GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** PHW56-TP01 **Version Number:** 2 **Date of next review:** 1 March 2021

RISK MANAGEMENT PROCEDURE

Introduction and Aim

This document describes the processes for management of risk. It explains key terms and concepts, outlines the responsibilities of staff, and details the arrangements for the management of risk from initial identification through to eventual removal.

Linked Policies, Procedures and Written Control Documents

Risk Management Policy
Health and Safety Policy
Information Governance Policy

Scope

The procedure will apply to the management of risk across the organisation and applies to all staff. Responsibilities are clearly set out in the document and are additional to those general responsibilities found in the Risk Management Policy.

Equality and Health Impact Assessment	Insert link to completed **Integrated Screening Tool**.
Approved by	Audit and Corporate Governance Committee
Approval Date	13 March 2018
Review Date	1 March 2021
Date of Publication:	15 March 2018
Accountable Executive Director / Director	Sian Bolton, Acting Executive Director, Quality Nursing and Allied Health Professionals
Author	John Lawson, Chief Risk Officer

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments Highlighted in grey**
2	8-Feb-18	13-Mar-18	15-Mar-18	Introduction of Risk Appetite model. Revised risk scoring matrix and indicators.

Contents

Abbreviations

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.

Introduction

Risk is defined as ‘The effect of uncertainty on objectives’.

The avoidance of risk is as undesirable as it is impossible. Risk surrounds us in our everyday lives and we as people have evolved to deal with it as a matter of course. We accept and take risks every day of our lives and indeed in order to develop we need to.

Organisations are no different. An organisation that is not prepared to take any risks whatsoever, will not survive very long. By the same token however, an organisation which is reckless in the risks it takes will have a very bleak future. For this reason organisations have to understand the risks it faces and then manage them effectively enough to ensure that they don’t prevent them from achieving what they want to achieve. This is the discipline of risk management.

Public Health Wales is developing its Risk Management System (RMS) in line with the requirements of the International Standard ISO31000. The aim is to develop a RMS which gives everyone in the organisation the confidence that they understand their risk and control environments, what their responsibilities are and how to discharge them effectively.

Risk in Public Health Wales is managed through the Datix software platform, which itself is managed by the Risk and Information Governance Team. For further details, please consult the relevant controlled documents.

Summary of responsibilities

Specific responsibilities in this procedure

This document sets out specific responsibilities for individuals. These are detailed in the main text of the document but the table below summarises those responsibilities.

Role	Responsibilities	Page refs
Chief Executive*	SRO for CRR & BAF	15,16
Deputy Chief Executive*	SRO for H&S and BC Risk Registers	15,16,17
Executive Director Quality Nursing and Allied Health professionals*	SRO for IG Risk Register	15,17
Executive Directors*	Scrutinising and managing Corporate and Directorate Risks	17
Divisional Directors*	Scrutinising and managing Directorate and Divisional Risks	17
Risk Owners	Ownership and accountability for risks Risk Assessment Risk Decision making Risk Action planning Risk Escalation / De-escalation	11 13 13 14 14
Risk Handlers	Quality check on risk description Identification of risk owners Liaison with reporters and risk owners	13
Datix Manager	Management of the Datix system Initial Quality Control check on new risks Liaison with risk owners / handlers	13
Chief Risk Officer	Maintenance of the Risk Management System	All
Board Secretary	Maintenance of the Board Assurance Framework	19
All staff	Identification of risks Entry of risks onto Datix	12

* In addition to any responsibilities assigned as risk owners

Section 1 – Guidance

Principles of risk management

There are as many definitions of risk as there are experts to cite them. The reality is that risk means many things to many people, and so for our purposes we need to keep it simple. In its simplest terms, a risk means that 'Something bad might happen'. The key word in there is 'might' or in other words there is always a level of uncertainty.

It is also true that in some fields, particularly strategic planning risks need to be considered in the context of opportunity. However, for the purposes of this process, risk will only be considered in terms of what might go wrong. Anyone wishing advice on opportunity risk should contact the Chief Risk Officer.

Hazards, risks, and problems

It is important to understand from the outset what you are dealing with. These terms are frequently used interchangeably which is incorrect; they are distinctly different and need to be considered as follows.

Hazard

A hazard is something which has the potential to cause harm. In the context of operational business risk, it is sometimes easier to use the term threat instead, and the word harm should be read as harm to what you are trying to achieve. In other words, if there is something which has the potential to stop you achieving your objectives, this is a hazard (or threat).

Risk

If a hazard has the potential to cause harm, then a risk is the likelihood of harm being caused. The key thing here is that for anything to be described as a risk there **MUST** be some level of uncertainty connected with it. If there is no uncertainty, then you do not have a risk – you have a problem.

