Likelihood



In conjunction with the definitions of risk management, risk registers, risk, hazards, likelihood, impact and control measures detailed in Section 2, the following expands on the key elements of the risk management process:

7.1 Establish Context & Identify Risks:

It is essential that the context of the risk identification process is established so as to enable an objective approach to what constitutes significant risk i.e. what will significantly impact on NIAS objectives and/or service delivery?

A methodical approach to risk identification must then be applied, with those responsible for identifying risks taking into account:

- The need to prioritise the identification of risks that might affect the achievement of NIAS objectives. Strategic risks linked to the corporate objectives and operational risks linked to service provision need, as a minimum to be identified and monitored.
- Relevant business plans, project plans, KPIs, best practice, audit reports, clinical audit documentation, self assessments, RQIA, 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 table of Risk Categories in Appendix 7 can be used to identify risks.

7.1.1 *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 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 8 for a risk description example.

7.2 Risk Analysis, Evaluation & Prioritisation:

The HSC Regional Risk Matrix at Appendix 6 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 Section 6.5.1).

7.2.1 Existing Controls:

The risk analysis, evaluation and prioritisation process must 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, must 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.

7.3 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

7.3.1 *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 6, 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.

7.4 Completing the Risk Register (DATIX):

Risks can be inputted directly to DATIX during a workshop led by the Risk Manager. Also see Appendix 5 for a risk assessment template (with action plan) which can be used for most risks. Each risk will be assigned a unique reference number (via DATIX).

7.5 Risk Appetite Statement:

The aim of this strategy, as stated in Section 1.2, is 'to establish a framework for the effective and systematic management of risk'. This requires NIAS to identify the level of risk it is prepared to accept (i.e. the risk appetite as defined in Section 2.5), whilst also ensuring relevant risks are escalated for additional action, as defined in Section 7.6.1.

There is a clear recognition that we must accept a level of risk in order to meet the high standard we set ourselves, and that is expected by the society we serve in the provision of a service in a potentially uncontrolled, unstable or even hostile environment. We accept the potential costs of such risks in the realisation that the benefits to patients can outweigh the risks; for example in emergency driving, Rapid Response Paramedics working alone and in the work of Hazardous Area Response Teams (HART). We acknowledge our staff regularly accept and manage significant risk in order to help others; for them not to do this would render us a much less effective organisation.

Each significant risk must be assessed individually when deciding whether it is within our risk appetite (tolerable), or whether additional controls (terminate, treat or transfer) are required. The following risk appetite principles should be applied.

The Northern Ireland Ambulance Service Health and Social Care Trust's:

a. Appetite for risks relating to patient safety and employee health and safety is very low, with controls required to reduce the risks so far as is reasonably practicable.
b. Appetite for risks relating to regulatory compliance, fraud, and information governance is also low, requiring appropriate risk controls.
c. Appetite for risks to non-critical functions and services is higher, whilst taking into account any potential impact on any strategic/business objectives.
d. Approach to risk management is designed to encourage and promote innovation and continual progress, and not to stifle or hinder growth and development, and NIAS appetite for risks to its strategic and/or directorate objectives should reflect this.

These principles have been agreed by Trust Board.

7.6 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 Significant Adverse Incidents (SAIs).
c. Rotation of directorate risk registers through the Assurance Committee, not less than three times per year.
d. Reviewing of relevant risks and risk registers at SEMT meetings i.e.
    - All extreme risks.
    - Selected high risks.
    - New or emerging risks.
    - Corporate Risk Register (principal risks).
e. Risk management summary reporting at all Trust Board meetings, including the Corporate Risk Register (principal risks).

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
- Informing the Risk Manager.

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.

7.6.1 *Escalation Process:*

The risk analysis and evaluation will enable risks to be categorised in accordance with Appendix 6. 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 SEMT and if necessary Trust Board Risk Manager informed ASAP.	Chief Executive or Director responsible	Senior Executive Management Team (SEMT). Report to Trust Board.	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 investigate, agree and oversee implementation of action plan. Risk Manager informed.	Director responsible or delegated Assistant Director	Director. Report to SEMT / Assurance Committee	Corporate or Directorate (depending on organisational impact and action plan)	**Action within one month.** **Review monthly**
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 to Assurance Committee as necessary	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	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 3a Recording and Escalating Risks and Appendix 3b De-escalation and Closure of Risks (Flow Charts).

