The Patient and Client Council

Risk Management Strategy and Policy

Any request for the document in another format or language will be considered

5th Floor,
14/16 Great Victoria Street
BELFAST
BT2 7BA
Tel: 0800 917 0222

https://pcc-ni.net/

Developed by:	Carol Collins, Interim Head of Business Support
Date approved by EMT:	
Equality screened by/date:	
Date approved by ARAC:	
Date approved by Council:	
Date to be reviewed:	2025

CONTENTS:

Appendices:

1. Introduction

Managing risk is an essential part of good governance, and is fundamental to how an organisation operates and is managed at all levels.

The Patient and Client Council (PCC) is committed to ensuring that it has, and maintains, a robust and effective system of risk management.

This Risk Management Strategy and Policy sets out the PCC's approach to risk management. It sets out how risk is managed across the organisation, and ensures a consistent approach to identify and deal with risks that may impact on the PCC's ability to achieve its strategic aims and objectives.

2. Risk Management in the Health and Social Care System

Following a regional review of risk management processes across Health and Social Care (HSC), a new Regional Model for Risk Management (including a Regional Risk Matrix) was endorsed by the HSC Chief Executives Forum in September 2018.

The model, which was developed by a Working Group, comprising senior managers working in risk management across the HSC, is based on the principles of the ISO 31000:2018 standard[1]. All HSC organisations, including the PCC, agreed to adopt the 'spirit' of ISO 31000:2018, but not to seek accreditation.

At the same time the Regional Working Group reviewed and updated the HSC Regional Impact Table and the HSC Regional Risk Matrix.

The Regional Working Group agreed that it was beneficial to maintain a common risk management standard across HSC organisations, The PCC Risk Management Strategy and Policy shows how the organisation's risk management system meets this standard.

3. Managing Risk According to the Principles of ISO 31000:2018

ISO 31000: 2018 has three components for managing risk:

(i) the core **principles of risk management**
(ii) The development of a **risk management framework,** and
(iii) The **risk management processes** These are described below.

3.1 Definition of Risk

There are many definitions that are used in the area of risk management, however the HSC organisations have adopted the following definition, based on the ISO 31000:2018 definition of risk:

[1] BSI ISO 31000: 2018: Risk Management Guidelines

DRAFT

Risk is the "effect of uncertainty on objectives"

Risk is also often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. This links with the HSC Regional Risk Matrix.

3.2 Core Principles of Risk Management

The following principles are the foundations of good risk management:

Integrated – risk management should be integrated within all organisational activities.

Structured and comprehensive – to contribute to assurances in the Governance Statement

Customised – the risk management framework and process should be customised and proportionate to the organisation's external and internal context related to its objectives.

Inclusive – the organisation's risk management system should be informed by appropriate and timely involvement of stakeholders.

Dynamic – risks can emerge, change or disappear as an organisation's external and internal context changes. The organisation's risk management system therefore needs to respond to these changes in a timely manner.

Best available information – information should be timely, clear and available to relevant stakeholders.

Human and cultural factors significantly influence all aspects of risk management.

Continual improvement – risk management is continually improved through learning and experience and will feed into the organisation's quality improvement framework/systems.

3.3 Risk Management Framework

The 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."[2]

The five key elements of a risk management framework as set out in ISO 31000:2018 are:

DRAFT

[2] HM Government 'The Orange Book: Management of Risk – Principles and Concepts' 2020 (Orange Book - GOV.UK (www.gov.uk))

Leadership and Commitment

Management needs to ensure that risk management is integrated into all organisational activities and demonstrate leadership and commitment by implementing all components of the framework. This in turn will help align risk management with its objectives, strategy and culture.

Integration

Integrating risk management relies on an understanding of organisational structures and context. Risk is managed in every part of the organisation's structure and everyone in an organisation has responsibility for managing risk.

Design

The organisation should examine and understand its external and internal context when designing its risk management framework.

Implementation

Successful implementation of the framework requires the awareness of all staff within the organisation.