Problem

A problem is simply something which is happening or has happened, and needs to be dealt with. Problems are not managed through the risk management system and so are not further referred to within this document.

Articulating a risk

Correct articulation of a risk helps to clarify the issues and enables effective risk management. If the risk is not properly articulated in the first place the difficulties in managing it are simply magnified as the process develops.

There are three steps to articulating a risk:

Step 1. Risk Description.

You must be able to start the risk description with the words, 'There is a risk that (something bad might happen)' If you cannot start the risk description with these words, then you probably don't have a risk, you have a problem. In articulating the 'something bad' it is important to consider what might go wrong or what might cause us to fail to meet our objectives.

Step 2. Cause.

This needs to start with the words 'This will be caused by...', followed by a simple description of the hazard or threat.

Step 3. Impact.

This needs to start with the words 'The impact will be that...' followed by a description of what the impact would look like if the risk were to be realised.

Risk assessment and scoring

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

Public Health Wales 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 to arrive at the final risk score (between 1 and 25 with 1 being the lowest).

The scoring is a very subjective process and so some guidance on what different likelihoods and impacts would look like is provided[1].

It is important to remember that these descriptors are provided only as guidance and you should not attempt to be too scientific with your assessment.

There are three different scores to be arrived at in assessing any risk:

[1] See Appendix A

Inherent Risk

This is the risk, considered without taking account of any controls. Sometimes called the raw risk score, this is important as it shows the true severity of the risk should it ever be realised. It should be noted that in some areas of risk management (notably Health and Safety) inherent risks are scored with controls already in place. This is inappropriate for corporate risk management as it does not give the risk owner sufficient understanding of the reliance placed on the controls.

Residual (Current) Risk

This is the risk, considered with any existing controls taken into account. The residual risk score will always be lower than the inherent risk, and the important point is that the greater the difference between the two scores, the greater the reliance on the control environment.

Target Risk

This is the risk score that the Risk Owner, having decided to treat[2] the risk, needs to be actively working towards. The target score may be the same as the residual, or lower, but will never be higher. If the target score is lower than the residual, it must be accompanied by an action plan to achieve the target.

Further guidance on how to assess risks is provided in the Risk Handler Training.

Risk Treatment and risk decision making

There are four options when deciding how to treat a risk and this is known as the 4T approach to risk decision making.

Terminate

This is where the activity that could lead to the risk being realised is itself terminated so that the risk can no longer occur.

Transfer

This is where a third party, usually on the payment of a premium agrees to take on the risk on your behalf. The most common form of risk transference is in insurance, whereby we pay insurance companies a premium to accept (usually a financial) risk on our behalf. This is a rare form of operational risk treatment and so anyone considering this as an option should contact the Chief Risk Officer for advice.

---

[2] See p13

Tolerate

This is where the risk has been assessed and the RO has determined that the risk is acceptable – in other words it is within our risk appetite. Once this decision has been taken, although the risk should be kept under regular review, there would not normally be any requirement for an action plan.

Treat

This is where the risk has been assessed and the RO has determined that it still presents an unacceptable level of exposure and so needs further treatment. Treatment may be in the form of investment in resources, contingency planning or any other action that may help to reduce the risk further.

Controls and Assurances

A control is something which is actively working to control a risk. For a control to be valid it must be:

- Actively working at the time (i.e. not planned for some future date)
- Something which is actually within our control

The whole network of controls for a particular risk is called the risk's 'control environment.'

An assurance on the other hand is something which provides evidence that a control is effective.

Risk action planning

Risk action planning is no different to any other form of action planning and there are clear advantages to using the tried and tested SMART process for developing an action plan.

- S - Specific
- M - Measureable
- A - Achievable
- R - Relevant
- T – Timescaled

This system is adequately detailed in management training and so no further explanation is provided here, except to say that in this context 'Relevant' must mean that the action once complete (either on its own or in conjunction with other actions) will have some effect on the control environment.

Section 2 – Management and Ownership of risk

Risk architecture

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

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.

Procedure for setting risk appetite

Roles and responsibilities

Board members

- Setting the risk appetite levels together with supporting statements against each Strategic Objective.
- Signing off the final Annual Statement of Risk Appetite.

Chief Executive

- Ensuring that all Corporate risks take account of the Annual Statement of Risk Appetite.

Executive Directors / Directors

- Ensuring that all Directorate risks take account of the Annual Statement of Risk Appetite.

Chief Risk Officer

- Advising and training Board members and risk owners in the development and implementation of the Annual Statement of Risk Appetite.

- Preparing the Annual Statement of Risk Appetite in accordance with the Board's direction.

Board Secretary and Head of Corporate Governance

- Ensuring that the Annual Statement of Risk Appetite is published in accordance with organisational governance requirements.

