Estyn

Arolygiaeth Ei Fawrhydi dros Addysg a Hyfforddiant yng Nghymru
His Majesty's Inspectorate for Education and Training in Wales

Risk management policy and guidelines November 2023

Information sheet

Information box

For further advice contact: Head of Governance / Assistant Director Inspection and Central Services

Date of publication: November 2023

Planned review date: September 2025

Version control

Document version	Author	Date of issue	Key changes
1.0	Phil Sweeney	Oct 2009	
1.1	Phil Sweeney	Jan 2010	Reflect changes to Estyn management/group structure
1.2	Phil Sweeney	Dec 2010	Composite risk register
1.3	Phil Sweeney	April 2013	Risk ratings (matrix) and Tracking Report
1.4	Phil Sweeney	August 2015	Minor amendments
2.0	Phil Sweeney	August 2017	Added: risk control criticality levels and evaluation of and assurances on effectiveness of controls.
3.0	Phil Sweeney	November 2019	Added risk escalation route and minor changes from updated HM Treasury: Orange Book 2019
4.0	Phil Sweeney	November 2021(draft but not published)	Updates included from Orange Book and added risk appetite appendix
5.0	Cheryl Davies	November 2023	Updates included from: • Internal audit recommendations • other best practice guidance including HM Treasury: Orange Book 2021

Any enquiries or comments regarding this policy should be addressed to:
Estyn
Anchor Court
Keen Road
Cardiff
CF24 5JW or by email to enquiries@estyn.gov.wales

This and other Estyn publications are available on our website: www.estyn.gov.wales

Impact Assessment

An impact assessment has been carried out and this policy is not deemed to adversely impact on:

- any people on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation and the Welsh language
- the delivery of our strategic objectives and contribution to sustainability.

Contents

Section 1: Introduction

1.1 Risk management is an essential part of governance and leadership and is fundamental to how Estyn is directed, managed, and controlled at all levels. This risk management policy forms part of Estyn's internal control and Corporate governance framework – 2023 and provides a framework to identify, assess and manage potential risks and opportunities. It provides guidance for all staff within Estyn to make informed management decisions.

1.2 In trying to achieve our key objectives there are going to be threats and opportunities from both internal and external sources. By and large, evaluating and controlling risks effectively will ensure that opportunities are not lost and less management time is spent fire-fighting. This should increase our ability to meet our objectives efficiently.

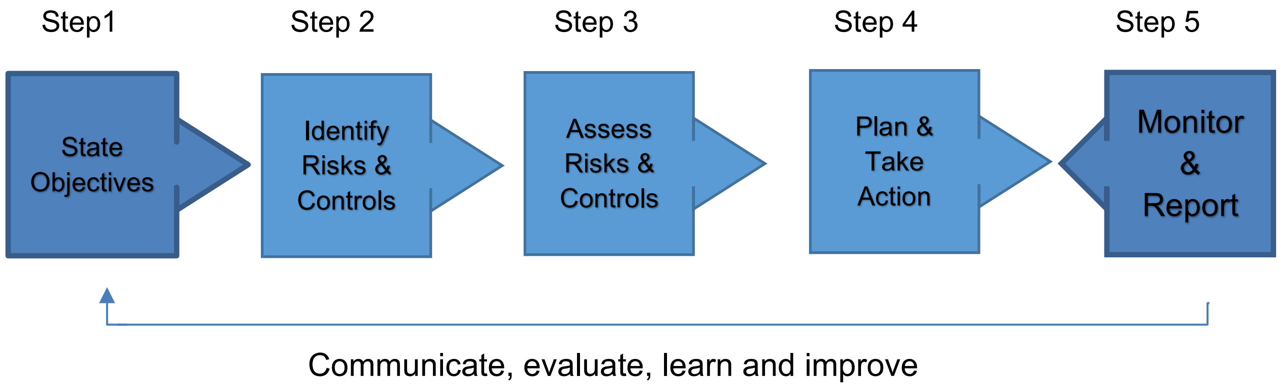
1.3 This policy has been approved by our Strategic Management Group, who will provide the necessary support and commitment to continue embedding risk management processes throughout the organisation.

1.4 Risk management shall be collaborative and informed by the best available information and expertise. To ensure a widespread understanding, all our staff should be aware of, and comply with, the principles set out in this document.

1.5 The risk management policy explains our underlying approach to risk management and includes:

- the purpose of our risk management arrangements
- risk management principles
- relevant responsibilities
- risk tolerance and risk appetite
- the risk framework and how it will work
- how risk management contributes to providing assurance

1.6 The risk management policy is based on a common set of definitions of risk management; these definitions are to be found in Appendix 1. A guide to completing the strategic and corporate risk registers is provided in Appendix 3.



Section 2: The purpose and context of Estyn's risk management arrangements

2.1 Daily we manage risk without necessarily describing this as 'risk management'. We consider what might go wrong and take steps to reduce the impact if things do go wrong. However, we cannot rely on informal processes alone. Also, as a public body, we must provide assurance to Estyn's Accounting Officer, auditors, Audit and Risk Assurance Committee and stakeholders that we are managing risk appropriately. We therefore need to identify key risks and mitigating actions formally.

2.2 Risk needs to be considered whenever key decisions are made. In particular, when objectives and activities are developed during the annual planning round, directors need to consider afresh the strategic and corporate risks in relation to what we intend to do over the forthcoming year.

2.3 Section 6 sets out our risk management framework that includes a principal strategic risk register and a corporate risk register, and appropriate risk registers for key projects.

2.4 Individual managers may also identify risks to their particular service areas and team activities. Mitigating actions/controls may be detailed within desk instructions, business plans, and/or be included in risk registers. Risks that are identified as potentially requiring a corporate action/control should be discussed with an appropriate member of the Operational Group / Inspection Leadership Group .

