GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** PHW56 **Version Number: 2** **Date of next review:** Sept 2028

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 avoided, if it is understood and managed properly it can benefit the organisation, its staff and key stakeholders, through identification of risk opportunities. 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, once the risk has been understood in its entirety. 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 in the delivery and achievement of its objectives.

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 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 including corporate risks) and the Strategic Risk Register and Board Assurance Framework for strategic risks.

There is specific training available for all staff in relation to Risk Management, with those staff who have specific responsibilities to undertake additional training in order to allow them to carry out the roles.

Supporting Procedures and Written Control Documents

All corporate policies and procedures are available on the Public Health Wales website

Other related documents are:

• Risk Management Procedure • Information Governance Policy • Health and Safety Policy • Putting Things Right Incident and Management Procedure	
Scope This policy will apply to all staff working for Public Health Wales, including contractors and agency staff and any hosted organisations	
Equality and Health Impact Assessment	An Equality and Health Impact Assessment has been completed and can be viewed on the policy webpages.
Approved by	Public Health Wales Board
Approval Date	25/09/2025
Review Date	25/09/2028
Date of Publication:	27/0/2025
Group with authority to approve supporting procedures	Audit and Corporate Governance Committee
Accountable Executive Director/Director	Claire Birchall, Executive Director of Nursing, Quality and Integrated Governance
Author	Beth Osborne, Risk Manager

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 the Board Business Unit

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**
1	2020	26/11/2020	22/01/21	First Policy
2	2025	25/09/2025	27/10/25	Updated policy to reflect Strategic Risk Register, Split of Information Risk responsibilities and the current planning cycle. Updates to reflect re-organisation changes relevant to the risk responsibilities Updates following formal consultation Updates following review by Leadership Team

Introduction

This policy introduces the Public Health Wales approach and expectations in relation to risk management. The document outlines the Board responsibilities and expectations, describes the way Public Health Wales 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, hosted organisations and visitors.[1]

Aim

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

Objectives

This policy will:

- Explain the role and expectations of the Board in relation to risk management;
- Detail the high-level responsibilities for implementing this policy;
- Signpost the specific policies and procedures which Public Health Wales will publish to ensure that all staff understand what is required of them;
- 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 have a strategic plan to 2035. We develop a 3-year IMTP on a rolling cycle and we have an annual operational plan.

Strategic risks are identified against the long-term strategic plan priorities.

To deliver these priorities, 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 Auditor General for Wales describes the role of the Board as to govern Public Health Wales effectively and in doing so build public and stakeholder confidence that their health and healthcare are in safe hands.

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 source of the principal assurance tools for the Board is the Strategic Risk Register. The Strategic Risk Register forms part of the wider Board Assurance Framework within which the Board receives assurance in a number of areas, including risk management.

The Board will scrutinise the Strategic Risk Register at formal Board meetings for the purpose of challenge and receiving assurance at a frequency determined by the Board Business Unit. Through the scheme of delegation, all relevant Board Committees will receive a version of the Strategic Risk Register pertinent to the function of the respective Committee and the Audit and Corporate Governance Committee having a lead role in providing overall assurance to the Board in relation to the management of strategic risks.

Chief Executive

The Chief Executive is the responsible officer for Public Health Wales and is accountable for ensuring that Public Health Wales 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 delegated responsibility for implementation of this policy and associated procedure to the Executive Director of Nursing, Quality and Integrated Governance.

Executive Director, Nursing, Quality and Integrated Governance

Is responsible for:

- Operational implementation of the risk management policy and procedures (responsibility has been delegated to the Head of Risk Management).

Senior Information Risk Owner (SIRO)
Is responsible for:

- The SIRO is currently the Director of Research, Data and Digital who is responsible for the organisation's information risk management system

Executive Director of Operations and Finance

Is responsible for:

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

National Director of Health Protection and Screening Services, Executive Medical Director

Is responsible for:

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

Executive Directors[2]

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.

[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 and other members of the Executive Team. Divisional Director should be read as Divisional Directors and the direct reports of Executive Team members.

- Assuming ownership of risks assigned to them in the Board Assurance Framework 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.

Assistant Directors

Are responsible for:

- The active review and management of corporate risks collectively as the Leadership Team.
- As individuals, members of the Leadership Team are fully briefed on corporate risks within their Directorates in order to provide any additional information required in order for the collective Leadership Team to consider the risks.

Board Secretary and Head of Board Business Unit

Is responsible for:

- Ensuring the Annual Governance Statement includes the system of internal control and establishes the Business Executive Team, Committee and Board work plans to include strategic and corporate risk register.

Head of Risk Management

Is responsible for:

- Development and maintenance of the Risk Management Framework.
- Development and maintenance of the Strategic and Corporate Risk Registers.
- Development of procedures as are required under this policy (with the exception of Health and Safety and Business Continuity – see interim Executive Director of Operations and Finance and Medical Director/ National Director of Screening and Health Protection Services above).
- Delivery of training to staff who have responsibilities under this policy, delegated to the Risk Manager.
- Supporting Executive Directors, members of the Executive Team and senior managers in managing their risks.
- Overall management and suitability of the risk management system (namely Datix Web).

Section 2 – Categories of Risk

Strategic Risks

These are the highest-level risks that could threaten the organisation's ability to deliver on the strategic priorities, as laid out in the Strategic Plan. Strategic Risks are identified at Board level during annual planning processes. All strategic risks are assigned an Executive lead, and this lead will review their strategic risks, internal controls and associated action plans on a regular basis and provide updates to both the Executive Team and Board.