7.7 <u>Corporate Risk Register (Principal Risks):</u>

The Corporate Risk Register details the principle (key) risks to the organisation, it will normally comprise one or more 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.

8.0 RISK MANAGEMENT IN PARTNERSHIPS / CONTRACTED SERVICES & PROJECTS / PROGRAMMES:

8.1 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.

8.2 Project / Programme Risk Management:

Directors must ensure arrangements for project/programme risk management are in place. All projects/programmes/service developments must incorporate and be supported by the appropriate risk management documentation. Where possible Appendix 6, HSC Matrix should be used.

9.0 RISK MANAGEMENT TRAINING:

All staff will attend training appropriate to their responsibility. Some training will be delivered as part of induction and some 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.
- 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. E-learning for risk management training will be introduced.

10.0 APPENDICES:

Appendix 1 – Risk Management Communication Structure.
Appendix 2 – Committee Structure.
Appendix 3a – Recording & Escalating Risks.
Appendix 3b – De-escalation & Closure of Risks.
Appendix 4 – Responsibility, Accountability & Support Matrices.
Appendix 5 – Risk Assessment Template.
Appendix 6 – DHSSPS Regional Risk Management Matrix.
Appendix 7 – Risk Categories.
Appendix 8 – Risk Descriptions.

11.0 EQUALITY STATEMENT:

11.1 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.

11.2 The outcome of the equality screening for this procedure undertaken on 13th September 2016 is:

Major impact ☐
Minor impact ☐
No impact. ✓☐

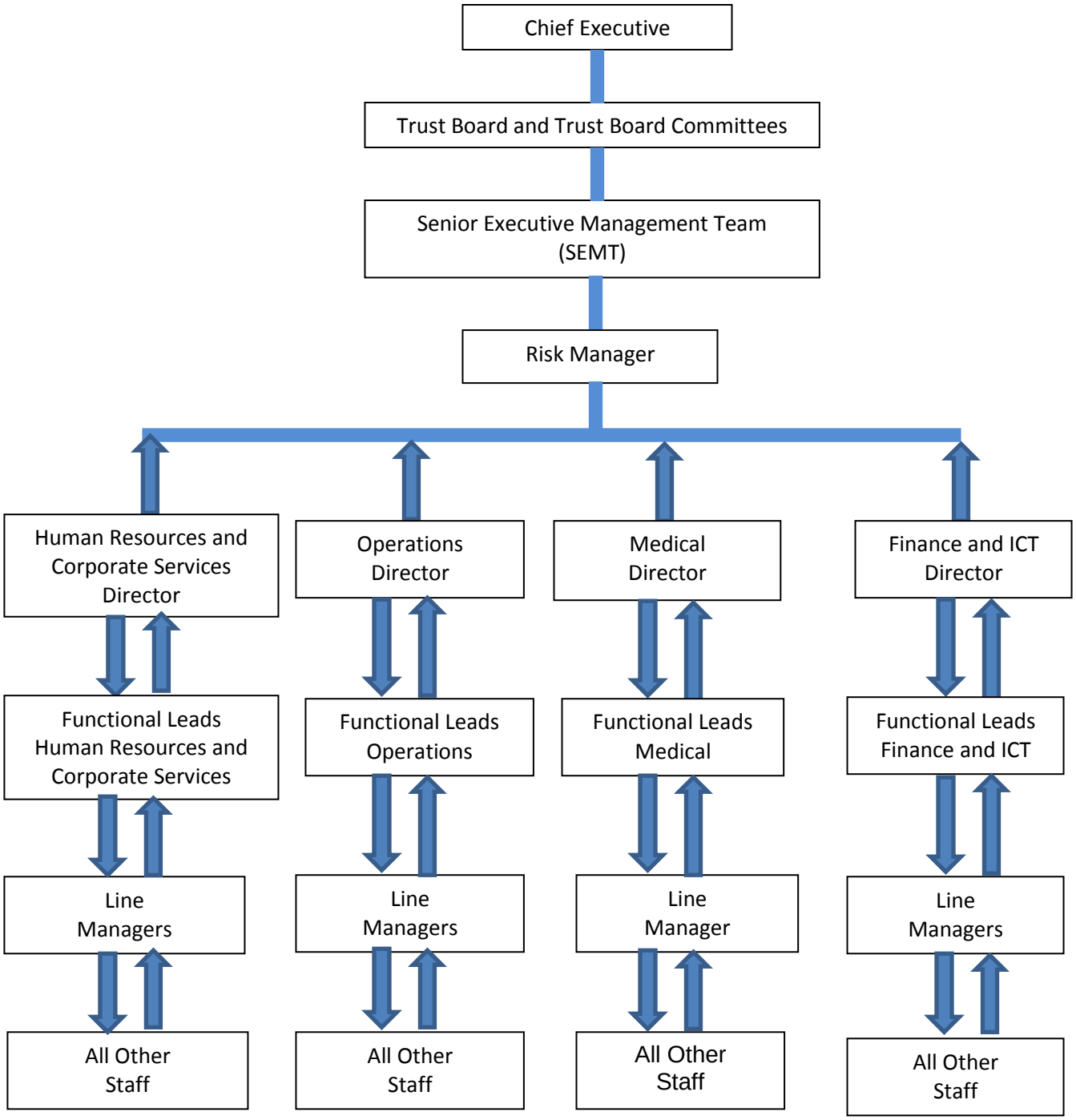
12.0 SIGNATORIES:

Katrina Keating **Date:** 6 October 2016
Lead Author

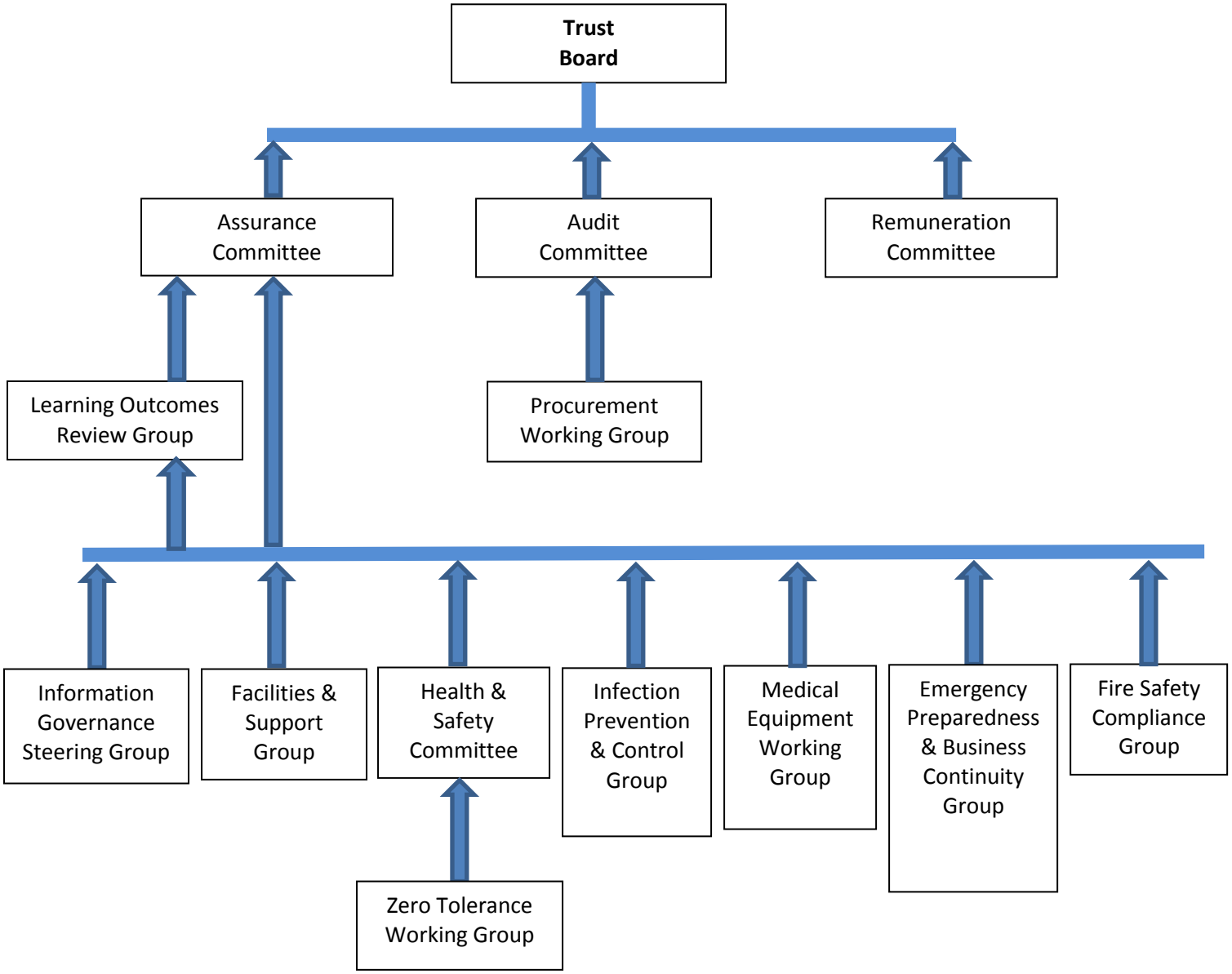
Dr David McManus **Date:** 6 October 2016
Lead Director

