RISK MANAGEMENT POLICY

Executive Sponsor & Function: Board Secretary

Document Author: Board Secretary

Approved by: HEIW Board

Approval Date: 30 July 2020

Scope:

1.2 This Risk Management Policy and any arrangements made under it applies to:

- all persons employed or engaged by Health Education and Improvement Wales (HEIW) including part time workers, temporary and agency workers and those holding honorary contracts.

- Visitors, contractors and volunteers.

Other NHS Health Boards and Trusts will have their own health and safety policies which will apply to HEIW staff working in NHS premises elsewhere across Wales.

Date of Equality Impact Assessment: [19/04/19]

Equality Impact Assessment Outcome:

This policy has been screened for relevance to equality. No potential negative impact has been identified so a full equality impact assessment is not required.

Review Date: July 2021

Version: v2

CONTENTS **Page**

Policy Statement

Health Education Improvement Wales (HEIW) 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.

HEIW 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 HEIW.

Policy Commitment

HEIW 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. 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 HEIW's risks are managed through the use of risk registers (for operational risk) and the Board Assurance Framework for strategic risks. Health and safety risks are however, managed through Datix.

All Senior staff and managers are required to attend mandatory training in Corporate Risk Management.

Introduction

This policy introduces the HEIW 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 HEIW categorises risk and the risk architecture of the organisation.

Section 1 – General

1.1 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]

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

1.2 Aim

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

1.3 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 HEIW 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.

1.4 Strategic Context

HEIW 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.

1.5 Roles and Responsibilities

1.5.1 HEIW Board

The role of the Board is to govern HEIW effectively. 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 once per year for the purpose of scrutiny and challenge. Through the scheme of delegation, the Audit and Assurance Committee meetings will also receive the BAF once per year.

The Corporate Risk Register is focussed on HEIW's key objectives and identifies the principal risk and key controls. Given this the Corporate Risk Register shall be the vehicle for providing regular assurance for the BAF. The Corporate Risk Register shall be reviewed by the Board twice a year and by the Audit and Assurance Committee on a quarterly basis.

1.5.2 Chief Executive

The Chief Executive is the responsible officer for HEIW and is accountable for ensuring that HEIW 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 policy to the Board Secretary.

1.5.3 Board Secretary

Is responsible for:

- operational implementation of the risk management policy;
- as the Senior Information Risk Owner (SIRO), ultimate responsibility lies here for information risk management;
- development of policies and procedures relating to the above;
- development and ongoing review of the Board Assurance Framework;
- ensuring that the Board and its Committees receive the appropriate reports and assurance for consideration.

1.5.4 Executive Directors

Are responsible for:

- the management of risk both collectively as the Executive Team and 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 enough resource for their Directorate to enable effective management of their risks;
- the individual Directorate Risk Register.

1.5.5 Deputy Chief Executive / Director of Workforce and Organisational Development

In addition to the Executive Director responsibility is also responsible for:

- Executive Team level management of risk in relation to both Health and Safety and Business Continuity.

1.5.6 Directorate Managers

Directorate Managers 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;
- 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.

1.5.7 All staff

All HEIW staff are responsible for identifying and reporting anything which they believe could present a risk to our business functions or people.

1.6 Allocation of Responsibility for a Risk

Executive Directors shall take responsibility for managing risks within their Directorates. Where a risk arises from a project, programme or matter undertaken on a cross-Directorate basis the risk will be allocated to the Executive Lead as detailed within the IMTP.

1.7 Training

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 Owners

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

Level 3 – SIRO and other specialist roles

This will be bespoke training required for those charged with managing the Risk Management System.

Section 2 – Categories of Risk

2.1 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 objectives are assigned an Executive Lead within the IMTP. This person will review their strategic risks and associated action plans on a regular basis and provide updates to both the Executive Team and the Board.

2.2 Corporate Risk

Corporate Risk in all its forms is subject of this policy.

The term Corporate Risk is used in HEIW 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 failing to meet their objectives. This can include:

- Operational Risk
- Project / Programme Risk
- Educational Risk
- Financial Risk
- Public Relations Risk

All these risks will be captured and managed through risk registers and a system of policies and procedures.

2.3 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 Director of Workforce and Organisational Development.

2.4 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.

2.5 Service or Business Continuity Risk

Business Continuity Risk is subject to a specific policy.

Business Continuity risks are those derived from those possible events which threaten the organisation’s ability to deliver its key products and services.

Most Business Continuity risks will tend to be high impact / low likelihood events.

Business Continuity Risk Management is the responsibility of the Director of Workforce and Organisational Development.

