



GIG
CYMRU
NHS
WALES

Iechyd Cyhoeddus
Cymru
Public Health
Wales

Reference Number: PHW56

Version Number: 1

Date of next review: January 2020

RISK MANAGEMENT POLICY

Policy Statement

Public Health Wales recognises that no organisation can operate in a risk free environment. Risk however is not something to be feared, rather if it is understood and managed properly it can benefit the organisation, its staff and key stakeholders. The purpose of this Policy is to lay the foundations for an effective risk management system.

Public Health Wales will manage risks at all levels. Strategic risks will be identified by the Board and managed by the Executive Team, whereas operational risks will be identified and managed at the most appropriate level. The organisation will maintain a risk management system which will enable and empower staff to identify, assess, manage and where appropriate exploit risks to the benefit of Public Health Wales.

Policy Commitment

Public Health Wales is committed to the effective management of risk throughout the organisation, and will develop and maintain the appropriate systems to allow such management. The organisation will lay out clearly the roles and responsibilities of all staff when it comes to the management of risk, and these can be found both here and in the Risk Management Procedure, or where appropriate in the relevant process document. All staff are required to understand their role and responsibilities and to comply with the requirements of both this policy and all relevant processes.

All staff will be expected to use the appropriate corporate systems for risk management. At the time of developing this policy, risk is managed through the Datix platform and the use of risk registers (for operational risk) and the Board Assurance Framework for strategic risks.

Whilst there is no specific mandatory training requirement for staff in Corporate Risk Management, those staff who have specific responsibilities will have the appropriate training in order to allow them to carry out the roles.

Supporting Procedures and Written Control Documents

Other related documents are:

Risk Management Procedure
Information Governance Policy
Health and Safety Policy

Scope	This policy will apply to all staff working for Public Health Wales, including contractors and agency staff.
Equality and Health Impact Assessment	
Approved by	Public Health Wales Board
Approval Date	1 June 2017
Review Date	January 2020
Date of Publication:	7 June 2017
Group with authority to approve supporting procedures	Audit and Corporate Governance Committee
Accountable Executive Director/Director	Rhiannon Beaumont-Wood, Executive Director of Quality, Nursing and Allied Health Professionals
Author	John Lawson, Chief Risk Officer

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or [Corporate Governance](#).

Summary of reviews/amendments				
Version number	Date of Review	Date of Approval	Date published	Summary of Amendments

Introduction

This policy introduces the Public Health Wales (PHW) position and expectations in relation to risk management. The document outlines the roles and responsibilities of staff and how they will be trained, and describes the way PHW categorises risk and the risk architecture of the organisation.

For more detail in the procedures to be followed for managing risk, please refer to the associated document 'Risk Management Procedure'.

Section 1 – General

Scope, Aim and Objectives

Scope

This is a Policy which is intended to cover the identification, assessment and management of risk in all forms. The policy and associated procedures relating to risk and will apply to all staff, contractors and visitors.¹

Aim

The aim of this document is to outline the high level arrangements within which PHW will achieve a holistic and effective approach to risk management.

Objectives

This policy will:

- Detail the specific roles and responsibilities for those staff who are charged with the management of risk.
- List the specific policies which PHW will publish to ensure that all staff understand what is required of them
- Outline the training requirements for staff
- Explain the arrangements for complying with all relevant legislation

¹ In the interests of brevity, the term staff is used throughout this document to refer to staff, contractors, agency staff, volunteers, and secondees and visitors

Strategic Context

Public Health Wales is required annually to produce an Interim Medium Term Plan (IMTP), which details what the organisation plans to do over the coming years. The plan sets out the organisational priorities and sets strategic objectives. In order to deliver these objectives, it is necessary to understand the environment in which we operate, and to have clear visibility on what might get in the way of our delivering them. This is why an effective Risk Management System is necessary.

Risk Management starts at the top of the organisation, with the Board setting our direction and our risk appetite, and then permeates down through every level.

Roles and Responsibilities

Public Health Wales Board

The role of the Board is to According to the Auditor General for Wales, the role of the Board is to govern Public Health Wales effectively and in doing so build public and stakeholder confidence that their health and healthcare are in safe hands.

In order for the Board to discharge its responsibilities, it needs to receive assurances that the organisation is effectively managing its risks to ensure delivery of its mission and objectives. One of the principle assurance tools for the Board is the Board Assurance Framework (BAF).