2.5 Our risk management arrangements should:

- improve business performance by informing and improving decision-making and planning
- promote a more innovative, less risk averse culture in which the taking of calculated risks in pursuit of opportunities to benefit the organisation is encouraged
- provide a sound basis for integrating risk management into our day-to-day decision-making rather than seeing risk management as a separate component of our business function
- form a component of good corporate governance and the internal control procedures on which the Accounting Officer annually comments within the Governance Statement as part of Estyn's resource accounts

2.6 The benefits that our risk management arrangements should provide include:

- an increased likelihood of achieving the organisation's aims, objectives and priorities
- prioritised allocation of resources
- early warning of potential problems
- greater confidence among staff about taking controlled risks
- protection and enhancement of the reputation and standing of the organisation through visible and appropriate stewardship

Section 3: Risk management principles

3.1 The principles contained in this policy will be applied by all managers within Estyn.

3.2 The risk management policy applies to all aspects of our work, both internal and external. It will also be used to consider strategic external risks arising from or relating to our partners in the Welsh Government and other organisations.

3.3 We will not only look at the risk of things going wrong, but also the impact of not taking opportunities or not capitalising on corporate strengths.

3.4 All risk management activity will be aligned to corporate aims, objectives and organisational priorities.

3.5 Risk-analysis will form part of strategic and operational planning processes, including business planning/cases and options/project appraisal and management procedures.

3.6 Risk management will be founded on a risk-based approach to internal control that is embedded in day-to-day operations of the organisation.

3.7 Our risk management approach will inform and direct our work to gain assurance about the reliability of our organisational systems and procedures. It will become one of the key means by which our Strategy Board gains its direct assurance.

3.8 Staff at all levels in Estyn will have a responsibility to identify, evaluate and manage or report risks, and will be equipped to do so.

3.9 Risk management shall be continually improved through learning and experience. As part of our culture of training and development, we will spread the lessons learned and expertise acquired from our risk management activities across the organisation.

3.10 When undertaking performance appraisals and staff development reviews, managers will include explicit reference to risk management roles and responsibilities.

3.11 Risk management processes shall be structured and proactive. Strategic, corporate and operational risks will be identified, objectively assessed, actively monitored, managed and reported.

3.12 The aim is to anticipate, and, where possible, avoid unacceptable risks rather than to have to deal with their consequences. However, for some key areas where the likelihood of a risk occurring is relatively small but the impact on the organisation could be severe, we may cover that risk by developing contingency plans, e.g. our business continuity plans. This will allow us to contain the negative effect of events that are unlikely but would be serious if they did occur.

3.13 In responding to any risk, the cost of mitigation and control actions, and the impact of risks occurring will be balanced against the benefits of reducing risk. This means that we will not necessarily set up and monitor controls to counter risks where the cost and effort are disproportionate to the impact or expected benefits.

3.14 We also recognise that some risks can be managed by transferring them to a third party, for example by contracting-out some of our work and putting in place agreements as to quality and standards.

Section 4: Responsibilities

4.1 Responsibility for identifying and managing risks will be a routine part of the role of management at all levels with risks being managed at the lowest level at which the manager has the authority, responsibility and resources to take action. All managers will be responsible for encouraging openness and honesty in the reporting and escalation of risks and in securing good risk management practice within the organisation.

4.2 All personnel have a responsibility for maintaining good internal control and managing risk in order to achieve personal, team and corporate objectives. All staff need the appropriate knowledge, skills, information, and authority to establish, operate and monitor the system of internal control. This requires an understanding of:

- Estyn and its objectives
- the risks staff are empowered to take
- the risks that should be avoided
- the risks that should be reported upwards

4.3 Specific risk management responsibilities of the Strategy Board, Strategic Management Group, the Operational Group / Inspection Leadership Group , working group/remit/project leaders and the Audit and Risk Assurance Committee are set out in Appendix 2.

Section 5: Risk tolerance and risk appetite

5.1 'Risk appetite' is the level of risk which an organisation **aims** to operate. It can vary over time and from work area to work area. The Strategic Management Group encourages the taking of controlled risks, the grasping of new opportunities and the use of innovative approaches to achieve our objectives provided the resultant exposure to risk is within our risk tolerance range. The Strategic Management Group should therefore, when considering risk, discuss the appetite for risk as they see it.

5.2 To deliver our objectives we need to balance opportunities to innovate and improve with our responsibilities in terms of accountability, propriety, regularity and value for money. The level of risk that is acceptable may vary on a case-by-case basis depending on the perceived benefits of the issue being considered. For example, we may be prepared to accept a higher risk in relation to a project that would be likely to offer major potential benefits for the education and training sector in Wales compared to one with similar risks but where the benefits are more tenuous or more limited. The Strategy Board will keep a watching brief to maintain a consistent approach and make sure that risk appetite for all key strategic risks is duly considered.

5.3 Appendix 5 provides a useful framework to use when considering the level of risk we are prepared to accept.

Acceptable risk areas

5.4 We should be willing and able to take calculated risks to achieve objectives. The associated risks of proposed actions and decisions should be properly identified, evaluated and managed to ensure that the extent of risk exposure is acceptable in relation to the expected benefits.

5.5 Particular care is needed in taking any action which could:

- impact aversely on Estyn's reputation
- undermine our independent and objective reviews
- result in censure of any kind or breach any code of conduct or affect any statutory obligation that applies
- result in financial loss, poor value for money, inappropriate use of public funds or any breach of regularity and propriety

5.6 Any threat or opportunity that has a sizeable potential impact on any of the above should be examined, defined, and discussed with the appropriate line manager, board or group to clarify and agree the risk appetite.

Prohibited Risk Areas

5.7 Organisational policies and guidance define where there are mandatory processes and procedures, e.g., the frameworks for inspection, Government Financial Reporting Manual, and our own terms and conditions of service, etc. All staff must comply with the standards as they apply to their roles. The Accounting Officer's annual Governance Statement will record our compliance with these standards.

5.8 Non-compliance with prescribed procedures therefore constitutes an unacceptable risk.

Section 6: Risk Framework

6.1 A Strategic and Corporate Risk Register will be maintained by the Secretariat team. .

6.2 The Strategic Management Group will maintain and monitor a current strategic risk profile. The Operational Group / Inspection Leadership Group will maintain and monitor a current corporate risk profile.