APPENDIX 1 – RISK MANAGEMENT COMMUNICATION STRUCTURE

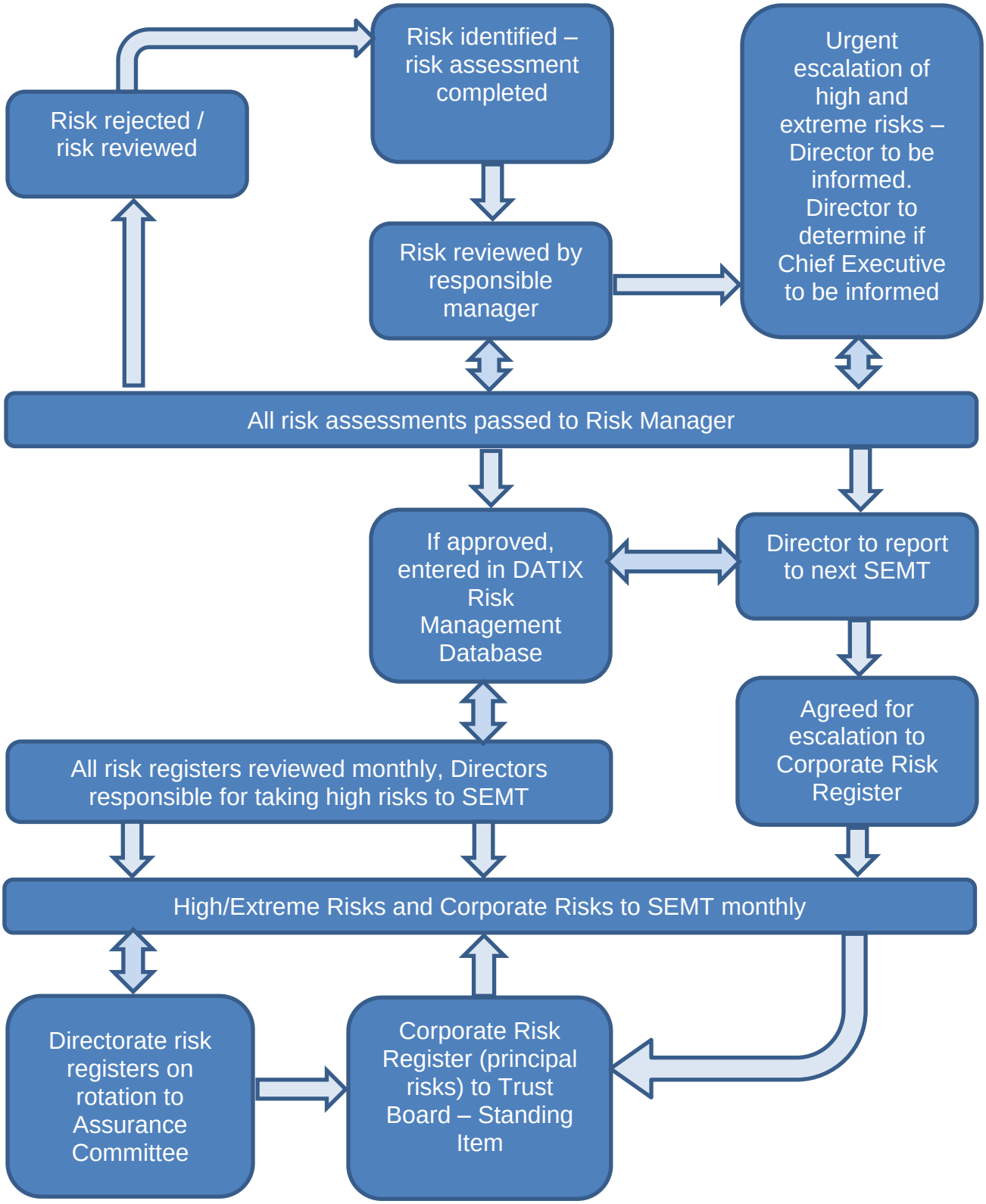
This structure identifies the lines of communications for identification, management and escalation of risks throughout NIAS.