Operational Risks

Any 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 are considered operational risks. Such examples are:

- Clinical Risk
- Resource Risk (Staffing)
- Reputational Risk
- Project/Programme Risk
- Financial Risk
- Quality Risk
- Safety Risk
- Information Risk
- Business Continuity Risk

All operational risks will be captured and managed through both Datix Web 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 Interim Executive Director Operations and Finance. It is the responsibility of the Interim Executive Director of Operations and Finance to ensure that the policy complies with the approach and principles set out in the Risk Management Policy and Procedure.

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. Responsibility for Information Risk Management sits with the SIRO being responsible for Information Governance risks, IT and cyber security risk.

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 Register[3], or by the Local Risk Registers[4].

Business Continuity Risk Management is the responsibility of the Medical Director/ National Director of Health Protection and Screening Services/ Medical Director. Based on the level of severity or categorisation of the risks identified, there may be a requirement to escalate these risks through organisational governance processes, to be captured via the Corporate or Strategic Risk Registers. Therefore, close alignment between Business Continuity Team and the Risk Management Team is useful to ensure operational triggers mirror risk management escalation arrangements.

Section 3 – Management of Risk

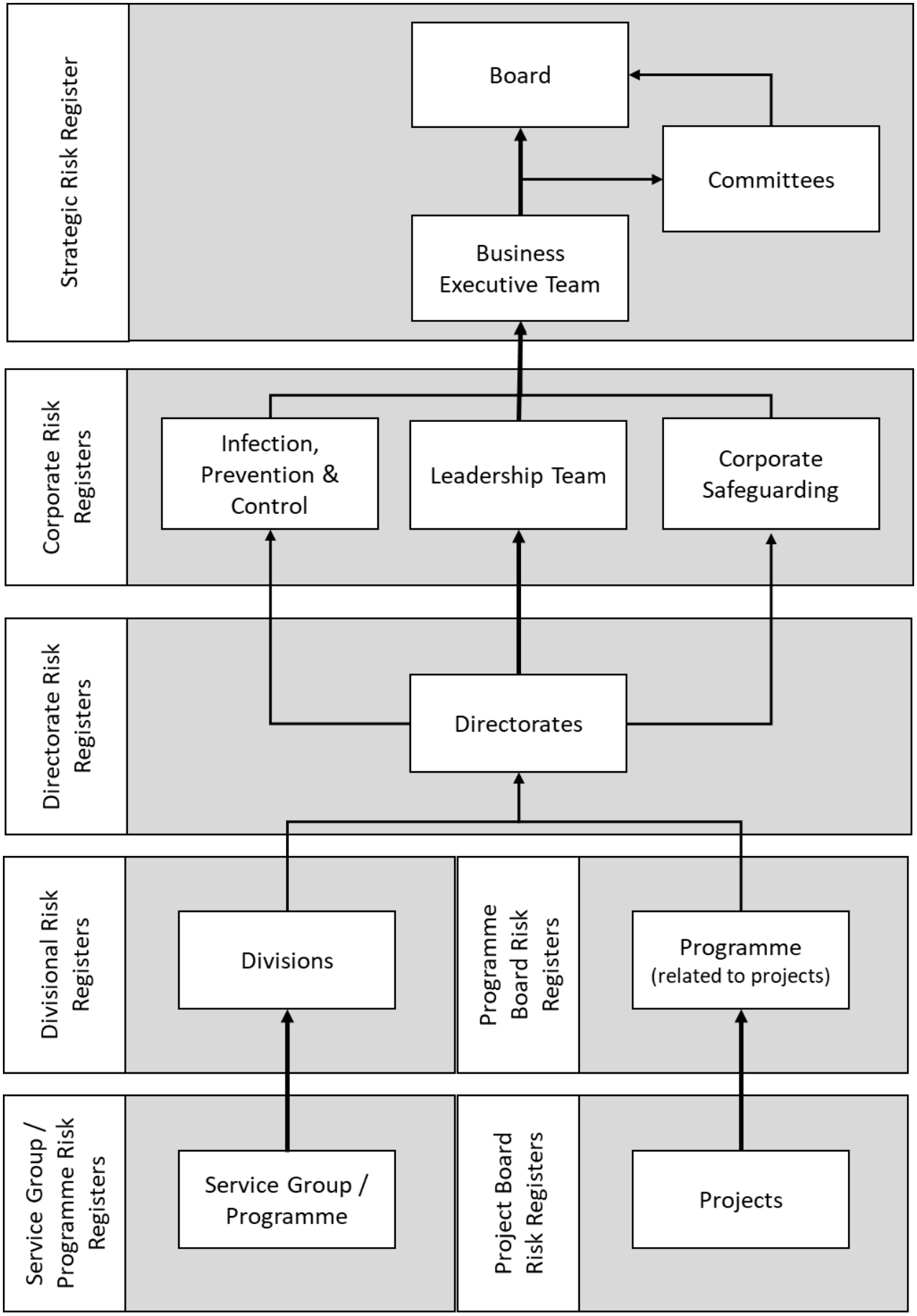
Introduction

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.


Strategic Risk Register
Board
Committees
Business Executive Team
Corporate Risk Registers
Infection, Prevention & Control
Leadership Team
Corporate Safeguarding
Directorate Risk Registers
Directorates
Divisional Risk Registers
Divisions
Programme Board Risk Registers
Programme (related to projects)
Service Group / Programme Risk Registers
Service Group / Programme
Project Board Risk Registers
Projects

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' strategic 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.

Once it is confirmed that a new risk has been identified, the details should be entered onto the Datix Web 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 severity of the risk. Generally, risk should be managed at the lowest level possible, proportionate to the level of exposure.

Risk Registers

A Risk Register is 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'.*