Risk owners

- Assessing their risks against the scoring system in Appendix 1
- Regularly reviewing their risks to ensure that they align properly to the Annual Statement of Risk Appetite.

Procedure

- The Board will agree the Strategic Objectives for the year in question.

- Having agreed the strategic objectives, the Board will then consider each strategic objective in turn, and for each one consider and agree the appetite level as set out below.

- Having agreed the appetite level, the Board will agree a short statement of rationale to support the level agreed.

- The Board will communicate the agreed levels together with the supporting statements to the Chief Risk Officer.

- The Chief Risk Officer will prepare the Annual Statement of Risk Appetite and submit it to the next available Executive Team meeting for approval prior to submission to Board.

- The final Annual Statement of Risk Appetite will be presented to the next available Board meeting for approval.

- Once formally approved by the Board, the Chief Risk Officer will ensure that the Annual Statement of Risk Appetite is communicated to all risk owners.

- All risk owners will then review their current risks to ensure that they align to the Annual Statement of Risk Appetite.

- The Chief Executive will review the Corporate Risk Register to ensure that all identified Corporate risks are aligned to the Annual Statement of Risk Appetite.

- All Executive Directors / Directors will review their Directorate Risk Register to ensure that all identified Directorate risks are aligned to the Annual Statement of Risk Appetite.

Risk ownership

For risk management to be really effective, risks need to be managed at the lowest appropriate level and only escalated when the risk is either so serious that it requires a higher level of management, or that the actions required to manage it are beyond the capacity or authority of the manager.

This means that one person needs to take responsibility for managing any risk, and be accountable to their managers for it. This person is known as the Risk Owner (RO). In Public Health Wales, ROs are usually Executive Directors or members of the Executive Team, or their direct reports. This is not exhaustive however, and the important point is that the RO needs to be in the right position and have sufficient seniority to be able to take responsibility for the risk in question. ROs will be supported by appropriate training.

Risk handlers

Risk Handlers (RH) are suitably trained staff who are able to support ROs with the administrative arrangements around the management of their risks. RHs are trained in how to use Datix, how to produce and update risk registers and how to escalate and de-escalate risks. They are also given training in risk management to enable them to advise and support risk owners in their decision making.

Management levels

Risks will generally be managed at one of four levels

- Strategic
- Corporate
- Directorate[3]
- Divisional / service level

When a risk is first identified, the Risk and Information Governance Team (RIGT) will make an initial assessment of which level is most appropriate and will assign a RH. That handler will identify the most appropriate person to be the RO and initiate discussions with the owner to manage the process.

[3] Directorate will also encompass H&S, IG and BC. See p15 for details

Section 3 – The Risk Management Process

Initial identification, articulation and assessment

Risk Identification

This is the initial identification of any given risk. Staff can either raise the risk with their manager or if appropriate may enter the risk directly onto Risk Management module within Datix. Any staff who have not received training in Risk Management are encouraged to refer to the document 'Risk Management FAQs' which is available for download from Datix, prior to entering details of the risk.

Except in cases of urgency, it is recommended that the person identifying the risk should discuss the matter first with their line manager.

Responsibilities: All staff are responsible for bringing to the attention of their manager, any situation which they believe may pose a risk to the organisation.

Datix Entry

This is where the risk is entered onto the Datix system. For full details on how to enter risks onto the system, refer to the user guides available through the Datix interface

Responsibilities: All staff have access to Datix for the purposes of reporting a risk.

Quality Control Check

This is where the risk is reviewed by the Datix Manager (DM) to ensure that the reported risk complies with this procedure in terms of reporting requirements. It is important to note that this is not an assessment of the detail or content.

Responsibilities: The DM is responsible for carrying out the quality control check. Once completed, the DM can either return the risk to the reporter with feedback, or escalate the risk to a designated Risk Handler.

Risk Handler Check

At this stage the RH will liaise with the person raising the risk, and carry out a second quality check, this time on the actual content. S/he will then identify an appropriate RO and assist them to assess the risk.

Responsibilities: The DM is responsible for identifying the initial RH, who in turn is responsible for identifying the initial RO.

Risk Assessment

At this stage the RO, working with the RH will assess the inherent risk in terms of likelihood and impact as described previously. The control environment will be considered before determining the residual risk score. The risk decision (see below) is taken next and if applicable a target risk score is set together with an action plan of how to get there.

Responsibilities: Although the RH will assist, responsibility for assessing the risk, risk decision making and action planning rest with the RO.

Risk Register

This is the final part of the process, in which the risk appears on the appropriate risk register in order that it can be managed at the appropriate level[4].

Responsibilities: Production and circulation of risk registers is considered on p16.

