GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** xxxx **Version Number:** 3.2.4 **Date of next review:** TBC

RISK MANAGEMENT PROCEDURE

Policy Statement

This procedure describes the process for the management of risk across the organisation and any hosted organisations. 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 closure/removal.

Risk management is an integral part of decision making and supports the longevity of the organisation(s) by reducing the potential for loss and capitalising on opportunities for the organisation to deliver it strategic objectives.

Policy Commitment

The purpose of the procedure is to set out the responsibilities for staff within the organisation(s) and support colleagues to be competent and capable in managing risks effectively.

Supporting Procedures and Written Control Documents

Risk Management Policy
Health and Safety Policy
Information Governance Policy
Putting Things Right Incident Reporting and Management Procedure

Scope

The procedure applies to all staff across the organisation(s).

Equality and Health Impact Assessment	Insert link to completed **Integrated Screening Tool**.
Approved by	Audit and Corporate Governance
Approval Date	TBC
Review Date	TBC
Date of Publication:	TBC
Group with authority to approve supporting procedures	Leadership Team

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 Corporate Governance.

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**
2	08/02/2018	TBC	TBC	Introduction of Risk Appetite model. Revised risk scoring matrix and indicators.
2.1	06/02/2020			Draft for comment
3.0	01/10/2020			Changes to reflect Strategic Risk Register, Split of Information Risk responsibilities and the current planning cycle.
3.1	29/11/2024			Full revision to reflect level of risk maturity.
3.2	19/02/2025			Revisions as a result of feedback from the Risk Assurance
3.2.1	03/03/2025			Revisions as a result of feedback from the BBU relating to the governance elements
3.2.2	18/03/2025			Revisions following review by the Head of Risk
3.2.3	17/07/2025			Revisions following formal consultation
3.2.4	18/09/2025			Revisions following review by Leadership Team

1. Contents

2. Introduction

Risk surrounds us in our everyday lives and we as people have evolved to deal with them as a matter of course. We accept and take risks every day of our lives so to prosper and grow. Organisations are no different. An organisation that is not prepared to take any risks whatsoever, will not survive very long. By the same token, an organisation which is reckless in the risks it takes will have a very bleak future.

For this reason, Public Health Wales and any hosted organisations have to assess both the internal and external environment in which they operate to establish any risks they face and manage these effectively enough to ensure that they don't prevent the achievement of their objectives. This is the discipline of risk management.

Risk is defined as 'the effect of uncertainty on objectives', in other words, something might happen which might have an effect on the organisation. This effect can be a positive outcome (opportunity risk) or a negative outcome (downside risk). If there is no uncertainty i.e. we know something is going to happen, is happening now or has already happened, this is not considered a risk and the management of these issues and events are not covered in this procedure.

Public Health Wales continues to develop its Risk Management Framework in line with the International Standard ISO31000 and adopts the Enterprise Risk Management framework to achieve this. The framework aims to give everyone in the organisation(s) the confidence and capabilities to understand their risk and control environments, understand what their responsibilities are and how to discharge them effectively.

By adopting the Enterprise Risk Management (ERM) framework, the organisation can define and manage its overall approach to risk and control at a corporate level. To achieve this, all identified risks must be documented and tracked using the Datix Web software. This system helps analyse risk data, identify patterns and trends, and ultimately informs the organisation's strategic risk decision.

3. Roles and Responsibilities

The following roles and responsibilities are set out as follows:

- Board – setting the risk appetite and signing of the Annual Statement of risk appetite. In addition, the Board approves the risk management strategy.
- Audit and Corporate Governance Committee – on an annual basis, receive a report outlining the internal system of control of risk and seek assurance that the system is effective and fit for purpose.
- All other Committees – as delegated by the Board, seek assurance that the strategic and corporate risk registers are being managed appropriately and provide a structured environment for appropriate challenge and scrutiny for all risks reported within its remit.
- Board Business Unit – ensures the Annual Governance Statement includes the system of internal control and establishes the Business Executive Team (BET), Committee and Board work plans to include strategic and corporate risk register.
- Chief Executive and Executive Directors – actively review and manage the strategic risk register as part of the Terms of Reference of the Business Executive Team.