APPENDIX 2 – COMMITTEE STRUCTURE (INCORPORATING WORKING GROUPS THAT SUPPORT THE COMMITTEES)



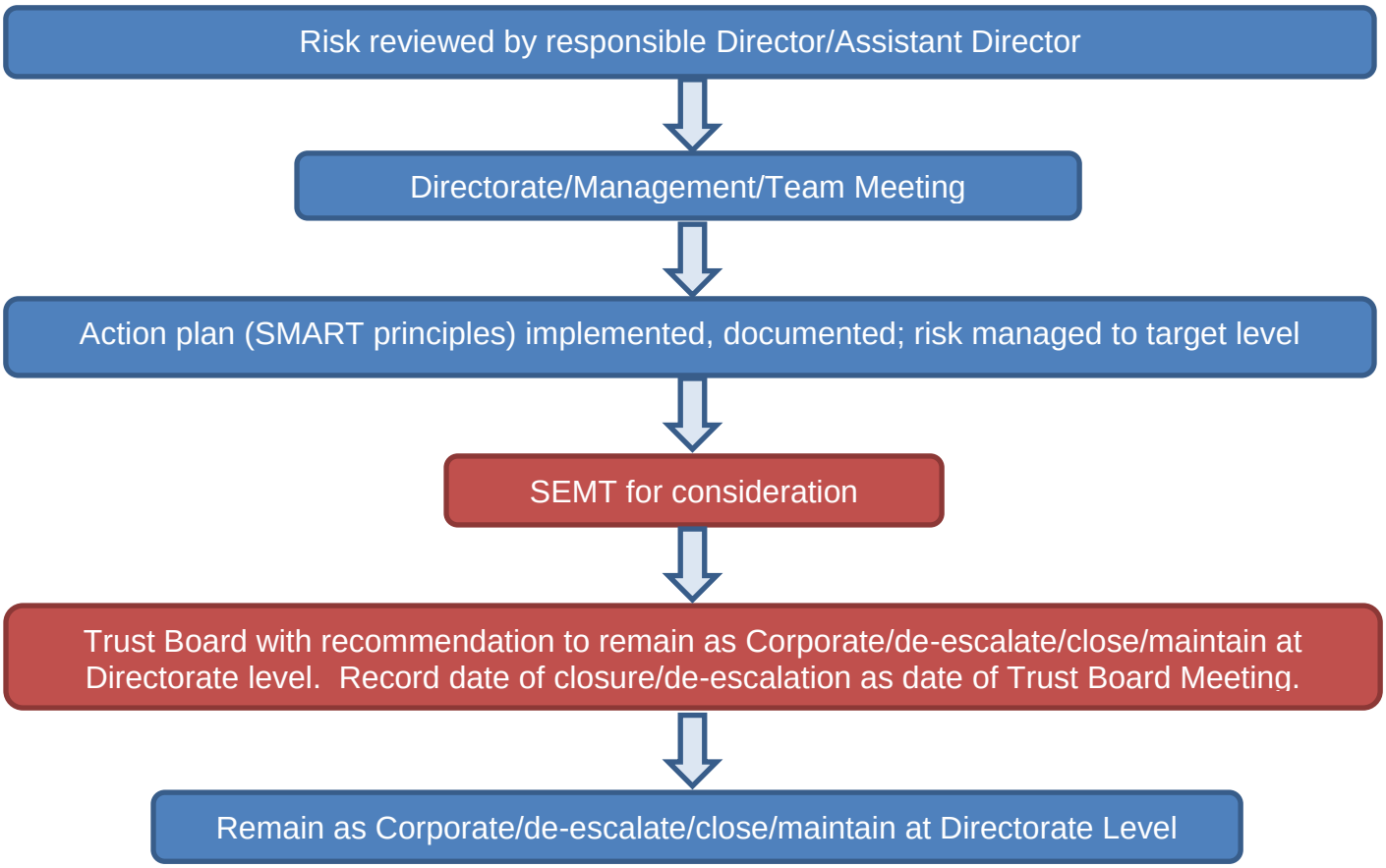
APPENDIX 3a – RECORDING & ESCALATING RISKS