The Board will receive the BAF all formal Board meetings for the purpose of scrutiny and challenge. Through the scheme of delegation, the Audit and Governance Committee meetings will also receive the BAF, whilst relevant sections of it will be received at all other committee meetings.

Chief Executive

The Chief Executive is the responsible officer for PHW and is accountable for ensuring that PHW can discharge its legal duty for all aspects of risk. As the accountable officer, the Chief Executive has overall responsibility for maintaining a sound system of internal control, as described in the annual governance statement. Operationally, the Chief Executive has designated responsibility for implementation of this procedure to the Executive Director Quality Nursing and Allied Healthcare Professionals.

Executive Director, Quality, Nursing and Allied Healthcare Professionals

Is responsible for:

- Operational implementation of the risk management policy and procedures (responsibility has been delegated to the Chief Risk Officer).
- As the Senior Information Risk Owner (SIRO), ultimate responsibility lies here for information risk management.

Deputy Chief Executive / Executive Director of Operations and Finance

Is responsible for:

- Executive level management of risk in relation to both Health and Safety and Business Continuity
- Development of policies and procedures relating to the above

Executive Directors²

Are responsible for:

- The management of risk both collectively as the Executive Team and also at a Directorate level for the risks specifically relating to their directorate.
- Assuming ownership of risks assigned to them in either the Board Assurance Framework or the Corporate Risk Register and reporting as required to the Executive Team and the Board and its committees on the management of that risk.
- Appointing of sufficient risk handlers for their Directorate to enable effective management of their risks.

Board Secretary and Head of Corporate Governance

Is responsible for:

- Development and ongoing review of the Board Assurance Framework.
- Ensuring that the Board and its Committees receive the appropriate reports and assurance for consideration.

² In the interests of brevity the terms Executive Director and Divisional Director are used throughout this document. Executive Director should be read as meaning Executive Directors, other members of the Executive Team and the Director of NHS Wales Health Collaborative. Divisional Director should be read as Divisional Directors and the direct reports of Executive Team members.

Chief Risk Officer

Is responsible for:

- Development and maintenance of the Risk Management System (RMS).
- Development and maintenance of the Corporate Risk Register (CRR) and the Directorate Risk Registers (DRR).
- Supporting the Board Secretary in the development and ongoing review of the Board Assurance Framework
- Development of procedures as are required under this policy (with the exception of Health and Safety and Business Continuity – see Deputy Director Operations and Finance above).
- Delivery of training to staff who have responsibilities under this policy.
- Supporting Executive Directors, members of the Executive Team and senior managers in managing their risks
- Overall management of the Datix system through the Datix Manager
- As Head of Information Governance, management of Information Risk

Divisional Directors

Divisional Directors are responsible for:

- Assuming ownership of risks which are assigned to them in the Directorate Risk Registers and reporting as required to their Executive Director on the management of that risk.

Risk Handlers

Are responsible for:

- Supporting their Directorate risk owners in the management of risk
- Ensuring that new risks are assigned an owner, correctly articulated and assessed by their owner.
- Maintaining the Datix system in so far as it relates to risks for which they are handlers

Datix Manager

Is responsible for:

- Day to day management of the Datix system
- Quality checking all new risks entered onto the Datix system
- Assigning risk handlers to all new risks
- Supporting risk handlers and owners in managing their assigned risks

All staff

All Public Health Wales staff are responsible for:

- Identifying and reporting anything which they believe could present a risk to our business functions, people or service users.

Training

Induction

All staff on induction to Public Health Wales will be provided with a 'Guide to Risk Management' leaflet as part of their induction process.

Level 1 – Staff required to report risks

Whilst there are many different training requirements for specific aspects of risk management (e.g. Health and Safety, Fire, Information Governance), there is no mandatory training requirement for Risk Management in the broader context. All staff who need to report a risk are signposted to a short self directed study package which will cover the basics of identifying, articulating and reporting risks.

Level 2 – Risk Handlers

Face to face training will be delivered to risk handlers which will cover the basic concepts of risk management as described above, but also the practical application of the principles and the mechanics of the Datix system for management of risks.

Level 3 – Risk Owners

Face to face training will be delivered to Risk Owners and is aimed at Executive Directors and other senior managers who need to understand the implications of risk ownership, risk appetite, risk decision making and the escalation of risk.