- Leadership Team – actively review and manage the corporate risk register as the Business Executives Team delegated authority.
- Head of Risk Management – develops the risk management framework and is the corporate resource to maintain the strategic risk register.
- Risk Manager – provides operational support and expertise across the organisation(s) and is the corporate resource to maintain the corporate risk register.
- Specialist Leads/Groups – Provide specialist advise and support where risks relate to the subject in which they are expert. Where those risks are deemed to require being managed at a corporate level, the associated groups will take over the active management.
- Owners – responsible for the management of risks and escalation in accordance with the organisations risk appetite.
- Handlers – support the risk owner to ensure risk records are up to date, reports prepared and the timely submission of information.
- All colleagues - are responsible for raising and reporting any potential risks.

4. Definitions

Where required, each section of this procedure will provide a description of the element being covered, however some additional general terminology is described below.

Risk

Risk is defined as 'the effect of uncertainty on objectives', in other words, something might happen which might have an impact on the organisation. This impact can be a positive outcome (opportunity risk) or a negative outcome (downside risk).

Risk Cause

In Public Health Wales, we describe anything in the internal or external environment that has the potential to impact the organisation's ability to achieve its agreed objectives as the cause. These can be described as a hazard, threat, driver or opportunity. It is less important to distinguish the differences between these terms as long as we clearly describe the cause that exists.

Issues and Events (Incidents)

An issue or event (incident) is defined as a realised risk. If there is no uncertainty as to whether a risk will be realised, whether this be because we have not identified or managed a risk in a timely manner, it is already happening or has happened, these must be managed appropriately but are not covered by this procedure. Please refer to the Putting Things Right Incident Reporting and Management Procedure.

5. Risk Identification and Reporting

Risks can be identified at any time and by anybody. All colleagues have a responsibility to raise or report any potential risks they identify. In the first instance, it should be raised with their manager and except in cases of urgency, risks should be raised at the next appropriate meeting i.e. weekly Team meeting, in order to ensure the risk is a risk and has been articulated correctly. It then must be reported on Datix Web. All staff have permissions to report a risk on Datix Web and are

supported by relevant training. All staff are recommended to undertake Level 1 Risk Management Training. Further information and resources on this can be found on the Risk Management SharePoint site Risk Management Training and Guides.

6. Risk Statuses

Risks will go through a lifecycle until they are either realised (issue/event) or until they longer exist. The following stages have been incorporated into Datix.

New Risk
A risk has been identified and reported on Datix Web. A review is undertaken by the risk manager (or member of the NHSWPI Corporate Governance team in relation to risks related to NHSWPI) to ensure that the risk is indeed a risk, the Datix Web system has worked as expected, the risk along with any controls and mitigations are articulated sufficiently to progress to the initial assessment stage. The risk is then moved into the 'initial assessment required' status.

Holding, awaiting additional information
This is a holding status should the corporate review be unable to be completed as it requires additional information from the reporter. Once this additional information is received, the Risk Team will move the risk into the 'initial assessment required' status.

Initial assessment required
This is the stage where Directorates/Divisions/Team table the risk at their next scheduled Directorate or Divisional meeting, in order to carry out the following:

- Updating the description, cause and impact should it require additional articulation.
- Confirm the inherent score is appropriate.
- Assign a risk handler and owner.
- Confirm the controls and mitigations are appropriate and enter any additional that have been identified.
- Ascertain the residual and target score.
- Assign a risk register and risk decision.
- Identify actions.
- Indicate the next review date.
- Move the risk into the 'live management' status.

Live Management
This is the stage where the group responsible for risks assigned to a risk register i.e. Monthly Divisional meetings responsible for the management of risks on the Divisional Risk Register will continually review and progress the active management of the risk. Each time a risk is review, the Datix record should (but not limited to) update:

- Review and update the residual score.
- Review and update the controls and mitigations.
- Review and update the action plan.
- Escalate and Deescalate risks as appropriate (see section 20).
- Indicate the review date and assigned the next review date.

- Provide a summary of the outcome of the review in the review tab.
- Add any suitable documentation relating to the management of the risk.

Closed
This is the stage the risk no longer exists or is deemed low enough to no longer need active management. The following actions need to be carried out in the Datix Web record:

- Review and update the residual score.
- Review and update the controls and mitigations.
- Update and close down all outstanding actions.
- Indicate the review date.
- Provide a summary of the outcome of the review in the review tab and rationale for closure.
- Change the status to closed and enter a closed date.

Rejected
Where an issue, event (incident) or duplicate risk has been reported, the risk record will be assigned to the rejected status with a rationale as to why this decision has been made. This is carried out by the Risk Manager in collaboration with the risk reporter.