Ongoing Risk Management

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

In part 1, the risk owner will already have decided on the required risk treatment. The decision made will then inform the next actions required.

Terminate

The decision to terminate an activity which leads to a risk may be a very simple or very complex one. The RO will need to consider this carefully and if necessary develop an action plan to terminate the activity.

Transfer

As previously mentioned, the transfer of risk is a specialist area which managers are unlikely to need to consider. If the issue does arise however, advice should be sought from the Chief Risk Officer in the first instance.

[4] For more detail on risk registers please see p15

Tolerate

If the risk is to be tolerated, this means that Public Health Wales will take no further action to mitigate the risk beyond anything already being done. The risk will remain open in Datix, and the RO will be responsible for monitoring the risk and the control environment and ensuring that nothing has changed which would require a re-appraisal of the risk.

Treat

If the risk is to be treated, then the RO is responsible for developing an action plan. Any actions planned must have the intended outcome that it will have a positive impact upon the control environment i.e. it will add an effective control.

All risks have a cause and that is the element of the risk which needs to be controlled, so more often than not any added controls should act upon the cause of the risk to reduce the likelihood of it occurring. Occasionally a control may be implemented which will reduce the impact of a risk, although this is uncommon.

The RO is responsible for ensuring that the action plan is entered in Datix in order that it can be properly monitored and tracked.

The RO is then accountable to their manager for the delivery of the action plan.

Escalation

Another form of treatment is to escalate a risk to the next higher level. As previously stated, to be effective, risk needs to be managed at the lowest appropriate level. The RO will only escalate a risk when they either have concerns about their capacity or authority to manage it, or they do not have the resources (e.g. budget, staff etc) to manage it[5].

Not having the 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.

In the event of a requirement to escalate a risk, the RO will complete the Risk Escalation form[6] and ensure that it is signed off by the relevant people before being uploaded onto Datix to provide the audit trail for the decision.

---

[5] See Appendix C

[6] See Appendix D

Once agreed the risk will be moved to the appropriate new level in Datix by the DM.

De-escalation

This is the reverse of escalation and the process to be followed is the same.

Escalation and de-escalation of risks should not be done in isolation and consultation should be made with managers at all levels prior to final decision making.

Removal

Risks should not be removed from the system until such time as the risk has been completely eliminated. Risks may reduce in their importance over time, and so may be de-escalated down to an appropriate level of management. However removal of a risk completely from the system should be approached with care, as it is easy to expose the organisation by doing so. Anyone considering removal of a risk from the system should seek advice from the Chief Risk Officer.

Use of Datix

Use of the Datix platform is covered in a series of user guides which are available through the Datix interface. Anyone requiring further information or specific training is advised to contact the Datix Manager.

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 who need 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 4 – Risk Registers

Description of risk registers

Public Health Wales uses the Datix platform for the recording and tracking of risks and associated actions. The system is fully auditable and traceable to establish who has carried out what actions on any given risk at any point in time. However there is a need to have a clear visual summary at a variety of levels to enable risks to be reviewed, discussed and managed at the appropriate management meetings. This is done with a series of risk registers.

It is important to remember however that risk registers do not manage risk. Risk registers are simply a 'snap-shot' of the risk information contained in Datix at any given moment in time. The information contained in a risk register is therefore only as good as the information entered into Datix.

Risk registers are created as Excel spreadsheets and Risk handlers receive training in how to download risk registers from Datix and convert them into the standard corporate spreadsheet template for use in meetings.

It is essential that updates to risks and associated actions are entered directly onto Datix and not the spreadsheets themselves.

Use of risk registers as a management tool

Risk registers can be created for a wide variety of applications, such as meetings of management teams and project boards, covering certain categories of risks and so on. However the production of certain risk registers are now a mandatory element of the risk management system and these are as follows:

- Corporate Risk Register
- Directorate Risk Registers
- Divisional Risk Registers
- Health and Safety Risk Register*
- Information Governance Risk Register*
- Business Continuity Risk Register*

*These registers will only contain the organisation wide risks for the relevant subjects. Local risks will continue to be managed through Directorate or Divisional Risk Registers.

Anyone requiring a risk register to be created for an application not listed above should contact the Datix Manager.

All Risk Registers are then allocated a Senior Responsible Owner (SRO) and are used as management tools as follows:

Corporate Risk Register

This will be a standing agenda item in the monthly Business Executive Team meetings and the register will be presented each month by the Chief Risk Officer. Updates to the risks on this register must be made by no later than 6 working days prior to the meeting. The Chief Risk Officer will then be responsible for ensuring that copies of the register are circulated with meeting papers.