6.3 To help meet their responsibilities to identify, evaluate and manage operational risks, project managers for key projects will maintain their own project-related risk registers.

6.4 Branch Heads and Assistant Directors will oversee the maintenance and monitoring of operational risks for the enabling business / inspection areas. Team or group meetings can be used to discuss the management of risks however staff are required to report key risks to management as and when they arise. Risks that are identified as potentially requiring a corporate action/control , in spite of mitigating/control actions, will be reported to and reviewed by the relevant Operational Group / Inspection Leadership Group . Operational risks will be directly managed within each functional / inspection area – with risks and control actions being identified and recorded according to usual desk instructions, frameworks, performance standards,and operational procedures.

6.5 The risk management process is a dynamic and ongoing one. We will ensure that the process allows for regular periodic review of risks and for the consequent adjustment of the control response. The monitoring and review process should determine whether:

- the measures adopted have resulted in what was intended
- the procedures adopted and information gathered for understanding the assessment were appropriate
- better information would have helped us to reach better decisions and this will identify what lessons can be learned for future assessment and management of risks

6.6 Risk registers will include detail of the Impact and Probability (likelihood) of each of the risks identified, indicate Ownership/Responsibility (at an individual level) and specify actions being taken in order to manage the risk. Each risk register will be reviewed at least quarterly and will be fully updated annually. Evidence of risk reviews will be recorded in the minutes of relevant meetings and within the relevant risk register.

6.7 The progress of the risk management programme will be a standing agenda item discussed at quarterly meetings of both the Strategic Management Group, and Operational Group / Inspection Leadership Group, with one quarterly meeting used to undertake an annual review of the whole risk profile and formally review the effectiveness of risk control actions. Each financial year the Audit and Risk Assurance Committee will seek assurances and be required to confirm that they are content with Estyn’s risk management processes.

6.8 **Appendix 3** provides a practical step-by-step guide for completing the strategic and corporate risk registers. Project managers may also wish to use this format.

Risk escalation

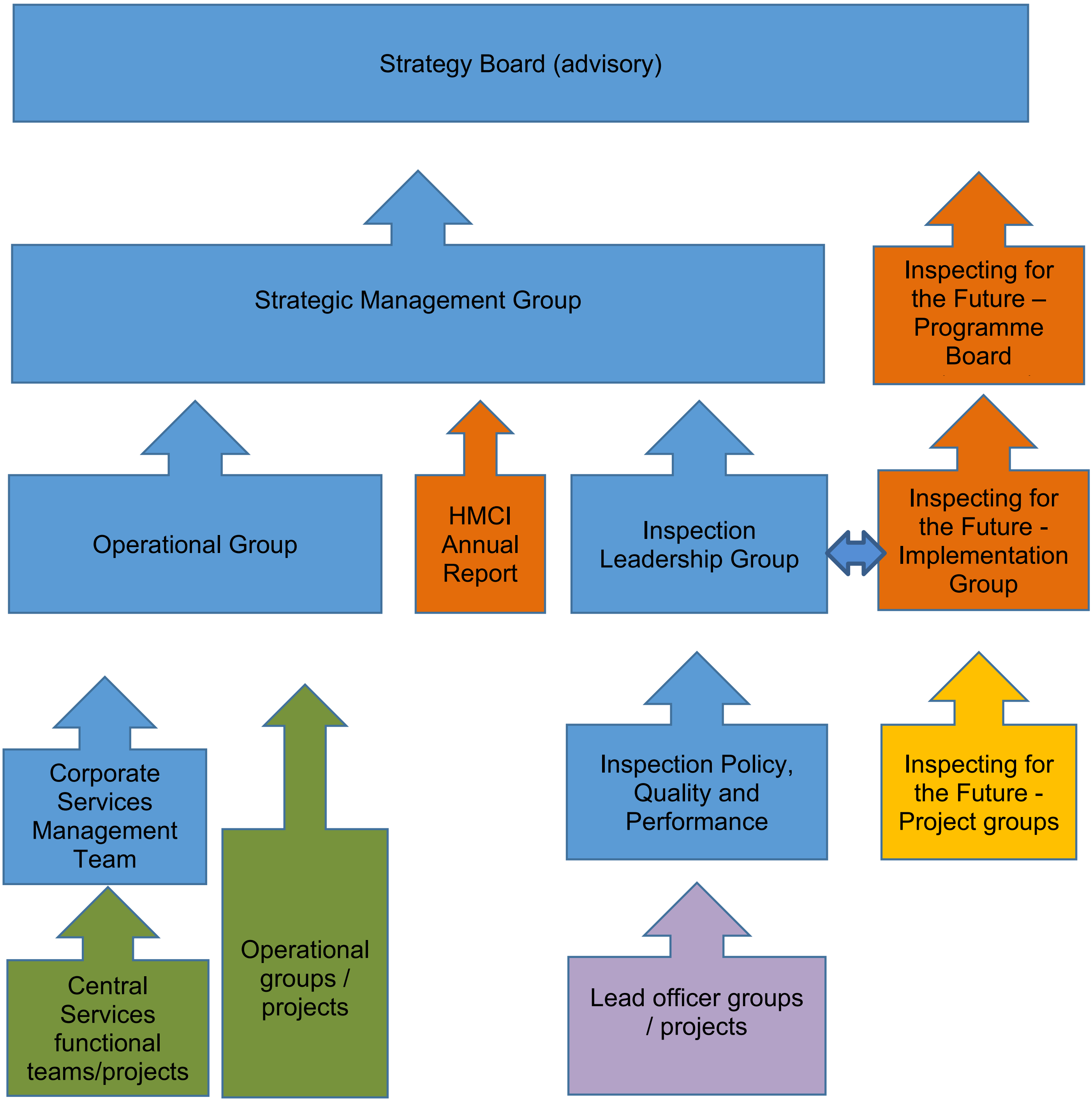
6.9 Risk should be managed at the most appropriate level to achieve effective mitigation/control and robust contingency planning. If risk cannot be managed at the level to which responsibility has been assigned, risk owners and/or managers at the current level should consider whether it is appropriate to escalate responsibility for ownership and management of a risk to a higher management level.