7. Risk Articulation

In Public Health Wales, a risk is split into three elements, it describes what might happen (description), why it might happen (cause) and if it did happen what the outcome might be (impact).

Risk Description
Clearly describe in plain language the positive or negative outcome that might happen in the future. If you cannot start the risk description with the words 'there is a risk that…' then you probably don't have a risk, you have an issue or event. 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. Conversely in articulating the 'some good' it is important to describe what the outcome might be should the organisation take the opportunity risk.

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

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. It is rare that only one impact might be realised as such it is important to consider the impact holistically i.e. reputational damage, financial implications, harm to service users and so on. Please refer to section 24 for examples of the various domains that might be impacted.

8. Risk Scoring

Once a risk has been appropriately articulated, an overall score is indicated. The purpose of scoring a risk is to provide a snapshot into how significant or insignificant a risk is considered, to enable the organisation to identify those 'uncertainties that matter' to allocate resources to manage the risks appropriately.

The risk score considers two factors, the likelihood and the impact. Public Health Wales utilises a common form of risk scoring referred to as a 5x5 risk matrix as demonstrated below. The likelihood and the impact are assessed on a scale of 1 to 5, with the two scores are multiplied to arrive at the final risk score (between 1 and 25 with 1 being the lowest).

	Consequence (current)				
Likelihood (current)	**1 Negligible**	**2 Minor**	**3 Moderate**	**4 Major**	**5 Critical**
5 Almost certain					
4 Highly Likely					
3 Likely					
2 Unlikely					
1 Highly Unlikely					

Scoring is a very subjective process which is why it is important to consider risks with appropriate colleagues to come to a consensus building upon each individuals own view, experiences and knowledge. In addition, examples on what different likelihoods and impacts would look like is provided in section 24. 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.

Inherent Risk

This is the risk when it is first identified, considered without taking account of any controls or mitigations. 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 existing controls or mitigations taken into account. As a risk is managed and reviewed, the residual risk score should be updated to take into account any progress made. In the main, the objective is to reduce the residual risk to be lower than the inherent risk working positively towards achieving the target risk, however a change in the internal or external environment may result in the residual risk increasing and this should also be reflected. An important point is that the greater the difference between the inherent and residual scores, the greater the reliance on the control environment. Please refer to section 15 in relation to what constitutes strong and weak controls.

Target Risk

The target score of a risk reflects how much action is needed to bring the risk to a level that aligns with the organisation's risk appetite and tolerance, based on the nature (or theme)

of the risk. This helps ensure the organisation is comfortable accepting the risk while still working toward its objectives.

9. Risk Appetite

Risk appetite is defined as:

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

Strategic Risk Appetite

The risk appetite for the organisation is set on an annual basis by the Board, during the period when decisions are being made around the organisation's strategic priorities for the following year.

Board 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 Head of Risk Management 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 Head of Risk Management will ensure that the Annual Statement of Risk Appetite is communicated to all risk owners.

Operational Risk Appetite

In order for Risk Owners to reflect the appropriate appetite level to all risks, a framework is being developed and will be reflected in this procedure once approved by the Board.

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

Where risks are being tolerated outside the agreed risk appetite level, they should be escalated following the escalation process (please refer to section 20) through the appropriate governance routes. Escalation will enable Directorate Management Teams or Senior Leadership Team to consider and identify further controls and mitigations.

10. Risk Decision

Once the residual and target risk scores have been identified based on the organisations risk appetite, there are four options to indicate the risk treatment, 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 or robust controls and mitigations are in place that it is not anticipated that the risk might occur.

Transfer
This is where a third party, usually on the payment of a premium agrees to take on the risk on our 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 as there will still be elements of the risk that the organisation will still need to manage i.e. reputational risk. For any owners considering this risk decision, agreement will be required from the Risk Management Team.

Tolerate
This is where the risk has been assessed and the residual (current) risk score demonstrates that the risk has been managed appropriately to reach the target score and therefore sits within the 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 it has been 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.

In addition, where a risk is sat outside the risk appetite, consideration needs to be made as to whether it needs to be escalated should it be identified that the current owner is not in a position to address the risk to a tolerable level. Please refer to Section 20 in relation to the escalation process.