Additionally, at each meeting the Executive Team will receive a report on Directorate Risk Registers on a rotational basis. Referred to as a 'deep dive' exercise, this will allow the Executive to scrutinise and challenge the risks on a Directorate level. Directorate Risk Registers (which will include the H&S, BC and IG Risk Registers) will be received at Executive meetings no less than twice per year on a cycle to be agreed by the Executive Team.

SRO - Chief Executive.

Directorate Risk Register

This will be a standing agenda item in the monthly Directorate meetings. The production and circulation of the register will be a matter for determination by the Chair in liaison with one of the Directorate RHs.

Additionally, there will be a need for the Directorate Senior Management Team (SMT) to a report on Divisional Risk Registers on a rotational basis. Referred to as a 'deep dive' exercise, this will allow the SMT to scrutinise and challenge the risks on a Divisional level. The frequency of these exercises will be a matter for determination by the relevant Director and will depend on the risks carried by each division.

SRO – the relevant Executive Director.

Divisional Risk Register

This will be discussed in appropriate divisional meetings. The production and circulation of the register will be a matter for determination by the Chair in liaison with one of the Directorate RHs.

SRO - relevant Divisional Director.

Health and Safety Risk Register

This will be discussed in the Health and Safety Group meetings. It is important to note that this will contain only those organisation wide Health and Safety risks which cannot be managed at a local level. The production and circulation of the register will be a matter for determination by the Chair of the Group.

SRO – Deputy Chief Executive

Information Governance Risk Register

This will be discussed in the Information Governance Working Group meetings. It is important to note that this will contain only those organisation wide Information Governance risks which cannot be managed at a local level. The production and circulation of the register will be a matter for determination by the Chair of the Group.

SRO – Executive Director Quality, Nursing and Allied Healthcare Professionals

Business Continuity Risk Register

This will be discussed in the Business Continuity Group meetings. It is important to note that this will contain only those organisation wide Business Continuity risks which cannot be managed at a local level. The production and circulation of the register will be a matter for determination by the Chair of the Group.

SRO – Deputy Chief Executive

N.B. It must be remembered that once downloaded or printed a risk register is uncontrolled and so may not reflect the latest position in Datix. It is essential that before being used, any risk register needs to be checked to ensure that it contains the most up to date information in Datix.

It is recommended that risk registers are downloaded or printed for a specific purpose (e.g. a management meeting or discussion) and then destroyed, in order to avoid the danger of using out of date information.

Risk Registers and Board Committees

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.

Board Assurance Framework

One of the principle assurance tools for the Board is the Board Assurance Framework (BAF).

The BAF is very similar in appearance to a risk register but relates to strategic risks i.e. risks which could threaten the organisation's ability to meet its strategic objectives. It also contains much greater detail on controls and assurances so that the Board can understand the assurances that it requires and where those assurances come from.

All strategic risks are assigned an Executive Director who will be responsible for managing the risk and providing the assurances required by the Board. The BAF is reviewed bi-monthly by the Executive Team at their Business meeting in readiness for formal Board meetings. The Executive Director must update the Board Assurance Framework no later than 6 working days prior to the Business Executive Team on a bi-monthly basis (i.e. in July, September, November, January and March)

The BAF is received at all formal Board meetings and the Audit and Governance Committee meetings, whilst relevant sections of it are received at all other committee meetings.

The Chief Risk Officer will provide the updated information to the Board Secretary and Head of Corporate Governance who is responsible for management of the BAF and for circulating it in line with Board and Committee requirements for papers.

SRO – Chief Executive

The Board role in operational risk registers

Whilst the Board does not manage operational risk, it is vital for the Board to be assured that operational risks are being effectively managed. In order to obtain this assurance, the Board will receive the Corporate Risk Register once every six months at a formal Board meeting for the purposes of scrutiny.