Level 4 – Caldicott Guardian, SIRO and other specialist roles

This will be any bespoke training required for those charge managing the RMS. This will include training required by the Risk and Information Governance Team.

Section 2 – Categories of Risk

Strategic Risk

These are the highest level risks that could threaten the organisation's ability to deliver on the strategic priorities, as laid out in the Integrated Medium Term Plan (IMTP). Strategic Risks are identified at Board level during the annual development of the IMTP. All strategic risks are assigned an Executive lead and this person will review their strategic risks and associated action plans on a regular basis and provide updates to both the Executive Team and Board.

Corporate Risk

Corporate Risk in all its forms is subject of this policy and the related procedure.

The term Corporate Risk is used in Public Health Wales to encompass all of the operational risks that pose a direct risk to the day to day business of the organisation, or could lead to Directorates or Divisions failing to meet their objectives. This can include:

- Operational Risk
- Project / Programme Risk
- Clinical Risk
- Financial Risk
- Quality Risk

All of these risks will be captured and managed through both Datix and a system of policies and procedures.

Health and Safety Risk

Health and Safety Risk is subject to a specific policy.

Health and Safety is a complex area of legislation one requirement of which is for the organisation to have a Health and Safety Policy. Senior management of Health and Safety Risk is the responsibility of the Executive Director Operations and Finance.

Information Risk

Information Risk is subject to a specific policy.

Information Risk Management is an integral element of good Information Governance. It encompasses numerous disciplines, including use of IT systems, management of paper records, cyber security and physical security of our facilities. Information Risk Management is the responsibility of the SIRO.

Service or Business Continuity Risk

Business Continuity risks are those derived from those possible events which threaten the organisation's ability to deliver its key products and services. These generally fall into three categories of service failure:

- Access to premises.
- Access to resources (e.g. IT systems).
- Access to staff.

The majority of Business Continuity risks will tend to be high impact / low likelihood events, and many are derived from either the National Threat Assessment / National Risk Register³, or by the Local Risk Registers⁴.

Business Continuity Risk Management is the responsibility of the Executive Director Operations and Finance.

Section 3 – Management of Risk

Introduction

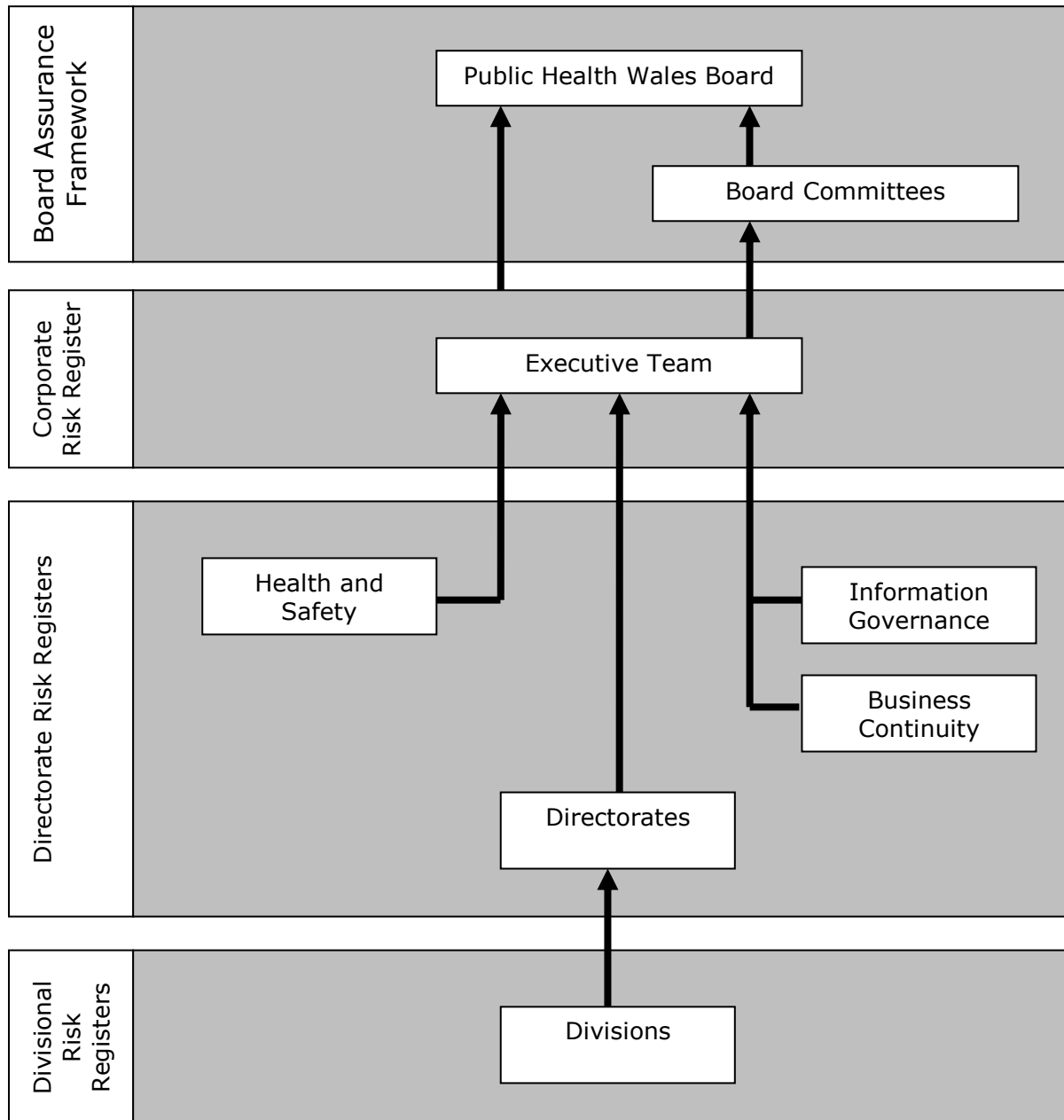
Whilst this section gives an overview of how risk is managed throughout Public Health Wales, full details of how risk should be managed are contained within the controlled document 'Risk Management Procedure'