11. Risk Registers and Escalation

Risk Registers are assigned to demonstrate which responsible group (i.e. a Division) is taking ownership of the active management of a risk. In line with the Enterprise Risk Management framework, colleagues are supported to feel confident and capable to manage risks at the lowest level when the following conditions can be met:

- The responsible group has the capacity, authority and responsibility to manage the risk.
- The responsible group has the resources to manage the risk.
- The risk is expected to be managed before it becomes an issue/incident/complaint.
- The risk is primarily not required to be managed by the Infection, Prevention and Control or Safeguarding Groups.

- The residual risk is within the risk appetite and tolerance.

Should one or more of the conditions above be unable to be met, the risk must be escalated (please refer to section 20).

Risk Registers are simply a 'snapshot' of the risk information that is contained within Datix Web at any given moment in time. Risk Registers are created from an extract of applicable risks in Datix Web for the purpose of discussion. It is essential that updates to risks and associated actions are entered directly onto Datix Web and not the spreadsheets themselves. It is also vitally important that Directorate level and Divisional level risk registers are used to inform business agendas and most significant risks are discussed at the respective DMT/SMT meetings to ensure focus is placed in the most appropriate areas.

Risk Register Types

The following risk registers are currently in place:

- Corporate Risk Register
- Directorate Risk Registers
- Divisional Risk Register
- Programme Risk Register (related to projects)
- Project Risk Register
- Service Group/Programme Risk Register
- Infection, Prevention and Control Risk Register*
- Corporate Safeguarding Risk Register*

*The Infection, Prevention & Control, and Safeguarding risk registers contain organisational wide risks which are actively managed by the associated Group. Local risks will continue to be managed through Directorate, Divisional or Service Group/Programme Risk Registers.

Any additional risk registers that are required should be requested through the Risk Management Team.

Corporate Risk Register

The Corporate Risk Register is a standing agenda item at the Leadership Team meetings and the register is presented on a bimonthly basis by the Risk Manager. In addition, any risks that have been proposed to be escalated onto the Corporate Risk Register will be submitted for consideration. Updates by the risk Owner/Handler to the risks on this register and any proposed risks for escalation must be made by no later 14 days prior to the meeting.

Additionally, the Leadership Team will receive a report on Directorate Risk Registers on a rotational basis. Referred to as a 'deep dive' exercise, this will allow the Group to scrutinise and challenge the risks on a Directorate level.

The Senior Responsible Owner for the Corporate Risk Register is the Chief Executive. The last approved Corporate Risk Register from Leadership Team is received by the Business Executive Team prior to any Board or Committee meetings.

Directorate Risk Registers

Directorate Risk Registers are a standing agenda item in the monthly Directorate meetings. In addition, any risks that have been proposed to be escalated onto the Directorate Risk Register will be submitted for consideration The production and circulation of the register and any proposed risks for escalation will be a matter for determination by each respective Chair in liaison with one of the Directorate Risk Handlers.

Additionally, there will be a need for the Directorate Senior Management Teams to receive a report on Divisional Risk Registers on a rotational basis. Referred to as a 'deep dive' exercise, this will allow the Senior Management Team 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.

The Senior Responsible Owner for Directorate Risk Registers is the relevant Executive Director (or equivalent if job title differs).

Divisional Risk Register

Divisional Risk Registers are a standard agenda item in the appropriate divisional meetings. In addition, any risks that have been proposed to be escalated onto the Divisional Risk Register will be submitted for consideration The production and circulation of the register and any proposed risks for escalation will be a matter for determination by the Chair in liaison with one of the Division's Risk Handlers.

The Senior Responsible Owner for the Divisional Risk Registers is the relevant Divisional Director (or equivalent if job title differs).

Programme (related to projects) Risk Register

Programme Risk Registers are for any risks that relate to a group of projects that are managed as an overall programme. This should not be confused with the term used to describe a Screening Programme for example. They may or may not relate to projects or programmes that fall under the remit of the Portfolio Management Office. The risk registers are a standard agenda item in the appropriate Programme Board meetings with risks extracted from Datix Web and incorporated into the standard RAIDD log. The production and circulation of the register will be a matter for determination by the Chair in liaison with one of the Programme's Risk Handlers.

The Senior Responsible Owner for the Programme (related to projects) Risk Registers is the relevant Programme Manager (or equivalent if job title differs).

Project Risk Register

Project Risk Registers relate to any projects and may or may not fall under the remit of the Portfolio Management Office. The risk registers are a standard agenda item in the appropriate Project meetings with risks extracted from Datix Web and incorporated into the standard RAIDD log. The production and circulation of the register will be a matter for determination by the Chair in liaison with one of the Project's Risk Handlers.