Evaluation

The organisation should periodically measure its risk management framework against its purpose, implementation plans, risk management key performance indicators and expected behaviour, to ensure it remains fit for purpose.

Improvement

The organisation should continually review, monitor and update its risk management framework to ensure it is fit for purpose.

3.4 Risk Management Processes

The third component for managing risk under ISO 31000:2018 is the risk management process, which is comprised of the following:

(i) Communication and consultation
(ii) Scope, context and criteria
(iii) Risk assessment
- Risk identification
- Risk analysis
- Risk evaluation

(iv) Risk treatment
(v) Monitoring and review
(vi) Recording and reporting

The PCC Risk Management Process is set out in the following paragraphs.

DRAFT

4. Risk Management in the PCC

Risk Management is “the coordinated activities designed and operated to manage risk and exercise internal control within an organisation”[3]

It enhances strategic planning and prioritization, assists in achieving objectives and strengthens the organisation’s ability to be agile in responding to challenges. While risk must be managed, public sector organisations cannot be risk averse and successful; risk is inherent in everything we do to deliver high-quality services.

“Risk management is not the same as minimising risk. It is important to remember that being excessively cautious can be as damaging as taking unnecessary risks. Risk taking is the basis of progress. Without it, you cannot have innovation and the benefits that come from developing new procedures and interventions or changing business practices. Boards have to carefully consider whether or not potential long-term rewards will be greater than shortterm losses.” (HSC Board Members Handbook - 2020)

Risk management is an essential part of good management and good governance within the PCC, and is central to good decision making, accountability and therefore in aiding the organisation to achieve its business objectives in line with our corporate and annual business plans.

It is embedded in the culture of the organisation, from the Chief Executive Officer through all staff across the PCC, aided by good communication. Risk is recorded, monitored and reported through Corporate and Department Risk Registers, enabling escalation and de-escalation and facilitating an inclusive ‘top-up’ and ‘bottom-down’ process. It complements and informs the corporate and business planning and performance reporting processes, and promotes an ethos of continuous improvement.

Risk management is a key element of the PCC’s Assurance Framework and the system of internal control. It facilitates better use of resources, encourages the organisation to be better aware of potential challenges and opportunities in both the internal and external environment, and therefore helps reduce unwelcome surprises.
As such it has an important function in both providing assurance to the Council and in supporting the Council in their overarching leadership and oversight of the organisation.

4.1. Risk Management Process within the PCC

The PCC Risk Management Process incorporates

- Commitment from Council and Senior Management
- Integration with how the PCC does its business and makes decisions
- Good communication

DRAFT

[3] HM Government ‘The Orange Book: Management of Risk – Principles and Concepts’ 2020

- Understanding that certain risks have to be accepted and managed accordingly
- Consistency in approach to risk management across the organisation Clear reporting and monitoring

Risk Management is part of an integrated governance system within the PCC, including:

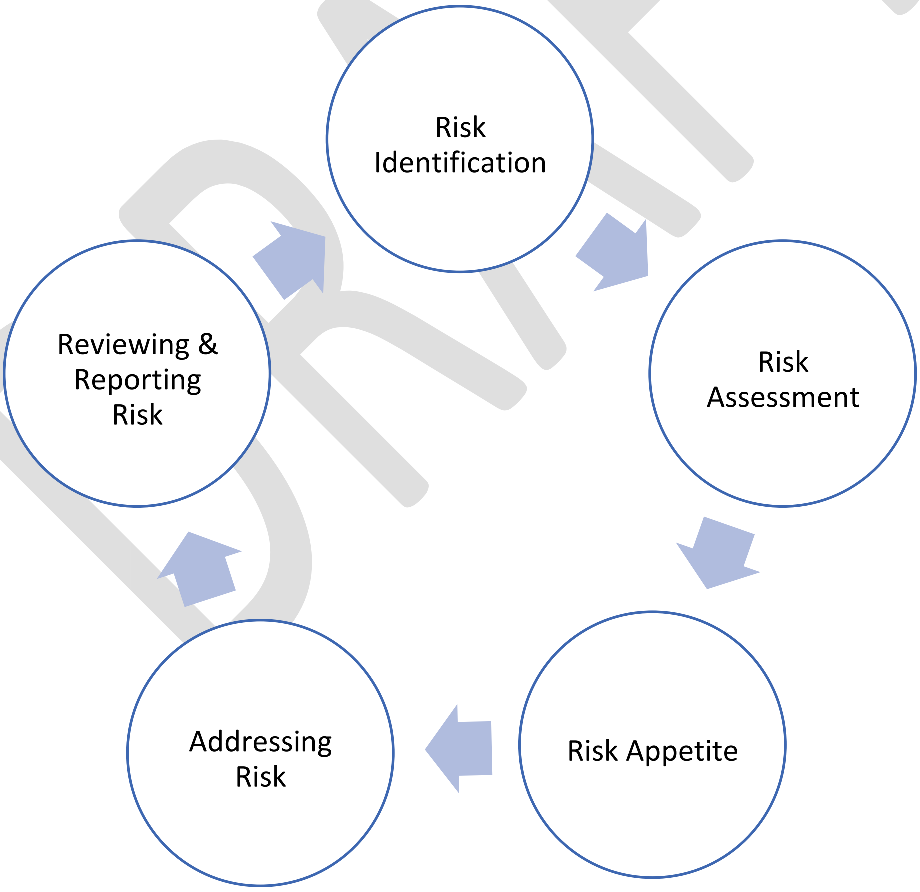
- Risk Management Strategy and Policy
- Corporate Risk Register
- Department Risk Registers
- Governance Statement and Mid-Year Assurance Statement
- Assurance Framework
- Internal Audit programme (which is informed by the Corporate Risk Register)
- Reporting to the Audit and Risk Assurance Committee (ARAC) and

Council

- Information Risk Management Policies
- Business Continuity Policy and Plan

The PCC Risk Management process comprises 5 steps, as set out in Figure 1 below:

Figure 1: The Risk Management Process[4]



Step 1 Risk Identification

The process of identifying risks which may impact on the organisation's ability to achieve its objectives, is a formal, structured process that considers sources of risk, areas of impact, potential events and their causes and consequences. The process is conducted at all levels of the organisation – Corporate and Department.

Risks are identified during the regular formal review of Department and Corporate Risk Registers, but critically risk identification should also be an integral part of all activities, including strategy or policy development and implementation and business plan development and monitoring.

The HSC Regional Impact Table identifies six categories or domains of risk:

[4] Risk Management Steps figure based on 'Good Practice in Risk Management', NI Audit Office, June 2011

DRAFT

- People
- Quality and Professional Standards/Guidelines
- Reputation
- Finance, Information and Assets
- Resources
- Environmental

Risk can be influenced by both internal and external factors and can relate to existing policies, programmes or processes as well as to new introductions and initiatives.

All risks should be linked to a corporate objective, and should have an identifiable risk owner, at an appropriate level of seniority, who is responsible for ensuring that the risk is managed and monitored over time.

Step 2 Risk Assessment

Once the risk has been identified the level of the risk should then be assessed, to identify the '*inherent risk'*, that is the exposure arising from a specific risk before any action is taken to address it. This is done by assessing the likelihood of the risk occurring and the potential impact (consequences) on the business should it occur.

Risk is assessed using the Regional HSC Risk Matrix and the associated HSC Regional Impact Table (see appendix 4). Each risk will be categorized as either low, medium, high or extreme.

The impact and likelihood of risks occurring will be reassessed later in the risk management process (step 4) to reflect the level of risk as a result of the risk response. This is referred to as '*residual risk'*, that is, the exposure arising from a specific risk after action has been taken to address it, and making the assumption that the action is effective.

Step 3 Risk Appetite

This step of the risk management process evaluates and determines whether the exposure to risk is acceptable or unacceptable, that is, the PCC '*Risk Appetite'*.