³ Published annually by the Cabinet Office

⁴ Published annually by the Local Resilience Forum

Risk architecture

The risk architecture is the structure within which an organisation manages risk. The risk architecture within Public Health Wales is shown below.



Risk Appetite

Risk appetite is defined as

'The amount of risk that Public Health Wales is willing to seek or accept in the pursuit of its long term objectives.'

Public Health Wales' risk appetite is set on an annual basis by the Board, when the decisions are being made around the organisation's strategic priorities for the following year. The purpose of setting the risk appetite is to ensure that all staff throughout Public Health Wales are aware of it and understand the amount of risk to which the organisation is prepared to be exposed whilst going about their day to day business.

Identification and capturing of risks

All staff should be aware of the potential for risks to emerge which may affect the business and all staff should be prepared to identify and report risks as appropriate. When a possible risk is identified, staff should normally discuss it first with their line manager. This is to avoid duplication of effort, as sometimes risks are identified which are already being managed but have perhaps been articulated differently.

Once it is confirmed that a new risk has been identified, the details should be entered onto the Datix system. This will normally be achieved through one of the Directorate's risk handlers.

Once correctly identified and assessed, the risk will then be transferred to one of a series of risk registers, depending on the seriousness of the risk. Generally risk should be managed at the lowest level possible, proportionate to the level of exposure to which the risk.

Risk Registers

A Risk Register is simply a visual representation of the identified risks, together with an assessment of their severity, the risk management measures in place, the control environment and any further actions which are planned or required. The register is a snapshot of the risk information at the moment it is taken. Public Health Wales has risk registers at various levels. Full details of the publication and distribution of risk registers can be found in the document '*Risk Management Procedure*'

Appendix 1 - Glossary of Terms

BAF –	Board Assurance Framework
BC –	Business Continuity
CRO –	Chief Risk Officer
CRR –	Corporate Risk Register
DirRR –	Directorate Risk Register
DivRR –	Divisional Risk Register
DM –	Datix Manager
H&S –	Health and Safety
IG –	Information Governance
RH –	Risk Handler
RIGT –	Risk and Information Governance Team
RM –	Risk Management
RMS –	Risk Management System
RO –	Risk Owner
SIRO –	Senior Information Risk Owner
SRO –	Senior Responsible Owner

NOTE

In the interests of brevity the terms Executive Director and Divisional Director are used throughout this document. Executive Director should be read as meaning Executive Directors and other members of the Executive Team. Divisional Director should be read as Divisional Directors and the direct reports of Executive Team members.