The Senior Responsible Owner for the Project Risk Registers is the relevant Project Manager (or equivalent if job title differs).

Service Group/Programme Risk Register

Service Group/Programme Risk Registers are a standard agenda item in the appropriate team meetings. The production and circulation of the register will be a matter for determination by the Chair in liaison with one of the Team's Risk Handlers.

The Senior Responsible Owner for the Service Group/Screening Region Risk Registers is the relevant Head/Manager (or equivalent if job title differs).

Infection, Prevention and Control Risk Register

The Infection, Prevention and Control Risk Register is a standard agenda item on the Infection, Prevention and Control Group. It is important to note that this register will contain only those organisation wide risks which cannot be managed at a local level for active management, but the Group will also receive a report on any other related risks that sit at on a Directorate, Divisional or Service Group/Programme risk registers for information. The production and circulation of the register will be a matter for determination by the Chair of the Group.

The Senior Responsible Owner is the Executive Director or Nursing, Quality and Integrated Governance.

Corporate Safeguarding Risk Register

The Corporate Safeguarding Risk Register is a standard agenda item on the Safeguarding Group. It is important to note that this register will contain only those organisation wide risks which cannot be managed at a local level for active management, but the Group will also receive a report on any other related risks that sit at on a Directorate, Divisional or Service Group/Programme risk registers for information. The production and circulation of the register will be a matter for determination by the Chair of the Group.

The Senior Responsible Owner is the Executive Director or Nursing, Quality and Integrated Governance.

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 Web. 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 Web. 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.

12. Enablers Oversight

Some enablers within the organisation do not require standalone risk registers but require oversight of risks for information purposes. Datix Web has the ability to add a tag to enable sight of applicable risks. The following tags are currently in place:

- Programmes or Projects under the remit of the Portfolio Management Office
- Infection, Prevention and Control
- Safeguarding
- Health and Safety
- Information Governance

- Communications
- Medical Devices
- Medicine Management
- Data and Digital
- Welsh Language

Any additional tags that are required should be requested through the Risk Management Team.

13. Communication Responsibilities

There are few risks that are only applicable to one area of the organisation, as such it is important that relevant parties are identified and effectively engaged with in order to manage a risk well. Relevant parties can be any area/team that might be affected should a risk be realised, or their expertise or resources be required to effectively address a risk to an appropriate level. This might be other Directorates/Divisions or Enablers. One owner will take overall responsibility for a risk and will ensure that effective engagement takes place. It is incumbent on all members of staff that they actively engage and participate in the management of risks and if requested to accommodate cross-organisational working, then this should be prioritised.

14. Triangulation of Data, Links to Quality, Incident Management and Organisational Learning

In addition to the review of risk data, it is important to analyse data associated with incidents, concerns and service user experience to identify any themes or trends in order to identify quality improvement that can be made. This analysis should form part of the standard reporting as detailed in Section 11. The following considerations should be made in the data analysis:

- Are there incidents which may reoccur and as such would benefit from proactive management as a risk?
- Are there any risks/incidents/complaints occurring in certain areas of the organisation which may also be relevant to other areas?
- Is there evidence from the past that could be applicable to something we are planning to do in the future?
- Review of closed risks to consider how they were managed, did any incidents/complaints still occur after their closure?

The Nursing, Quality and Integrated Governance Directorate hold monthly Learning Group meetings in order to identify themes and trends at an organisational wide level. The Learning Group provide an array of specialist expertise specifically in relation to quality and organisational learning in order to provide evidence based and timely advice to areas of the organisation where improvements can be made.

15. Controls and Mitigations

The active management of risks requires controls and mitigations to be implemented in order to reduce an unacceptable risk to an acceptable level.

Controls aim to prevent an event from occurring therefore working to reduce the likelihood whereas mitigations aim to reduce the associated impact, therefore working to reduce the consequence.

In order for something to be considered a valid control or mitigation it must:

- Be having a positive influence on the risk.
- Relate to the risk in question.
- Already exist and be in place.
- The organisation must be in control of the control.

When identifying controls and mitigations, dependence on those which rely on humans to be effective should be avoided but rather those which do not rely on humans are the most robust and reliable. The following demonstrates the hierarchy of controls and mitigations:

Not reliant on humans

- Elimination.
- Substitution.
- Engineering controls.

Require humans to be effective

- Administrative controls.
- Personal Protective Equipment.