Risk appetite can be defined as the "*amount and type of risk that an organisation is prepared to seek, accept or tolerate*". ISO defines risk appetite as an "*organisation's approach to assess and eventually pursue, retain, take or turn away from risk*."

It is recognized that risk cannot be eliminated, and it is necessary to accept a level of risk in order to conduct business, and achieve the purpose for which the PCC was established.

The PCC is a publically funded HSC body, operating in an environment where safety, quality, viability and good stewardship of public funds are essential,

DRAFT

Therefore, the PCC will generally accept manageable risks, which allow the organisation to take opportunities and be innovative and creative in fulfilling its functions/providing a service to the public, thus demonstrating benefit. The PCC will not however accept those risks where the risk of harm or adverse outcomes to service users, staff, the PCC's business viability or reputation is significantly high and would outweigh any benefits to be gained.

An acceptable (or residual risk) is one where there are adequate control measures in place, where all reasonably practical measures have been taken to manage the risk in line with the PCC risk appetite.

It is recognised however, that it is not always possible to reduce an identified risk completely and it may be necessary to make judgments about achieving the correct balance between benefit and risk. A balance needs to be struck between the costs of managing a risk and the benefits to be gained.

Where a risk has been reduced to the point where the cost of further controls to reduce it outweigh the benefit that they may provide, it may not be considered reasonably practicable to implement those controls. However, where risk controls are available, it is the duty of the organisation to demonstrate that the cost of implementation outweighs the benefit, or that alternative effective control measures have been implemented. Risks requiring a cost benefit analysis must be considered as part of the PCC risk management process, allowing proper debate and decision on 'acceptability'

Step 4 Addressing Risk

There are four traditional responses to addressing risk:

Terminate	Decision is made to not take the risk or to cease the activity which causes the risk, where the risk outweighs the possible benefit. This is not always possible in the provision of public services.
Tolerate	Decision is made to accept the risk, for example where it stems from an external source and the opportunity to control is limited, or where the potential impact is so low that the cost of managing it would be greater than the cost of the risk being realized. This option may be supplemented by contingency planning for handling the impacts that will arise if the risk is realized.

Transfer	Where another party can take on some or all of the risk more effectively. It is important to note that some risks are not (fully) transferable, in particular it is generally not possible to transfer reputational risk even if the delivery of the service is contracted out.
Treat	Where action is taken to mitigate the risk by taking actions to reduce or eliminate the risk to an acceptable level.
Take Opportunities	For circumstances where the potential gain seems likely to outweigh the potential downside. This also needs to be managed well, with the necessary controls in place.

In practice the PCC will ‘treat’ or ‘tolerate’ the majority of risks.

Risk treatment involves an iterative process of:

- formulating and selecting risk treatment options/actions;
- planning and implementing risk treatment;
- assessing the effectiveness of that treatment;
- deciding whether the remaining risk is acceptable; □ if not acceptable, take further treatment/action.

Taking account of the actions and the controls that have been put in place to treat the risk, the risk assessment (in terms of likelihood and impact) should be repeated to identify the ‘residual risk’.

Step 5: Reviewing and Reporting Risk

The risk management process is evidenced through the maintenance of risk registers. The aim of the risk register is to capture, maintain and monitor information on the risk and the associated control actions that have been put in place to mitigate the risk.

Within the PCC risk registers are maintained at both Corporate and Department levels.

The Corporate Risk Register details risks of a strategic nature. It is formally reviewed on a quarterly basis by all Departments, paying particular attention to the corporate risks that fall within their area.

The Department Risk Registers detail risks which are of a more operational nature. The Department Risk Registers are also formally reviewed on a quarterly basis.

The Corporate and Department Risk Registers are part of an integrated risk management process. Risks can therefore be escalated and de-escalated between Department and Corporate Risk Registers.

Risk Registers will also be held for specific projects, and where appropriate risks can be escalated from project risk registers to Department or Corporate Risk Registers. Similarly information risks identified through the review of information asset registers or data protection impact assessments should also be recorded on the Department or Corporate Risk Registers where appropriate.