6.10 When escalated to a new level there must be an objective review process. This should include consideration of whether the risk is within the remit or area of effective control of the new level of management and is correctly assessed in terms of inherent and residual risk severity.

6.11 When a function/group agrees that a risk should be escalated this decision should be formally noted and reported to the higher level management group for consideration and agreement and, if agreed, management of that risk will thereafter be reported through the higher level risk register. Examples of potential trigger points for risks requiring escalation include:

- risks outside of the control of individual project/operational/functional managers (or that are not felt to be effectively managed at the current level of responsibility)
- risks with a wider impact than that on a specific project, area or function
- risks that will have a significant impact on key strategic objectives, business, processes, operational activities or the implementation of a change programme
- cross cutting dependencies, inter-relationships and resource conflicts
- significant risks with apparently inadequate mitigation measures/inadequate control measures
- systems or technology risks that may have a significant impact on service continuity

Escalation route for team/group/project risks



Strategy Board (advisory)

Strategic Management Group

Inspecting for the Future – Programme Board

Operational Group

HMCI Annual Report

Inspection Leadership Group

Inspecting for the Future - Implementation Group

Corporate Services Management Team

Operational groups / projects

Inspection Policy, Quality and Performance

Inspecting for the Future - Project groups

Central Services functional teams/projects

Lead officer groups / projects

Section 7: Assurance

7.1 The use of the risk management approach as outlined in this policy should help to identify aspects for detailed review within groups and inform and support Estyn’s annual Governance Statement.

7.2 A key to managing risk effectively is to ensure that risk controls are effective; the control or mitigation may not actually be effective or properly executed. All risk owners are responsible for periodically reviewing the effectiveness of risk control actions. For members of the Strategic Management Group, and the Operational Group / Inspection Leadership Group, the effectiveness reviews will be formally recorded and noted within Director /Assistant Director Annual Assurance Statements.

7.3 Risk profiles will inform internal audit work necessary to provide annual assurance to the Accounting Officer about the reliability and effectiveness of our control systems and procedures. For the principal risks identified by the Strategic Management Group, the Internal Audit Service may evaluate the effectiveness of the existing controls and risk management responses. The assurance from Internal Audit will include an assessment of the reliability and effectiveness of the organisation’s overall risk management arrangements.

Appendix 1: Risk management definitions we use

RISK MANAGEMENT is the sum of the culture, processes, controls and structures that are directed towards the effective, timely and appropriate management of potential changes, opportunities and threats to achieving Estyn's aims and objectives. Risk management is the coordinated activities designed and operated to manage risk and exercise internal control within an organisation.

RISK has to do with uncertainty about an event that will have consequences for an objective or outcome, whether positive opportunity or negative threat. It is the combination of likelihood and impact, including its perceived importance, that constitutes risk. Risk is something that could:

- have an impact by our not taking opportunities or not capitalising on corporate strengths
- prevent, hinder or fail to further the achievement of objectives
- cause financial disadvantage, i.e. additional costs or loss of money
- result in damage to, or loss of an opportunity to maintain and enhance our reputation

Risk is usually expressed in terms of causes, potential events, and their consequences:

- A **cause** is an element which alone or in combination has the potential to give rise to a risk.
- An **event** is an occurrence or change of a set of circumstances – it can be expected which does not happen or something that is not expected which does happen. Events can have multiple causes and consequences and can affect multiple objectives.
- **Consequences/effects** are the outcome of an event affecting objectives. Consequences can be certain or uncertain, can have positive or negative direct or indirect effects on objectives, can be expressed qualitatively or quantitatively, and can escalate through cascading and cumulative effects.

In stating risks, care should be taken to avoid stating consequences that may arise as being the risks themselves, i.e. identifying the symptoms without their cause(s).

PRINCIPAL RISK is an overarching, high level risk which could impact on most, or all, of the organisation and requires reference to and monitoring by the Strategic Management Group and the Strategy Board.

CORPORATE RISK is a significant risk with a wide-ranging impact requiring reference to and monitoring by members of the Operational Group / Inspection Leadership Group.

OPERATIONAL RISK is a risk requiring its management and resolution elsewhere in the organisation, e.g. through a project group or line-management.

ASSURANCE is the confirmation of the reliability of our systems, procedures, and controls. Appropriate assurance enables the Accounting Officer to complete the Governance Statement that accompanies the resource accounts throughout the year.

INHERENT RISK is the exposure arising from a specific risk before any action has been taken to manage it.

RESIDUAL RISK is the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.

RISK PROFILE is the documented and prioritised overall assessment of the range of specific risks faced by the organisation.

An example of an **operational risk** (event) from the perspective of the Inspection coordination team is shown:

Risk				
Cause		**Event**		**Consequence**
IC fails to send report for checking by due date	→	**Inspection report is not published within statutory deadline**	→	Statutory inspection report publication date missed – reputational damage incurred
IC fails to action response from provider	→			
IC completes inspection checklist without completing actions	→		→	Complaint made by provider and/or parents/other stakeholders – additional management time taken up to deal with this
IC Manager does not routinely check IC checklist and/or does not follow-up outstanding actions	→			
Unplanned absence of IC Manager – assurance process not covered by or delegated to a colleague	→		→	Performance Indicator is not met – explanation is required within Annual Report & Accounts (reputational damage)
There might be other 'causes' which are outside of the control of the IC team, e.g. report editing, QA, translation, web upload, etc.	→			

Risk Responses

TRANSFER (manage): Shifting the responsibility or burden for loss/damage to another party through legislation, contract, insurance or other means. For example, Trosol is made responsible for the quality of translation from English to Welsh of Estyn published documents.

TOLERATE (manage): Accept the risk in view of the potential benefits and the cost of either eliminating or mitigating the risk.