Where residual (current) risk score remains higher than the target risk score, strengthening or implementing additional controls and mitigations are required. Once identified, these are considered as 'gaps in controls and mitigations' until they can be implemented. They should form part of the action plan to address the risk, please see section 17 for further information on action plans.

16. Assurance

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.

Strategic Risk Framework

One of the principal assurance tools for the Board is the Strategic Risk Framework which is a key element of the wider Board Assurance Framework and the Strategic Risk Framework includes the Strategic Risk Register.

The Strategic Risk Register 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 Register is reviewed bi-monthly by the Executive Team at their Business meeting in readiness for formal Board meetings. The Executive Director must update the Strategic Risk Register no later than 10 working days prior to the Business Executive Team on a bi-monthly basis.

The Strategic Risk Register is received at formal Board meetings three times a year (as per the Board's work plan) and is reported to all of the Audit and Governance Committee meetings, whilst relevant sections of it are received at all other committee meetings. The Head of Risk will provide the updated information to the Board Business Unit who is responsible for circulation in line with Board and Committee requirements for papers.

The Senior Responsible Owner is the Chief Executive.

Corporate Governance and Effective Risk Management

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.

Committees

The Quality and Corporate Governance Committee will receive a quarterly Clinical Governance Report which may include the Infection, Prevention and Control Risk Register, the Corporate Safeguarding Risk Register and any risks that are deemed significant enough for the respective Committees to be made aware (risks relating to their remit).

17. Action Plan

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**pecific
- **M**easurable
- **A**chievable
- **R**elevant
- **T**imely

Not all actions, once completed become a control or mitigation. It is important to identify and record any other actions that support the active management or the risk. Some examples are

testing/auditing activities of the control environment, stakeholder engagement, assurance submissions and so forth.

18. Risk Ownership

For risk management to be 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 current responsible group.

Risk Owners

Whilst risks will be collectively reviewed and managed by a responsible group, one person needs to take responsibility for owning a risk and be accountable to their managers for it. This person is known as the Risk Owner. In the organisation(s), Risk Owners are usually Executive Directors, members of the Executive Team, or their direct reports. This is not exhaustive however, and the important point is that the Risk Owner needs to be in the right position and have sufficient seniority to be able to take responsibility for the risk in question. Risk Owners are supported by appropriate training.

Risk Handlers

Risk Handlers are suitably trained staff who are able to support Risk Owners with the administrative arrangements around the management of their risks. Risk Handler 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.

19. Review Frequency

The following frequency for reviewing risks are suggested:

Extreme Risks	Reviewed and progress on actions updated at least monthly.
High Risks	Reviewed and progress on actions updated at least every two months.
Moderate Risks	Reviewed and progress on actions updated at least every two months.
Low Risks	Reviewed and progress on actions updated at least every three months.

It is important to note that Risk Owners should ensure that any changes to the internal or external environment are reflected i.e. a low risk can increase due to a sudden change in the external environment and will require review, updating and risk score reflected.

NB: Once the operational risk appetite is approved and rolled out, this section will be updated to reflect.

20. Escalation and De-escalation

As detailed in Section 11, to be effective, risks should be managed at the lowest appropriate level. The Risk Architecture is shown in sections 23 and 24, which details the escalation and de-escalation structure.

Escalation

The Risk Owner will only escalate a risk when they either have concerns about their capacity or authority or do not have the resources (e.g. budget, staff etc) to manage it. 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 Risk Owner or Handler will indicate in the risk record on Datix Web, the register in which they propose to escalate onto and provide a rationale. The designated Risk Handler is responsible for extracting the relevant Risk Registers and submitting them to the appropriate group. Once these risks are reviewed and approved, the Risk Handler will update their status in Datix Web by assigning them to the agreed risk register.

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.

21. Risk Training

All colleagues are required to attend at the least, the lowest level training sessions, the various training level are set out as below:

Level 1

Applicable to all colleagues, provides an overview of the fundamentals of risk management including assessing the internal/external environment, definition of risk, risk articulation, inherent scoring, controls and a demonstration of the reporting form in Datix Web. This is provided by the Risk Manager.

Level 2

Applicable to those colleagues identified as being a Risk Owner or Handler. It covers the bow tie model, risk review stages, scoring, appetite, decision, registers & escalation, monitoring & reporting, assurance, effective risk champion and a demonstration of the management form in Datix Web. This is provided by the Risk Manager.