An individual member of staff can also identify and report a potential risk for consideration through their line manager. (See Appendix 5)

The updated Corporate Risk Register is brought to the Executive Management Team (EMT) on a quarterly basis for review and approval, prior to presentation to the Audit and Risk Assurance Committee (ARAC) for consideration and approval. It is forwarded to the full Council meeting for consideration at least annually.

5. Roles and Responsibilities

Chief Executive

The Chief Executive as the Accounting Officer of the PCC is responsible for ensuring that a robust risk management system is embedded and operating in the PCC.

As Accounting Officer she is required to sign the annual Governance Statement, as part of the preparation of the Annual Report and Accounts, confirming that a sound system of internal governance is maintained, with an adequate system for the identification, assessment and management of risk in place.

The Chief Executive champions the risk management process, ensuring leadership and commitment, that appropriate resources are available for risk management and the provision of appropriate risk management training for management and staff.

Audit and Risk Assurance Committee (ARAC)

The ARAC supports the Council and the Accounting Officer by providing independent and objective review and opinion on the adequacy and effectiveness of the PCC’s system of internal control. This includes having

DRAFT

oversight of the PCC risk management process and considering and challenging the Corporate Risk Register to provide assurances that the arrangements are effectively working in the organisation. The ARAC reviews the Corporate Risk Register on a quarterly basis.

PCC Council (Council)

The Council is responsible for ensuring that there are robust and effective arrangements for governance, risk management and internal controls in place throughout the PCC.

The Council receives reports from the ARAC on the adequacy of the Corporate Risk Register and also receives the full Corporate Risk Register at a full Council meeting at least annually. The Council should also ensure that the risk management arrangements are reviewed annually or when procedural, legislative or best practice changes occur, and for determining the PCC risk appetite.

Executive Management Team (EMT)

EMT members will develop and maintain a culture of risk management within their area of responsibility. This includes:

- Determining what types of risks are acceptable and which are not in accordance with this Strategy and Policy and the Council’s determination of the PCC risk appetite.
- Ensuring that line managers and all staff are aware of their risk and control responsibilities.
- Ensuring that risk management is incorporated within the horizon planning process.
- Determining the level of risk that the PCC will carry in relation to specific major activities or projects across the organisation as a whole.
- Approving major decisions affecting the organisation’s risk profile or exposure.
- Identifying risks and monitoring their management and control.
- Satisfying themselves that the less significant risks are being actively managed, with the appropriate controls in place and working effectively.
- Annually reviewing the PCC’s approach to risk management and approving changes or improvements to key elements of its processes and procedures.

DRAFT

- Ownership of Department Risk Registers for their area of responsibility.

- Complying with the process as set out in the “Serious Adverse Incidents Policy” and implementing controls to address weaknesses where appropriate.

- Ownership and approval of the Corporate Risk Register through quarterly review at EMT meetings.

Head of Development and Corporate Services

The Head of Development and Corporate Services provides objective advice based on sound evidence and analysis to the Chief Executive, the PCC Council and relevant sub-committees on corporate governance. They have lead responsibility for ensuring that effective and robust risk management processes and systems are in place to ensure good corporate governance within the PCC.

Line managers and staff

All line managers and staff are expected to:

- Have a knowledge of and comply with the PCC Risk Management Strategy and Policy and related policies.

- Alert management to emerging risks or control weaknesses. The Risk Identification template (See Appendix 5) is available for all staff to use.

- Participate fully in the regular risk review process.

- Assume responsibility for risks and controls within their own areas of work.

- Complete the PCC risk management e-learning and attend risk awareness workshops when arranged.

DRAFT

Internal Audit

Although risk management and internal control are management’s responsibility, Internal Audit supports the maintenance of effective internal control through its annual programme of work and subsequent reports. The Head of Internal Audit adopts a risk based approach to planning their work, referring to the PCC risk registers in identifying topics for review across the organisation. Individual audit reports are presented to the ARAC throughout the year, with a mid-year and annual report by the Head of Internal Audit, giving their opinion on risk management, control and governance to support and inform the Chief Executive’s (Accounting Officer) Mid-Year Assurance Statement and Governance Statement.