TREAT (reduce): This is the most likely category of response. We introduce **additional internal controls to reduce** the risk to an acceptable level. This could include, for example, monitoring the quality of work carried out by additional inspectors and editing reports. Alternatively, we might wish to consider changing the way we deliver aspects of our work to reduce the risks.

TERMINATE: This option is probably limited to more 'entrepreneurial' aspects of our operations where we might decide that the risks are too great and the potential rewards insufficient for us to engage in the activity at all. So, if a proposed project is very high risk and these risks cannot be mitigated we might decide to not go ahead with the project. Note there is unlikely to be an option to **eliminate** activities that fall within our core remit, but we can reduce (treat) risks.

RISK OWNERS are those people identified on the risk register as responsible for ensuring that controls, further actions and monitoring of specific risks is carried out. These people may not necessarily perform the actual actions (this is the responsibility of **ACTION OWNERS**) but they must either have necessary authority to ensure that others carry out the required actions or have access to a forum, such as Strategic Management Group, Operational Group / Inspection Leadership Group, in which any concerns about inaction can be raised and where necessary authority to require action to be taken can be provided.

Risk types

HM Treasury's "Orange Book" provides examples of categories of risk; these are not intended to be exhaustive:

STRATEGIC RISKS – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).

GOVERNANCE RISKS – Risks arising from unclear plans, priorities, authorities, and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

OPERATIONS RISKS – Risks arising from inadequate, poorly designed, or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.

LEGAL RISKS – Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).

PROPERTY RISKS – Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.

FINANCIAL RISKS – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

COMMERCIAL RISKS – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.

PEOPLE RISKS – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

TECHNOLOGY RISKS – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

INFORMATION RISKS – Risks arising from a failure to produce robust, suitable, and appropriate data/information and to exploit data/information to its full potential.

SECURITY RISKS – Risks arising from a failure to prevent unauthorised and/or inappropriate access to key government systems and assets, including people, platforms, information, and resources. This encompasses the subset of cyber security.

PROJECT/PROGRAMME RISKS – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost, and quality.

REPUTATIONAL RISKS – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

Some risks might not be categorised as ‘reputational’ but will have a reputational element. Where the reputational element is significant then consideration should be given to recording this as a separate risk on the risk register.

Appendix 2: Corporate risk management responsibilities

A2.1 As Accounting Officer, the Chief Inspector is ultimately accountable for the effective management of the organisation's business and, in particular, for ensuring that there are adequate risk management arrangements and a sound system of internal control. The Accounting Officer has designated the Assistant Director Inspection and Central Services responsibility for leading Estyn's overall approach to risk management.

A2.2 The Strategic Management Group is responsible for continuously identifying, managing, and reviewing risks at a **strategic** level. Members of the Operational Group / Inspection Leadership Group are responsible for ensuring that other **corporate** risks are properly managed. **Operational** risks will be managed through project and working groups or functional areas.

A2.3 The Strategic Management Group will require evidence that operational risk is being managed, and, where possible, that results are properly measured. Strategic Management Group is responsible for:

- developing and communicating organisational policy and information about the risk management programme to all staff, and, where appropriate, to Estyn's partners
- defining the organisation's risk tolerance / appetite (the overall level of exposure and nature of risks which are acceptable to the organisation – see section 5 above and appendix 5)
- setting policies on internal control based on the organisation's risk profile, its ability to manage the risks identified and the cost/benefit of related controls
- seeking regular assurance on the effectiveness of actions identified to control risks and that the system of internal control is effective in managing risks in accordance with the Strategic Management Group's policies

A2.4 Individual members of the Strategic Management Group, and the Operational Group / Inspection Leadership Group will assume ownership for managing specific principal strategic and corporate risks on **the strategic and corporate risk registers**, and for evaluating and providing assurances on the effectiveness of controls.

A2.5 All staff are responsible for compliance with the prescribed procedures set out in organisational policies and for undertaking their job within the risk management guidelines set down for them by their line manager. All staff have a responsibility to help their line managers to identify, evaluate and manage operational risks. Line managers are ideally placed to pick up those early warning indicators that problems are developing. Team meetings can be used to discuss risks and report information regarding the management of risks to line managers. This is an important responsibility.

Group leaders should bring emerging corporate risks identified by themselves or their staff to the attention of the Operational Group / Inspection Leadership Group via their line manager.

A2.6 Group leaders and Central Services line managers should ensure that everyone in their teams understand their risk management responsibilities and must make clear the extent to which staff are empowered to take risks in line with the terms of this document and other guidance that may have been issued on specific topics.

A2.7 Project Managers are responsible for identifying and managing project-specific risks on an ongoing basis and are required to maintain their **own project-related risk registers**. This will be separate from the strategic and corporate risk registers.

A2.8 The Accounting Officer, supported by the Strategy Board, will periodically assess whether the leadership style, opportunity for debate and Estyn policies support the desired risk culture, incentivise expected behaviours and sanction inappropriate behaviours.

A2.9 The role of Strategy Board is to ensure that Estyn manages risk effectively through the development of an all-encompassing corporate strategy. The Strategy Board is responsible for:

- further developing the risk management strategy in liaison with the Strategic Management Group overseeing the implementation of the risk management strategy across the organisation
- continuously assessing the nature and extent of the principal risks that Estyn is willing to take to achieve its objectives – its ‘risk appetite’ – and ensuring that planning and decision-making appropriately reflect this assessment
- using horizon scanning and scenario planning collectively to consider the nature of emerging risks, threats and trends
- agreeing the frequency and scope of its discussions on risk to review how management is responding to the principal risks and how this is integrated with other matters considered by the board, including business planning and performance management processes
- undertaking a ‘deep dive’ review of a principal risk periodically
- monitoring and reviewing the effectiveness of the risk management strategy

A2.10 The Audit and Risk Assurance Committee has a fundamental role to play in the managing risk. Its role is to:

- obtain or request from management an explanation of the risk management strategy
- gain assurance that appropriate risk registers are being compiled and that the greatest threats are being addressed
- satisfy itself that the less significant risks are also being actively managed, with the appropriate controls in place and working effectively
- ensure that internal and external auditors have plans to satisfy themselves on the adequacy of risk management and are able to provide an assurance on issues of corporate governance, risk management and internal control
- assess the approach to risk management, including effectiveness of the risk management framework, and approve changes or improvements to key elements of its processes, procedures, and Risk Management Policy
- assess compliance with the Corporate Governance Code
- review the draft Governance Statement for inclusion in the financial statements

A2.11 The role of Internal Audit is to provide an independent opinion as to the effectiveness of risk management systems and to support the effective development, implementation and review of risk management. Internal Audit is responsible for:

- reviewing the effectiveness of risk management throughout Estyn
- providing an annual opinion on the effectiveness of risk management for inclusion in the Governance Statement
- advising the Accounting Officer and Audit and Risk Assurance Committee through the provision of up-to-date, practical advice on risk management

A2.12 The role of External Audit is to report on whether the Governance Statement meets the requirements for disclosure specified by HM Treasury, or if the statement is misleading or inconsistent with other information of which they are aware from their audit of the financial statements. External Audit is responsible for:

- considering whether the disclosures are consistent with the External Auditor’s review of minutes of board and committee meetings and their knowledge of Estyn obtained during the audit of the financial statements
- attending Audit and Risk Assurance Committee meetings at which corporate governance, internal control and risk management processes are considered.

Appendix 3: Guide to completing the strategic and corporate risk registers

Risks are reported to the following meetings:

Meeting	Risks
Strategic Management Group	Strategic risk register – quarterly
Operational Group / Inspection Leadership Group	Corporate risk register – quarterly
Strategy Board	Strategic risk register – every meeting
Audit and Risk Assurance Committee	Strategic risk register – every meeting Corporate risk register – annually

The following is a step-by-step guide on how to complete the **strategic and corporate risk registers** and may be used with project registers:

Column heading	How to complete it
Risk reference	References are allocated to risks by secretariat as they are added to the register References will be added in the format of S / C followed by a number. Risks will retain their reference number even when moved to the closed risks section of the register.
Strategic objective	Risks spring from business objectives. Make the link at this stage to our strategic objectives.
Risk type	HM Treasury's "Orange Book" provides examples of categories of risk; these are listed in appendix 1 (risk management definitions). These are listed.
Risk owner and date registered	The 'overarching owner' of the risk – add name. Should be one person with overall responsibility. Strategic register – decision-making members of SMG. Corporate register – Head of Branch and above. The date the risk is added to the register.

Current/inherent risk description (cause and effect)	Details of the risk being identified. This should usually be in the format of 'if we do not do X then there is a risk of Y happening' although there may be exceptions. Gain an understanding of the risk to respond to it in the most effective way: what can happen? how can it happen? why can it happen? This involves a qualitative description of the likelihood of a risk coming about and the severity of the impact should this occur.
Underlying causes	Think about what might stop aims and objectives from being achieved and describe this in terms of 'underlying causes' of a risk.
Inherent risk impact/likelihood risk rating – impact x likelihood	This section requires 'scoring'**. Please refer to the risk scoring tab in the risk register** and to Appendix 4 of this guide. Insert a **number** for impact and likelihood. This is the risk as it was originally identified before any mitigations/controls were put in place. The total column is automatically generated: Green: 1 to 3 (tolerable risk) Yellow: 4 to 6 (moderate risk) Amber: 8 to 12 (substantial risk) Red: 15 to 25 (severe risk)
Current controls in place (what is actually happening)	Details of controls that have been put in place / mitigations should be added here.
Residual risk impact/likelihood risk rating – impact x likelihood	This section requires 'scoring'. **Please refer to the risk scoring tab in the risk register** and to Appendix 4 of this guide. Insert a **number** for impact and likelihood. This is the remaining level of risk after controls / mitigations and assurances have been put in place. The total column is automatically generated: Green: 1 to 3 (tolerable risk) Yellow: 4 to 6 (moderate risk) Amber: 8 to 12 (substantial risk) Red: 15 to 25 (severe risk)

Previous residual score / risk score movement	Risk score movement since the last review will be recorded to indicate the effectiveness of current controls / assurances and any further plans.
Strategy (accept & manage , reduce, eliminate)	Consider the current strategy for the risk (see Appendix 1 risk responses): Accept and manage – within existing controls / assurances with no further action required. May include transferring the risk to another party e.g. through contract. Periodic monitoring to ensure controls / assurances are effective. Reduce – identify what further actions need to take place place to further reduce the risk (**the most likely category of response**). Eliminate – probably limited to more 'entrepreneurial' aspects of our operations where we might decide that the risks are too great and the potential rewards insufficient for us to engage in the activity at all.
Further actions (what still needs to be done). And action owner and action deadline	Identify what further actions need to take place place to further reduce the risk. Consider the risk-mitigation strategy (e.g. if the impact is significant but it is very unlikely that the risk will occur, strategies/actions to reduce the impact rather than the likelihood may be more appropriate). Include who is responsible for the actions identified (Branch Head and above) and by when.
Target risk	Add what risk score is acceptable to the organisation, recognising that some risks cannot be avoided. What score can be tolerated? Check that the risk target / tolerance is aligned with the risk appetite for the business area or activity (refer to Appendix 5 of this guide for examples of the range of acceptable outcomes based on the adopted risk appetite).
Assurance – inhouse and 3rd party / independent	Record any assurance where applicable: • in house 1st line – performance data, monitoring statistics, incident reporting, group updates, feedback and complaints, PIQs, management information • in house 2nd line – compliance assessments re: policies, quality arrangements, health and safety, security, financial control assurance,action log reviews, assurance re: contractual arrangements, information management, etc. and/or

	• third party / independent - internal audit, other independent sources of assurance e.g. Cyber checks, CHS, GD, and external audit and benchmarking. Estyn considers/reviews risk through the Strategy Board, Audit and Risk Assurance Committee, our management structure and reporting (first and second line roles), the internal audit function and other external assurance providers such as external audit. This is in line with our Corporate governance framework – 2023 (page 7 – Estyn assurance and scrutiny framework arrangements) and the Institute of Internal Auditors Three Lines Model – three-lines-model-updated-english.pdf (theiia.org).
Risk target met Yes/ no	Confirm if risk target/tolerance met.
Updated by / date of update	Name of person updating the risk Add the date that the risk was reviewed/updated **NB** all updates should be made in RED for discussion at the relevant meeting.