2.6 Fraud Risk

To ensure enough focus is given to counter-fraud, and the steps taken to mitigate the risk of the same, it is a requirement that Fraud be a standard item on each Directorate Risk Register.

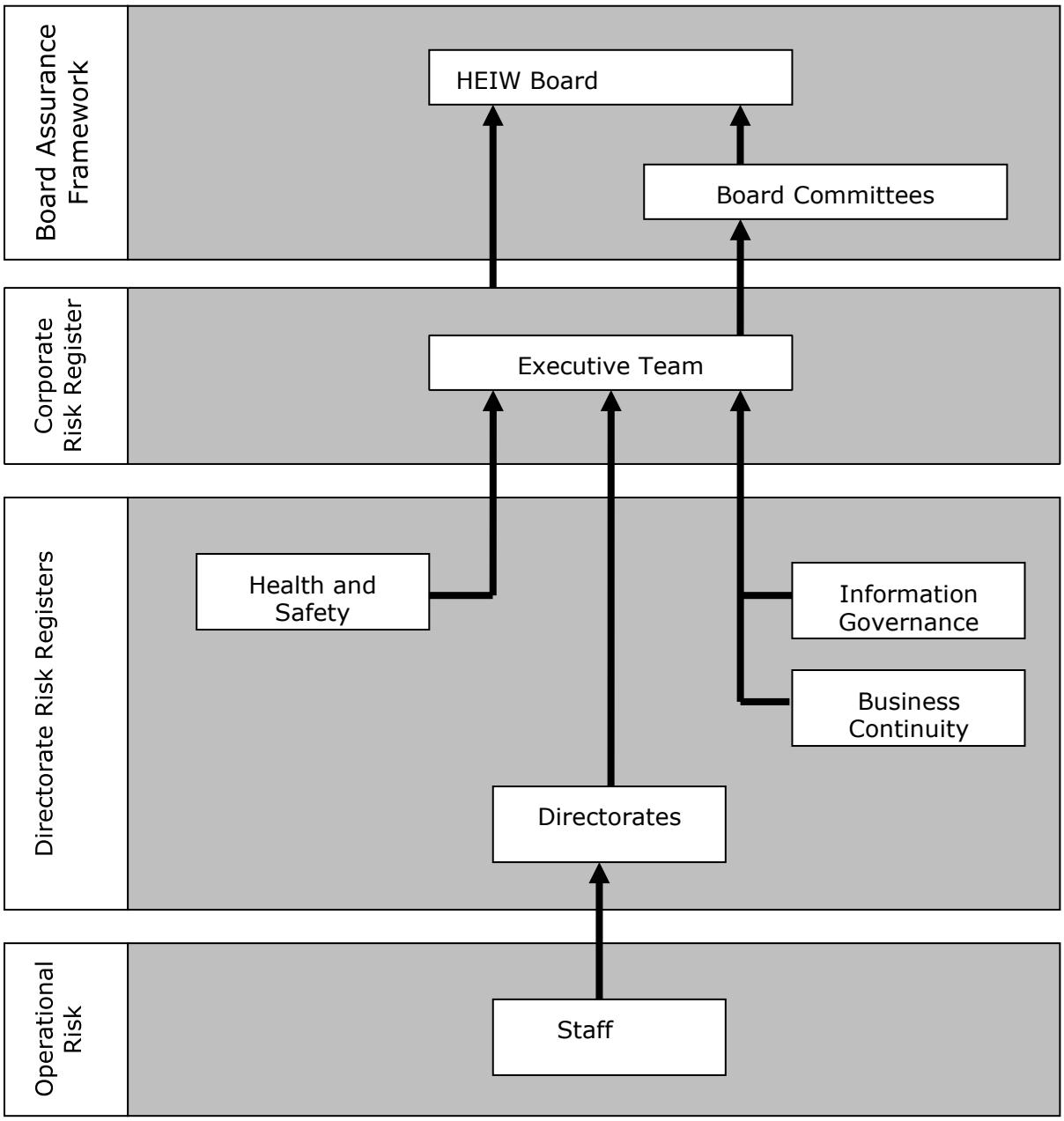
Section 3 – Management of Risk

Introduction

This section gives an overview of how risk is managed throughout HEIW.

3.1 Risk Architecture

The risk architecture is the structure within which an organisation manages risk. The risk architecture within HEIW is shown below.



3.2 Risk Appetite

HEIW's 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 HEIW 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. HEIW's Risk Appetite levels are detailed in Annex 1.

3.3 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 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.