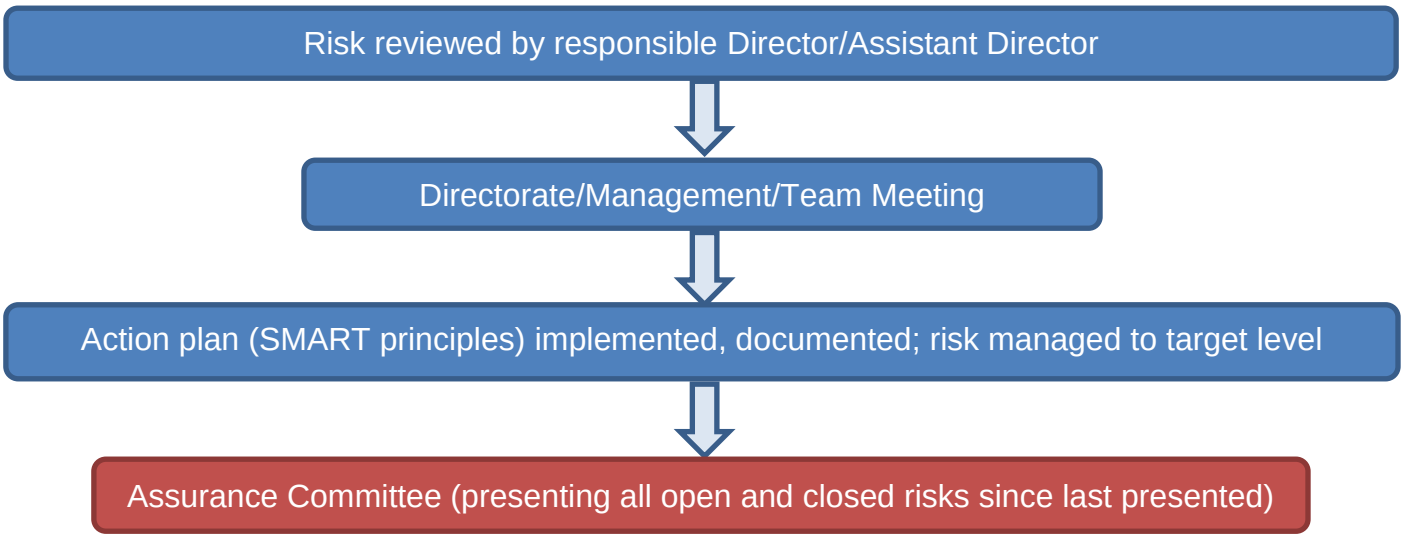
NOTE: Risk Owners are responsible for arranging annual workshops, providing updates to, and requesting latest registers held on DATIX from the Risk Manager

APPENDIX 3b – DE-ESCALATION & CLOSURE OF RISKS

CORPORATE / PRINCIPLE RISKS



DIRECTORATE RISKS



NOTE Risk Manager must be kept informed at all stages

APPENDIX 4 – RESPONSIBILITY, ACCOUNTABILITY & SUPPORT MATRIX:

	RISK MANAGEMENT FUNCTION	NIAS ROLE / POST							
		CEO	SEMT	MD	DHR & CS	DFIN	DOps	RM	Comments
1	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.	R	A	A	A	A	A	S	
2	Ensuring Trust Board is kept suitably informed of how effectively risk is being managed across NIAS.	R A		S				S	
3	Ensuring that all relevant risks i.e. those that pose a critical threat to NIAS operations and/or require external support to adequately manage are escalated to Trust Board for action.	R A		S				S	
4	Deputising for the CEO for 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.			R				S	CEO retains overall responsibility for risk management across NIAS
5	Ensuring the Corporate Risk Register (principal risks) is effectively monitored, and formally reviewed on a monthly basis, and that SMART based action plans are applied to risks requiring additional control measures.	R	A	A	A	A	A	S	
6	Identifying 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.		R	A	A	A	A	S	Other relevant key staff may attend SEMT to report/advise on specific risk areas
7	Lead on the effective implementation of the corporate risk management process across each relevant directorate, including: i. The effective management of directorate risks, taking into account corporate strategy, business planning and risks, by maintaining accurate directorate risk registers, and reporting on risk at SEMT each month. ii. The timely (immediate) escalation of relevant (critical) risks to the CEO/SEMT. iii. Effective communication on risk management to all relevant staff. iv. The provision and maintenance of appropriate training and resources within departments to support required competencies and effective risk management			R	R	R	R	S	Risks captured within the Corporate Risk Register will often have directorate level owners who are responsible for progressing agreed control actions

	RISK MANAGEMENT FUNCTION	NIAS ROLE / POST							
		CEO	SEMT	MD	DHR & CS	DFIN	DOps	RM	Comments
8	Ensuring all relevant actions/recommendation from incidents, including Serious Adverse Incidents (SAI's), audits, complaints, litigation, enforcement notices, etc. are monitored, implemented and reported on as required	R	A	A	A	A	A	S	
9	Ensuring all aspects of clinical governance and risk management are effectively managed, including: i. Dynamic risk assessment and decision making. ii. Management of the clinical aspects of EAC & NEAC. iii. Effective infection prevention and control. iv. Health and safety. v. Effective control and use of medicines, medical devices, etc. vi. Effective business continuity management, emergency planning and resilience. vii. Incident reporting, including SAIs process. viii. Safeguarding process. SIRO.	R		A				S	
10	Ensuring all aspects of Human Resources and Corporate Services Risks are effectively managed, including: i. The effective management of all staffing issues, including recruitment, competence, professional clinical registration checks, vetting, etc. ii. Relevant training and development of staff, including clinical supervision, training needs analysis, professional development, maintenance of competence etc. iii. Ensuring suitable procedures and resources are in place to support stress management across NIAS. iv. Ensuring relevant HR/Corporate policies and procedures are in place and working to meet legal requirements i.e. Equal Opportunities, Whistleblowing, etc. v. Direct management of the corporate whistleblowing process. vi. Transforming Your Care, Quality Improvement, Patient Experience	R			A			S	

	RISK MANAGEMENT FUNCTION	NIAS ROLE / POST							
		CEO	SEMT	MD	DHR & CS	DFIN	DOps	RM	Comments
11	Ensuring that internal aspects of NIAS financial, ICT and IG risks are effectively managed, including: i. Effective procurement. ii. Fraud prevention. iii. Effective insurance management. iv. Effective internal audit procedures. v. Suitable Information and Communication Technology. vi. Suitable arrangements for Information Governance.	R				A		S	
12	Ensuring that operational service risks are effectively managed, including: i. Fleet risks. ii. Estate risks, including security, fire risk, asbestos, legionella control, etc. iii. Operational staffing issues (cover, competency, etc.). iv. Meeting key operational performance objectives i.e. response times. v. Management of the operational aspects of EAC and NEAC, including staffing, emergency planning, etc.	R					A	S	
R	**Overall responsibility for the relevant risk management function.**								
A	**Accountability to the Responsible person for the effective delivery of the relevant risk management function.**								
S	**Supports the Responsible and Accountable persons in the effective delivery of the relevant risk management function as appropriate i.e. technical knowledge, procedures, etc.**								

Northern Ireland Ambulance Service Health and Social Care Trust

Appendix 5

RISK ASSESSMENT

Directorate:		**Division:**		**Station / Location:**	

Completed By:		**Designation(s):**	
Staff Consulted:		**Designation(s):**	

Task / Risk Description:	