Risk registers will provide evidence to support the Accounting Officer’s annual Governance Statement. They will also assist both Internal and External Audit in developing their audit programmes.

Appendix 4: Risk scoring – Estyn approach to prioritising risk

Once potential risks to the area of responsibility of the group or project are identified, it is necessary to analyse the risks to distinguish between minor acceptable risks and major risks. This process will also include determining the probability (likelihood) of the risk happening and the impact the risk will have on Estyn should the risk occur. Both the inherent and residual risk assessment uses the following:

Risk probability ratings

Value	Rating	Criteria
1	Rare	Can't believe that this will ever happen
2	Unlikely	Not expected it to happen, but may do
3	Possibly	May occur occasionally
4	Likely	Will probably occur, but is not a persistent issue
5	Almost certain	Likely to occur, on many occasions

Risk impact (severity) ratings

Value	Rating	Impact (text provided as guideline to aid process of judging the potential severity of a risk in terms of Finance – Reputation – Staff – Operations; not intended to be comprehensive or exact)
1	Negligible	Very small financial impact (<£2K), limited reputational damage, just a few whispers among staff, limited operational impact easily fixed
2	Minor	Small financial impact (<£5k), reputational damage might be evident to those close to event, unsettling rumours (among staff), minor operational impact (workarounds required)
3	Moderate	>£5k <£25k, reputation impacted in local/specialist area (not wider public), significant injury or cause for concern to staff, significant operational impact – disruption to several services – delays in processes.
4	Major	>£25k<£100k, reputational damage with lasting effect, widespread dissatisfaction and demotivation of staff, serious accident/injury, major operational disruption (e.g. long delays, wasted resources,)
5	Catastrophic	>£100k, severe reputational damage (e.g. prominent national media coverage), major impact on staff morale, staff fatality, severe operational disruption (e.g. service unavailable for more than one week)

This methodology helps us to prioritise our response to risk, to determine which risks we need to manage and which are less critical. Risk-review groups will actively monitor and manage those risks identified which fall within the 'Moderate' to 'Severe' areas of the following matrix:

Risk rating		**Impact**					
			Catastrophic	**Major**	**Moderate**	**Minor**	**Negligible**
Likelihood	**Description**	**score**	**5**	**4**	**3**	**2**	**1**
Almost Certain	Likely to occur, on many occasions	**5**	25	20	15	10	5
Likely	Will probably occur, but is not a persistent issue	**4**	20	16	12	8	4
Possible	May occur occasionally	**3**	15	12	9	6	3
Unlikely	Not expected it to happen, but may do	**2**	10	8	6	4	2
Rare	Can't believe that this will ever happen	**1**	5	4	3	2	1

Risk = 1- 3	**Tolerable risk**
Risk = 4-6	**Moderate risk**
Risk = 8-12	**Substantial risk**
Risk = 15-25	**Severe risk**

Target risk score: risk appetite

Use the example appetite levels defined by risk categories in appendix 5 to identify the risk appetite level (averse, minimal, cautious, open or eager) for each risk and then determine the target risk scores to include on the risk register.

Risk appetite level definition	Averse	Minimal	Cautious	Open	Eager
Target risk score	1 or 2	3 or 4	5 or 6	8 or 9	10 or 12

Note: The following matrix is an alternative that may be used outside of the composite risk register for plotting risks and management action, e.g. this may be useful for managing team and individual risks:

Impact	High	mitigation controls / contingency plans	mitigation controls / contingency plans – monitor closely	urgent action required – monitor rigorously
	Medium	tolerate – keep watching brief	mitigation controls / contingency plans	mitigation controls / contingency plans – monitor closely
	Low	tolerate – no action	tolerate – keep watching brief	mitigation controls / contingency plans
		Low	Medium	High
			Probability	

Appendix 5: Risk appetite

Risk appetite scale

Risk Appetite	Description
Averse	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is key objective. Activities undertaken will only be those considered to carry virtually no inherent risk.
Minimalist	Preference for very safe business delivery options that have a low degree of inherent risk with the potential for benefit/return not a key driver. Activities will only be undertaken where they have a low degree of inherent risk.
Cautious	Preference for safe options that have low degree of inherent risk and only limited potential for benefit. Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and/or realise an opportunity. Activities undertaken my carry a high degree of inherent risk that is deemed controllable to a large extent.
Open (Receptive)	Willing to consider all options and choose one most likely to result in successful delivery while providing an acceptable level of benefit. Seek to achieve a balance between a high likelihood of successful delivery and a high degree of benefit and value for money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk.
Eager	Eager to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk.

Example appetite levels defined by risk categories.

The following table provides example appetite levels defined by risk categories as set out in the Orange Book: Risk Appetite Guidance Note Risk Appetite Guidance Note (publishing.service.gov.uk). These represent a sample of risk appetites developed against a selection of the risk categories recommended in Annex 4 of the The Orange Book – Management of Risk – Principles and Concepts (publishing.service.gov.uk).

Risk category	Risk Appetite level definition				
	Averse	Minimal	Cautious	Open	Eager
Strategy	Guiding principles or rules in place that limit risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 5+ year intervals.	Guiding principles or rules in place that minimise risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 4-5 year intervals.	Guiding principles or rules in place that allow considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 3-4 year intervals.	Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2-3 year intervals.	Guiding principles or rules in place that welcome considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 1-2 year intervals.
Governance	Avoid actions with associated risk. No decisions are taken outside of processes and oversight / monitoring arrangements. Organisational controls minimise risk of fraud, with significant levels of resource focused on detection and prevention.	Willing to consider low risk actions which support delivery of priorities and objectives. Processes, and oversight / monitoring arrangements enable limited risk taking. Organisational controls maximise fraud prevention, detection and deterrence through	Willing to consider actions where benefits outweigh risks. Processes, and oversight / monitoring arrangements enable cautious risk taking. Controls enable fraud prevention, detection and deterrence by maintaining appropriate controls and sanctions.	Receptive to taking difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements enable considered risk taking. Levels of fraud controls are varied to reflect scale of risks with costs.	Ready to take difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements support informed risk taking. Levels of fraud controls are varied to reflect scale of risk with costs.