3.4 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.

HEIW's risk registers will utilise the risk assessment, risk appetite and scoring method outlined in Annex 1. HEIW's template risk register is attached at Annex 2. All HEIW Directorate Risk Registers shall use the template attached at Annex 2. All HEIW programme and project risk register will use this template as the basis for their risk register.

3.5 Ongoing Risk Management

Once a risk has been properly identified, articulated and assessed it can then be managed.

3.6 Escalation

As previously stated, to be effective, risk needs to be managed at the lowest appropriate level. A risk that is deemed sufficiently material by its lead Director may be escalated onto the Directorate Risk Register. A risk will be escalated from the Directorate Register to the Corporate Risk Register when the Directorate either have concerns about their capacity or authority to manage the risk, or they do not have the resources (e.g. budget, staff etc) to manage it, risk requires c or it is deemed to represent a significant public relations risk.

Not having capacity or authority to manage a risk should not be viewed as a lack of capability, but rather a recognition that a risk is either so severe that it needs to be managed

at a higher level, or possibly that it transcends more than one area of business or Directorate. It is anticipated, although this is not a binding requirement, that such a risk when being escalated onto the Corporate Risk Register will have a minimum risk score of 14.

In the event of a requirement to escalate a risk, from the Directorate Risk Register to the Corporate Risk Register, the matter will require the approval of the Executive Team.

3.7 Removal

The removal of a risk from the Corporate Risk Register shall require the approval of the Audit and Assurance Committee.

Risk should not be removed from the system until such time as the risk has been eliminated. Risks may reduce in their importance over time, and so may be de-escalated down to an appropriate level of management.

Annex 1

Risk Assessment and Scoring

In order to effectively assess a risk, it is necessary to consider two factors: Likelihood and Impact.

HEIW utilises a common form of risk scoring referred to as a 5x5 risk matrix. Likelihood and Impact are assessed on a scale of 1 to 5, and then the two scores are multiplied together to arrive at the final risk score.

As scoring is a subjective process guidance is provided through the tables below.

Risk Scoring Matrix

Level	Colour	Score Range
Low		1-6
Moderate		7-14
High		15-25

LIKELIHOOD						
	Probable	**5**	**10**	**15**	**20**	**25**
	Likely	**4**	**8**	**12**	**16**	**20**
	Possible	**3**	**6**	**9**	**12**	**15**
	Unlikely	**2**	**4**	**6**	**8**	**10**
	Rare	**1**	**2**	**3**	**4**	**5**
		Negligible	**Minor**	**Moderate**	**Major**	**Critical**

Risk Appetite Levels

Appetite Level	Described as:	What this means
None	Avoidance of risk and uncertainty is a key organisational objective.	Avoidance of loss is key objective, play safe, avoidance of developments. Priority for tight controls and oversight.
Low	Minimal, or as little as reasonably possible, is preferred for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential.	Prepared to accept the possibility of very limited financial loss if essential. Win any challenges re compliance. Innovations avoided unless essential.
Moderate	Cautious is preferred for safe delivery options that have low degree of inherent risk and may only have limited potential for reward.	Prepare to accept some possibility of some financial loss. Limited tolerance for sticking neck out. Tendency to stick with status quo, innovation in practice avoided unless really necessary
High	Open and willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and Value for Money).	Prepared to invest for return & minimise the possibility of financial loss. Value and benefits considered. Gains outweigh adverse consequences. Innovation supported.
Very High	Seek and be eager to be innovative and too chose options offering potentially higher business rewards (despite greater inherent risk). Or also described as mature and confident in setting high levels of risk appetite because controls, forwards scanning and responsiveness systems are robust.	Investing for best possible return & acceptance of possibility of financial loss. Chances of losing any challenge are real and consequences would be significant. Desire to break the mould. High levels of devolved authority – management by trust not control.

Annex 2 – Template for the HEIW Risk Register

[Risks should be scored on the basis of the Risk Scoring Matrix and Risk Appetite Levels contained within Annex 1]

Date Added	Ref (Risk Area)	Risk Description and [Executive/Manager] Owner	Inherent Risk			Risk Appetite	Mitigating Action	Residual Risk			RAG Status	Progress
		Details of risk If…then… impact…	Impact	Probability	Overall Score	None Low Moder. High V.High	Summary of action to date or proposed action to reduce risk impact or proximity – this should include a deadline or timetable for completing actions	Impact	Probability	Overall Score	R/A/G & trend	
1.		[If …….then ….. impact] **[Insert the name of the owner]**					[please populate this section in accordance with the above guidance]					