Level 3

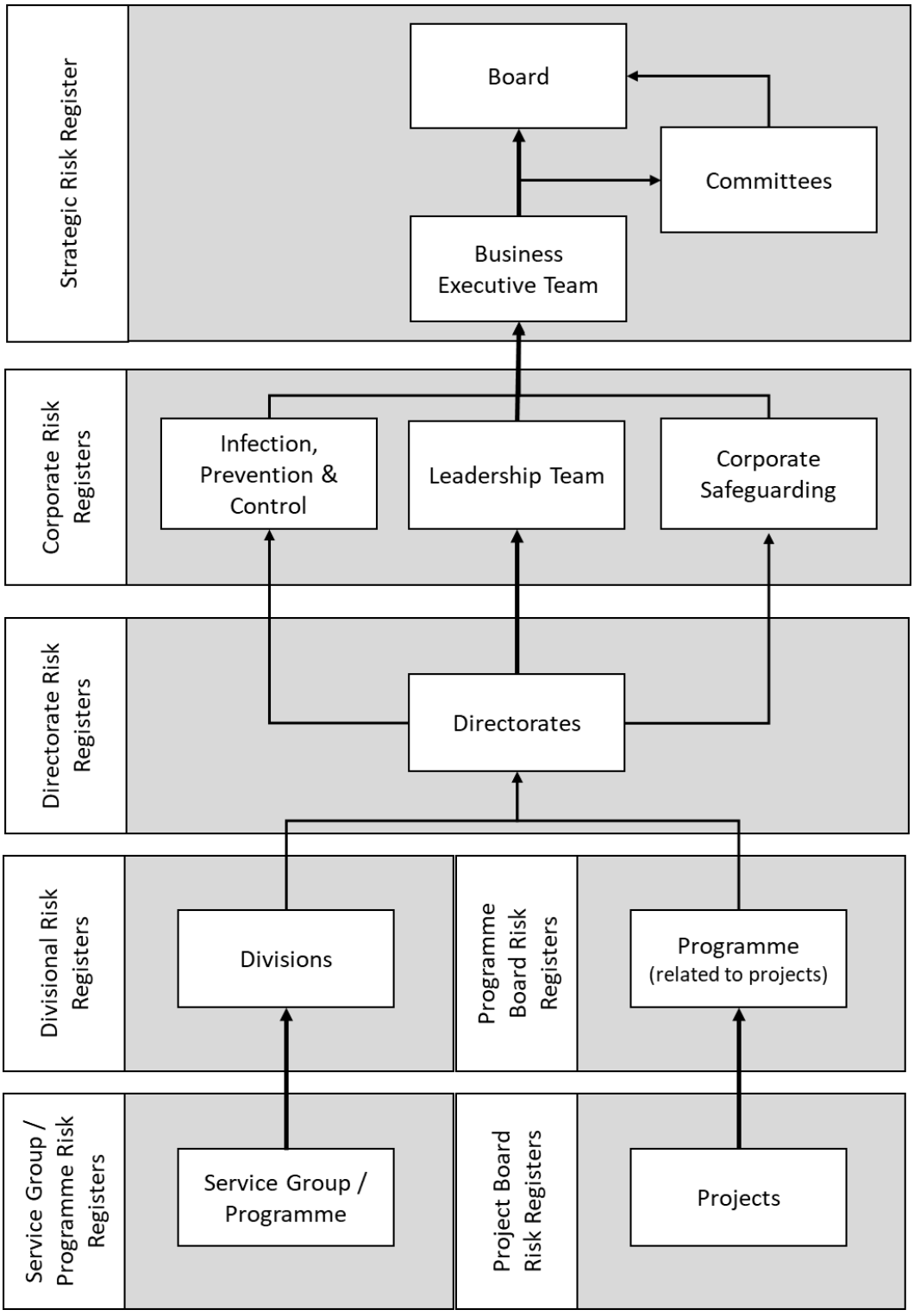
Applicable to the Executive Team, Board and Committee members. The Head of Risk Management provides bespoke training on risk appetite and strategic and corporate risk management.

Level 4

External accreditation of the Risk Team in qualification such as Certificate in Enterprise Risk Management.

22. Appendix 1 – Risk Architecture

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



23. Appendix 3 – Risk Scoring Matrix

To support colleagues in establishing the inherent, residual (current) and target risk score.