The Head of Internal Audit, or their deputy, attends the ARAC. They provide assurance on the effectiveness of the risk and control mechanisms in operation and also act as an independent advisor by providing advice on the management of risk, especially those issues surrounding the design, implementation and operation of systems of internal control.

6. Review of Risk Management Strategy and Policy

The risk management processes will be kept under review by the Head of Development and Corporate Services, at least annually, with approved amendments made to the Risk Strategy and Policy where appropriate.

The Risk Strategy and Policy will be formally reviewed and updated at least every 3 years.

7. Equality and Human Rights

This policy has been screened in accordance with the PCC’s statutory duty and is not considered to require a full impact assessment. [NB – equality screening has not yet been completed, and this needs to be done]

DRAFT

Appendix 1: *PCC Corporate Risk Register Template*

<table>
<tr><td colspan="2">Risk Reference:</td><td colspan="2">Date Risk Added:</td></tr>
<tr><td colspan="4">Corporate Risk:</td></tr>
<tr><td colspan="4">Context and Description of Risk:</td></tr>
<tr><td colspan="4">Link to Corporate Objectives:</td></tr>
<tr><td colspan="4">Link to Assurance Framework (Domain):</td></tr>
<tr><td>Risk Status:</td><td>Impact</td><td>Likelihood</td><td>Risk Score</td></tr>
<tr><td>Inherent Risk</td><td></td><td></td><td></td></tr>
<tr><td>Residual Risk (After Treatment)</td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Risk Owner</td></tr>
<tr><td colspan="4"></td></tr>
</table>

Existing Controls	Gaps in Controls & Assurances	Action Plan/Comments	Action Owner	Timescale	Progress on Actions	Assurances / Evidence of Control Effectiveness

Appendix 2 Department Risk Register Template

Corporate Objective:

RISK TITLE:

Description of Risk:

Date Added to Risk Register:

Risk Ref	**Existing Controls**	**Gaps in Controls and Assurances**	**Likelihood**	**Impact**	**Inherent Risk Rating**	**Treatment / Action Plan**	**Action timescale**	**Lead Officer**	**Residual Risk Rating (likelihood x impact)**

Appendix 3

HSC Regional Impact Table – with effect from April 2013 (updated June 2016 and August 2018)

DOMAIN	IMPACT (CONSEQUENCE) LEVELS [can be used for both actual and potential]				
	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 (eg, 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.

Appendix 4

HSC REGIONAL RISK MATRIX – WITH EFFECT FROM APRIL 2013 (updated June 2016 and August 2018)

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 5

RISK IDENTIFICATION TEMPLATE FOR ALL STAFF

All staff have a role in how governance and areas of risk are managed within the Patient and Client Council (PCC)

Each PCC Department has a risk register detailing specific risks. Each risk is assessed according to likelihood of it happening and impact it will have on the organisation. Each risk will have an action plan to mitigate the risk.

Please use this form to inform your manager without delay of any areas of risk or concern you may be aware of and which you feel should be considered as a possible Department risk. This might be about a system of work, a policy/protocol or something specific to your area of work.

Description of Risk	**What action could be taken to manage this risk?**

Department: ______________________________

Date: ______________________________

Appendix 6

The following PCC policies should be read in conjunction with this Risk Management Strategy and Policy:

- Assurance Framework
- Health and Safety Policy
- Fire Safety Policy
- Lone Worker Policy
- Policy on Business Continuity Management
- Standing Orders
- Standing Financial Instructions
- ‘Your Right to Raise a Concern’ Policy
- Fraud Response Policy
- Gifts and Hospitality Policy
- Standards and Guidelines for Monitoring and Handling of Complaints
- ISO 31000:2018 Standard
- Information Governance Policy