No.	Description of Hazard(s)	Persons Affected / Consequences	Existing Controls	Impact	Likelihood	Risk Rating	Further Controls?	
							Yes	No
1		E.g. staff, patients, public, visitors, contractors etc.						
2								
3								

If further controls are required you must complete an action plan (see over/attached)

Northern Ireland Ambulance Service
Health and Social Care Trust

RISK ASSESSMENT

ACTION PLAN

No.	Further Action To Control Risk	Person Responsible	Target Date	Date Completed	Revised Risk Rating		
					Impact	Likelihood	Rating
1		Note name & Designation					
2							
3							
4							
5							

For further details on the process including the regional matrix, consultation, review etc., please see the NIAS Risk Management Strategy.

ASAM / AD (Print Name):							**Division:**	
Signature:							**Date:**	
Agreed H&S Committee (Tick ✓):	**Yes**		**No**		**N/A**		**Date:**	
Agreed Directorate Meeting (✓)	**Yes**		**No**		**N/A**		**Date:**	

HSC Regional Impact Table – with effect from April 2013 (updated June 2016)					
APPENDIX 6	**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 June 2016)

Appendix 6

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 7 – 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.

Political	Delivery of objectives, strategy etc. Government policy, local political pressures, Ministerial direction, Commissioners, Boards, e.g. too slow, unfulfilled promises, political personalities, 'wrong' strategic priorities, corruption, limits of authority.
Economic / Financial	Ability of the organisation to meet its financial commitments, budgets, insurance, investments, pensions etc., also external economic changes, e.g. inflation. Consider financial planning, resources and controls, e.g. overspends, failure of projects, missed grants, inadequate control, fraud, tax, unrecorded liabilities, unreliable accounting records. Accountability/openness/trust.
Competitive	Competitiveness of the service (in terms of cost or quality) and/or its ability to deliver best value, quality improvement, position in performance tables, failure of bids for government funds, benchmarking, CAS, accreditations, media, RQIA, HCPC, JRCALC
Legal	Breaches of legislation, misinterpretation of legislation, legal challenges, failure to comply with procurement directives, breach of confidentiality, data protection, claims, FOIs, whistleblowing etc. Current or potential changes in European/national law, human rights etc.
Managerial / Professional / HR	Particular nature of each profession, e.g. competence. Managerial abilities, poor communication and management of change, staffing issues, recruitment, retention, sickness management, change management, stress management, over reliance on key officers, failure to retain/recruit key staff, lack of motivation, failure to comply with employment law, poor recruitment/selection, lack of training, lack of succession planning internal investigations/trends, tribunals, TU concerns/trends
Technological	Ability to identify and keep pace with technological changes/infrastructure requirements, use technology to meet changing demands, consequences of internal technological failure, e.g. hacking, corruption of data, breach of confidentiality etc. Reliance on operational equipment (IT, equipment, machinery). E.g. failure of IT project, systems crash, security breach, failure to comply with IT Security policy, poor management of website(s).
Social	Effects of changes in demographic, residential or social economic/trends. Failure to meet needs of disadvantaged communities, crime and disorder, lack of regeneration.
Partnership / Contractual /	Delivery of services or products to the agreed cost and specification, e.g. non-compliance, over reliance, failure to deliver, failure to monitor, poor selection, quality issues.
Physical	Clinical/patient safety incidents, SAIs, alerts, infection control, child protection, vulnerable adults, health and safety/accidents, violence and aggression, injury, fire, security, loss of assets, criminal damage, misuse of equipment, failure to upkeep land and property. Lack of service, business impact analysis, business continuity planning,
Customer / Citizen	Meeting current and changing needs and expectations of customers, e.g. lack of consultation, media, public relations/perception, high level of complaints, reputational risks and stakeholder satisfaction.
Environmental	Pollution, contaminated land, noise, energy and water efficiency, recycling, landfill requirements, emissions, waste storage, damage caused by trees/roots, weed etc. Environmental consequences of progressing the organisation's strategic objectives, e.g. transport policies.
Projects	Project management, e.g. new builds, new ventures, new initiatives
Opportunity	Partnerships, revenue generation, are we missing any opportunities?

APPENDIX 8 – 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.