The following table provide some examples of the different types of impacts that might be associated with a risk if realised. Using the information provided as the potential impacts of a risk, work through the first column to identify any applicable types. Then work along the same row to assess the scale of the impact to identify which column best fits the risk in question to identify the score (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**
Impact Type	**Negligible**	**Minor**	**Moderate**	**Major**	**Critical**
Service User Safety and Wellbeing (Psychological/ Physical Harm)	No/Minimal injury not requiring intervention. No long term effects. Not RIDDOR/MHRA/IRMER reportable. Delay in appointment or processing of test result, no change in therapy and no impact to patient recovery	Minor injury or illness requiring minor intervention. No permanent effects. Not RIDDOR/MHRA/IRMER reportable. Delay in appointment or processing of test result, change in therapy resulting in minor impact to patient recovery	Moderate injury requiring professional intervention. RIDDOR/MHRA/IRMER reportable incident. Delay in appointment or processing of test result, change in therapy resulting in moderate impact to patient recovery	Injury or illness resulting in long term hospitalisation or long-term effects. Life changing illness or injury. RIDDOR/MHRA/IRMER reportable incident. Mismanagement of service user care resulting in long term effects.	Multiple permanent injuries or irreversible health effects or death. Reportable to Police, RIDDOR, MHRA or IRMER Mismanagement of service user care resulting in permanent health effects or death An event which impacts a large number of service users.

Health & Safety (Psychological/ Physical Harm)	Minimal injury requiring no or minimal intervention of 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 injury	Life threatening traumatic injury. Potential ill-health retirement. Reportable to Police. Death of a service user, staff member or visitor
Quality, Complaints & Assurance	Single episode of suboptimal service provided. No failure to comply with set standards appropriate to service. May result in service user feedback/early resolution.	Minor service suboptimal. Single failure to comply with set standards appropriate to service. Early resolution complaint (local resolution).	Moderate service suboptimal. Multiple failures to comply but not constitute a significant breach of standard appropriate to service and/or result in major service user/stakeholders safety implications if not acted upon. Early Resolution or formal complaint (local resolution possible)	Major service suboptimal. Critical non-compliance which constitute a significant breach of standard appropriate to service with loss of accreditation or loss of service delivery. Independent Review. Formal complaint and/or with consideration of Duty of Candour.	Catastrophic service failure. Criminal prosecution, financial loss, public inquiry, ombudsman, permanent (life changing) injury or death to a service user. Formal complaint and/or with consideration of Duty of Candour with legal implications.

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 or 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)	Low level negative social media. Potential for public concern.	Local media coverage. Short term reduction in public confidence/trust. Short term negative social media. Public expectations not met. Elevated levels of complaints and concerns raised by the public.	Extensive media coverage. Noticeable increase in social media traffic requiring a response. Noticeable drop off in appointments from service users. Long term reduction in public confidence.	Prolonged national/professional media coverage. Extensive social media traffic requiring additional resources to manage. Noticeable drop off in appointments from service users. Service well below reasonable public expectation. Long term reduction in public confidence.	Extensive national/professional media coverage. Senedd questions tabled. Intense social media traffic outstripping out ability to manage it. Total loss of public confidence.

Business objectives/ projects	No impact on project No impact on delivery of objectives	Project cost over-run Isolated instances of missing deadlines with objectives	Significant cost over-run on project Repeated missed deadlines, objective delivery in doubt	Severe cost / time over run on project. Project delivery in jeopardy. Significant additional resources required to deliver objective(s)	Failure of project Failure to deliver objective(s)
Financial stability and impact of claims *Full claim amount including that covered by Welsh Risk Pool	Insignificant or no loss. Possibility of a claim remote.	Loss equivalent to 0.1 to 0.25% of budget. Claims less than £10,0008	Loss equivalent to 0.25 to 0.5% of budget. Claim(s) between £10,000 and £100,000*	Uncertain delivery of key objective. Loss equivalent to 0.5 to 1% of budget. Claim(s) between £100,00 and £1 million*	Non delivery of key objective. Loss equivalent to >1% of budget. 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

To assess the likelihood of a risk being realised, you should consider amongst other things any historical evidence. Do not limit yourself to historical evidence from our organisation 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 (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

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 overall risk score. This 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
			Highly unlikely	Unlikely	Likely	Highly Likely	Almost certain
			1	2	3	4	5
			Likelihood				

24. Appendix 4 – Risk Status

The following flow chart demonstrates the lifecycle of a risk which is mapped to the risk status in Datix.