Board Committees

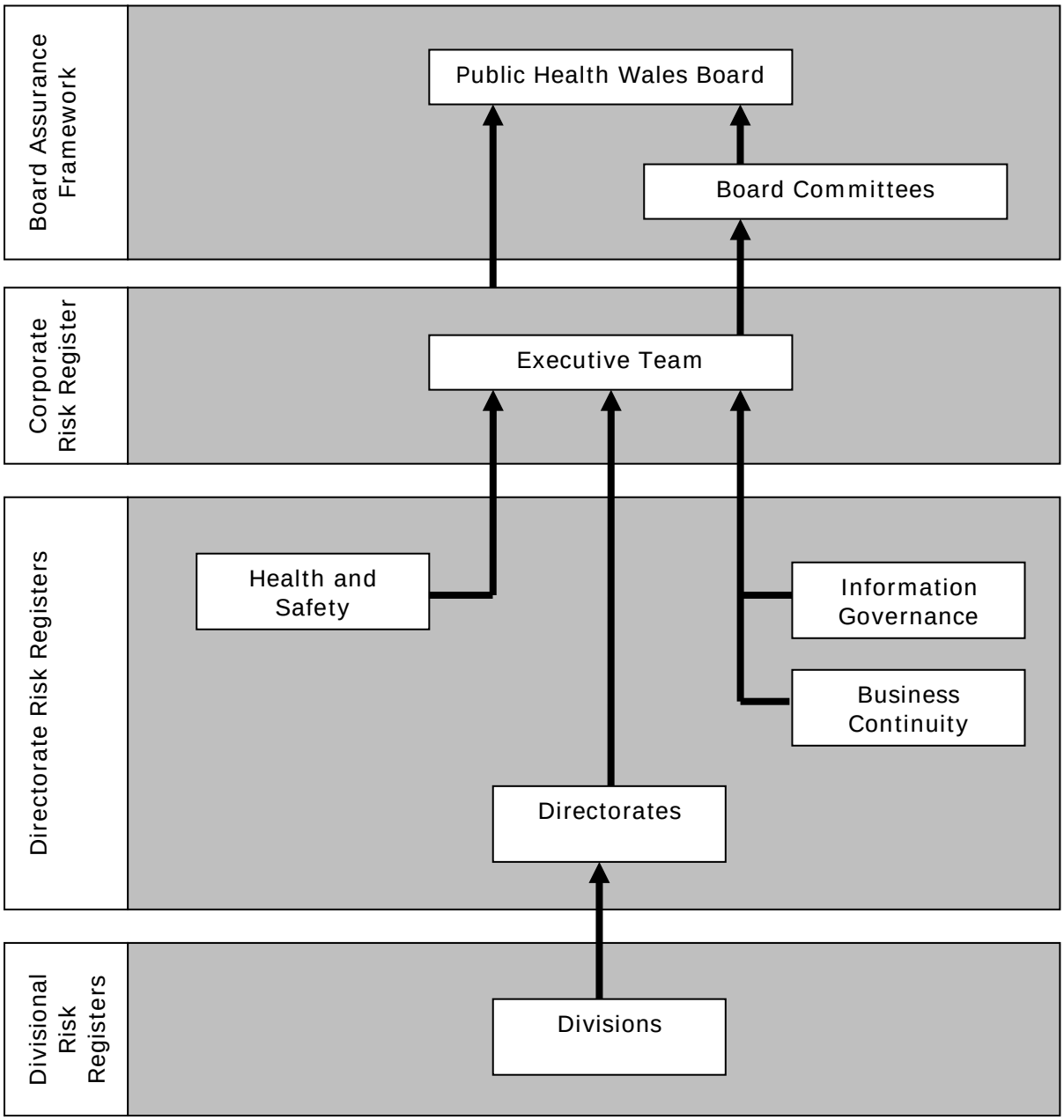
Additionally and for the same purpose, Board committees will receive the risk registers for their areas of interest as defined below, at their quarterly meetings together with relevant risks from the Corporate Risk Register. This will generally be confined to those risks, which are rated as being either high or extreme, but the risks to be presented will be at the discretion of the Chair of the relevant committee.

The Relevant registers and their Committees are:

Information Governance	-	Quality, Safety and Improvement
Health and Safety	-	People and Organisational Development
Business Continuity	-	Audit and Governance Committee

Appendix A – Risk Architecture

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



Appendix B – Risk Scoring Matrix

On its organisational Risk Registers Public Health Wales considers three risk 'scores':

Inherent Risk – This is the risk score without considering any of the controls in place. It is important to consider this 'raw' risk score so that the risk owner understands the implications if control measures are not effective enough or fail.

Residual Risk – This score is where the organisation is once existing controls have been taken into account. If this score is in accord with the statement of risk appetite then the risk should be tolerated and no further action should be required. If however the residual score is higher than that in the statement of risk appetite, then the risk must be treated and an action plan put in place to reach the target score. A residual score higher than a target score reflects the organisations risk tolerance.

Target Risk – This score reflects the organisations risk appetite. Target scores therefore must not be greater than those determined in the annual Statement of Risk Appetite.

Once the likelihood and impact in each case have been determined, the two are multiplied to generate the final risk severity score, which translates into one of four severity levels (as shown on the risk map below).

	Low Risk
	Moderate Risk
	High Risk
	Extreme Risk

Choose the most appropriate domain(s) for the identified risk from the left hand side of the table. Then work along the columns in same row to assess the scale of the impact on the scale of the impact. This will then show you the impact score of between 1 and 5. The descriptions are intended as a guide to assist your thinking and are not intended to be interpreted too literally or mathematically.