Risk category	**Risk Appetite level definition**				
	Averse	**Minimal**	**Cautious**	**Open**	**Eager**
		robust controls and sanctions.			
Operations	Defensive approach to operational delivery - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority.	Innovations largely avoided unless essential. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with clear demonstration of benefit / improvement in management control. Responsibility for noncritical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority –management by trust /lagging indicators rather than close control.
Legal	Play safe and avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge.	Want to be reasonably sure we would win any challenge.	Challenge will be problematic; we are likely to win and the gain will outweigh the adverse impact.	Chances of losing are high but exceptional benefits could be realised.
Financial	Avoidance of any financial impact or loss, is a key objective.	Only prepared to accept the possibility of very limited financial impact if essential to delivery.	Seek safe delivery options with little residual financial loss only if it could yield upside opportunities.	Prepared to invest for benefit and to minimise the possibility of financial loss by managing the risks to tolerable levels.	Prepared to invest for best possible benefit and accept possibility of financial loss (controls must be in place).
Commercial	Zero appetite for untested commercial agreements. Priority for close management controls and oversight	Appetite for risk taking limited to low scale procurement activity. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior	Innovation supported, with demonstration of benefit / improvement in service delivery. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management

Risk category	Risk Appetite level definition				
	Averse	**Minimal**	**Cautious**	**Open**	**Eager**
	with limited devolved authority.		management. Management through leading indicators.		by trust / lagging indicators rather than close control.
People	Priority to maintain close management control & oversight. Limited devolved authority. Limited flexibility in relation to working practices. Development investment in standard practices only	Decision making authority held by senior management. Development investment generally in standard practices.	Seek safe and standard people policy. Decision making authority generally held by senior management.	Prepared to invest in our people to create innovative mix of skills environment. Responsibility for noncritical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control
Technology	General avoidance of systems / technology developments.	Only essential systems / technology developments to protect current operations.	Consideration given to adoption of established / mature systems and technology improvements. Agile principles are considered.	Systems / technology developments considered to enable improved delivery. Agile principles may be followed.	New technologies viewed as a key enabler of operational delivery. Agile principles are embraced.
Data and Information Management	Lock down data & information. Access tightly controlled, high levels of monitoring.	Minimise level of risk due to potential damage from disclosure.	Accept need for operational effectiveness with risk mitigated through careful management limiting distribution.	Accept need for operational effectiveness in distribution and information sharing.	Level of controls minimised with data and information openly shared.
Security	No tolerance for security risks causing loss or damage to HMG property, assets, information or people. Stringent measures in place, including: • Adherence to FCDO travel restrictions • Staff	Risk of loss or damage to HMG property, assets, information or people minimised through stringent security measures, including: • Adherence to FCDO travel restrictions • All staff	Limited security risks accepted to support business need, with appropriate checks and balances in place: • Adherence to FCDO travel restrictions •Vetting levels may flex within teams, as required •Controls managing staff and limiting visitor access to information,	Considered security risk accepted to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes •	Organisational willing to accept security risk to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial

Risk category	Risk Appetite level definition				
	Averse	Minimal	Cautious	Open	Eager
	vetting maintained at highest appropriate level. • Controls limiting staff and visitor access to information, assets and estate. • Access to staff personal devices restricted in official sites.	vetted levels defined by role requirements. • Controls limiting staff and visitor access to information, assets and estate. • Staff personal devices permitted, but may not be used for official tasks.	assets and estate. •Staff personal devices may be used for limited official tasks with appropriate permissions.	Permission may be sought for travel within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices may be used for official tasks with appropriate permissions.	completion of vetting processes • Travel permitted within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices permitted for official tasks
Project/Progamme	Defensive approach to transformational activity - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority. Benefits led plans fully aligned with strategic priorities, functional standards.	Innovations avoided unless essential. Decision making authority held by senior management. Benefits led plans aligned with strategic priorities, functional standards.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Plans aligned with strategic priorities, functional standards.	Innovation supported, with demonstration of commensurate improvements in management control. Responsibility for noncritical decisions may be devolved. Plans aligned with functional standards and organisational governance.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control. Plans aligned with organisational governance.
Reputational	Zero appetite for any decisions with high chance of repercussion for organisations' reputation.	Appetite for risk taking limited to those events where there is no chance of any significant repercussion for the organisation.	Appetite for risk taking limited to those events where there is little chance of any significant repercussion for the organisation.	Appetite to take decisions with potential to expose organisation to additional scrutiny, but only where appropriate steps are taken to minimise exposure.	Appetite to take decisions which are likely to bring additional governmental / organisational scrutiny only where potential benefits outweigh risks.

Example: Risk appetite statement

Example prepared as a guide for organisational activity and decision making in relation to **financial risk.**

Financial risk

Estyn’s appetite for financial risk is **cautious.** Our financial decisions are heavily scrutinised, with value for money being a key factor in decision making. We will accept risks that may result in some small-scale financial loss or exposure on the basis that these can be expected to balance out but will not accept financial risks that could result in significant reprioritisation of budgets. Our appetite for risks associated with business as usual activity is naturally lower than with our transformation activity. Within this our risk appetite is:

- **Averse** for financial propriety and regularity risks with a determined focus to maintain effective financial control framework accountability structures.

- **Averse** in terms of risks related to our qualification of accounts, associated process, and deviation from reporting timetables.

- **Minimal** as to risk relating to breaching individual control totals (budget levels).

- **Open** for risks relating to innovation supported, with demonstration of benefit / improvement in service delivery