	Impact score and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Critical**
Safety of service users, staff or visitors	Superficial injury requiring first aid treatment. No sickness absence Not reportable No long term effects	Minor injury or illness requiring medical intervention Sickness absence up to 7 days Not reportable No permanent effects	Injury or illness resulting in hospital treatment as an in-patient Sickness absence up to 28 days RIDDOR/agency reportable incident Potential for long term effects	Injury or illness resulting in long term hospitalisation or long term effects Protracted sickness absence RIDDOR/agency reportable incident Life changing illness or injuries	Life threatening traumatic injury Potential ill-health retirement Reportable to Police Death of a service user, staff member or visitor
Quality	Single instance of suboptimal service No failure to meet Health and Care Standards 2015	Repeated instances of suboptimal service Single failure to meet Health and Care Standards 2015	Repeated failure to meet internal standards Repeated failures to meet Health and Care Standards 2015	Service delivery not fit for purpose Repeated major failures in the Quality Management System	Service delivery impossible / ceased Complete breakdown of Quality Management System
Staffing (availability of competent, trained staff)	No impact on staffing levels	Staffing levels impacted but no impact on service delivery	Staffing levels having major impact on service delivery	Staffing levels make service delivery unsafe	Staffing levels such that service delivery impossible

Legislative / Regulatory compliance	No breaches of legislation or regulatory requirements	Minor isolated breaches of legislation or regulatory requirements	Breaches of legislative / regulatory compliance requiring formal reporting to the relevant authority	External investigation resulting in formal notices from regulators	Criminal / penal sanctions for legislative breaches
Adverse publicity / reputation including Social Media (SM)	No media interest	Minor local media coverage	Extensive local media coverage including TV/Radio	National / professional media coverage	Extensive national / professional media coverage
	No WG interest	Informal enquiries from WG	Enquiries from WG Officials	WG Ministerial interest	Parliamentary questions tabled
	No social media traffic	Small amount of SM traffic	Noticeable increase in SM traffic requiring a response	Extensive SM traffic requiring additional resource to manage	Intense SM traffic outstripping our ability to manage it
	Potential for public concern	Elevated levels of complaints and concerns raised by public	Noticeable drop off in appointments from service users	Extensive cancellation of appointments or lack of bookings	Total loss of public confidence
Business objectives / projects	No impact on project	Project cost over-run	Significant cost over-run on project	Severe cost / time over run on project. Project delivery in jeopardy.	Failure of project
	No impact on delivery of objectives	Isolated instances of missing deadlines with objectives	Repeated missed deadlines, objective delivery in doubt	Significant additional resources required to deliver objective(s)	Failure to deliver objective(s)
Finance including claims	Insignificant or no financial loss	Loss of 5 per cent of budget	Loss of 10 per cent of budget	Loss of 15 per cent of budget	Loss of 20 per cent of budget
	Possibility of a claim remote	Claim less than £10,000	Claim(s) between £10,000 and £100,000	Claim(s) between £100,000 and £1 million	Claim(s) >£1 million
Service continuity	No impact on service delivery	Minor impact on service delivery managed locally	Major impact on service delivery requiring additional resources	Major impact on service delivery requiring major incident response	Failure of service delivery
Information Security	No impact on Information security	Data breach resulting in loss of personal data of <10 people	Data breach resulting in loss of personal data of <100 people	Data breach resulting in loss of personal data of <1000 people	Data breach resulting in loss of personal data of >1000 people

Likelihood score

In order to assess likelihood, you should consider amongst other things any historical evidence. Do not limit yourself to historical evidence from Public Health Wales as there may be relevant historical evidence from other sources. There will be cases however where no historical evidence exists, in which case the assessment is an entirely subjective one, based on the best information available at the time.

In order to have some degree of focus, consider the likelihood of an event occurring within the next 5 years.

Choose the most appropriate description of likelihood for the identified risk which will then give you the likelihood score above it of between 1 and 5.

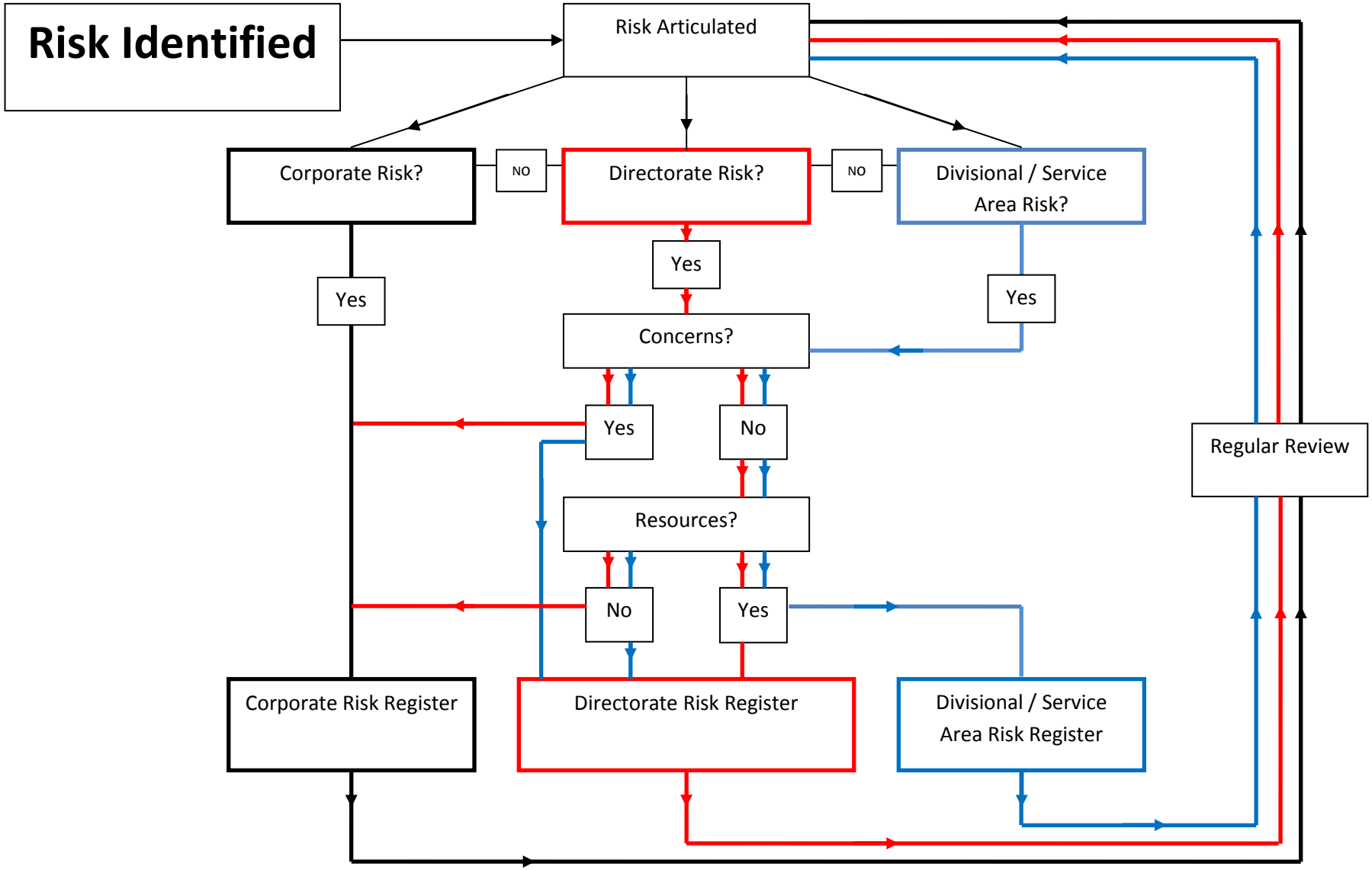
	Likelihood Score				
	1	**2**	**3**	**4**	**5**
Frequency	**Highly Unlikely**	**Unlikely**	**Likely**	**Highly Likely**	**Almost certain**
How often would you expect this event to occur within the next five years	No history, or very isolated historical examples. Almost certainly will not occur	Has occurred in the past but considered unlikely to occur again	Has occurred on numerous occasions in the past and / or other evidence exists to suggest that the likelihood exists that this will occur	Historical and / or other evidence suggests strong likelihood that this will occur	Significant historical and / or other evidence exists that suggests this will almost certainly occur

Risk Map

The risk map is where the two scores come together. The Impact and the likelihood are multiplied and the product of the two is the severity score. The severity score translates into one of four severity levels: low, moderate, high or extreme.

Impact							
	5	Critical	5	10	15	20	25
	4	Major	4	8	12	16	20
	3	Moderate	3	6	9	12	15
	2	Minor	2	4	6	8	10
	1	Negligible	1	2	3	4	5
			Rare	Unlikely	Likely	Highly Likely	Almost certain
			1	2	3	4	5
			Likelihood				

Appendix C – Risk Escalation map



Appendix D – Risk Escalation form

Datix Ref (ID number)	**Risk Description (as appears in Datix)**			
Current Risk Register	Corporate	Directorate	Divisional	Service Area
Current Risk Owner :			Position:	
Proposed Direction of travel	Escalate	De-escalate	Removal	
Proposed Risk Register	Corporate	Directorate	Divisional	Service Area
Rationale for recommendation				
Decision	Escalate	De-escalate	Removal	Retain
New Risk Owner :		Position:		
Meeting in which decision made:				
Signed:		Date:		
Name:		Position:		