Ormiston Latimer Academy

OAT Risk Management Policy and Framework

Approved by the Principal: September 2022
Review Date: September 2023

Ormiston Academies Trust

Ormiston Latimer Academy
Risk Management Policy

Policy version control

Policy Type	OAT Mandatory policy
Author:	Joanne Dawson, Chief Finance Officer/ National Director of Finance
Approved by	Exec, September 2021
Trust Board approved	9 September 2021
Next Release date:	September 2022
Description of changes	This policy has been substantially rewritten and further developed with consideration to the following: ▪ Internal feedback following the introduction of the previous Risk Management Policy and processes in September 2020. ▪ Feedback from internal audit following a review of the Trust policy and procedures. ▪ Research into external guidance on risk management practices. ▪ A review of policy and procedures of other organisations where these are available; and ▪ Government guidance on management of risk including that provided within the Academies Trust Handbook.

Contents

1. Introduction

1.1. This policy sets out the Trust's intended approach to risk management across the organization.

1.2. Risk management is an essential part of governance and leadership, fundamental to how the organization is directed, managed, and controlled at all levels. Therefore, risk management should be an integral part of all the Trust's activities, to support decision-making in achieving objectives.

1.3. Risk management processes involve identifying risks, assessing the likelihood of them occurring, then proactively managing those risks by planning, and implementing mitigations to each risk. The risk assessment is used to determine what level of mitigation is appropriate.

1.4. Risk can often never be eliminated and often it is not possible, nor financially affordable, to manage all risks at any point in time to the most desirable level.

1.5. This policy forms part of the Trust's internal control and governance arrangements.

2. Policy Scope

2.1. This policy applies to all Trust staff in all academies, leadership, central management, and support services, including individuals employed by the Trust, contractors, and agency staff.

2.2. It is the responsibility of all individuals in the Trust to familiarize themselves with this policy and comply with its provisions.

2.3. This policy if not concerned with Crisis Management, Incident Management, Business Continuity and Disaster Recovery specifically, although these are elements of the Trust's risk management activities.

2.4. Risk management covers the full operations and activities of the Trust, not only financial risks.

3. Legal and Regulatory Framework

3.1. The Academies Trust Handbook, updated in June 2021 and effective from September 2021, sets out several mandatory requirements in relation to risk management.

   3.1.1. The trust **must** manage risks to ensure effective operation and must maintain a risk register

      3.1.1.1. Overall responsibility for risk management, including ultimate oversight of the risk register, must be retained by the board of trustees, drawing on advice provided to it by the audit and risk committee.

      3.1.1.2. Other committees may also input into the management of risk at the discretion of the board.

3.1.1.3. Aside from any review by individual committees, the board itself must review the risk register at least annually.

3.1.1.4. Risks management covers the full operations and activities of the trust, not only financial risks

3.2. The Academy Trust Handbook also sets out mandatory requirements in relation to internal scrutiny, i.e., a program of checks to provide independent assurance to the board that its financial and non-financial controls and risk management procedures are operating effectively.

3.2.1. Internal scrutiny **must** focus on:

3.2.1.1. evaluating the suitability of, and level of compliance with, financial and non-financial controls. This includes assessing whether procedures are designed effectively and efficiently, and checking whether agreed procedures have been followed

3.2.1.2. offering advice and insight to the board on how to address weaknesses in financial and non-financial controls, acting as a catalyst for improvement, but without diluting management's responsibility for day to day running of the trust

3.2.1.3. ensuring all categories of risk are being adequately identified, reported, and managed.

3.2.2. The trust **must** identify on a risk-basis (with reference to its risk register) the areas it will review each year, modifying its checks accordingly. For example, this may involve greater scrutiny where procedures or systems have changed.

3.2.3. Internal scrutiny should take account of output from other assurance procedures to inform the program of work. For example, it should have regard to recommendations from the trust's external auditors as described in their management letter, and from relevant reviews undertaken by ESFA.

3.2.4. Independence in internal scrutiny must be achieved by establishing appropriate reporting lines whereby those carrying out checks report directly to a committee of the board, which in turn provides assurance to the trustees.

3.2.5. The internal scrutiny must be conducted by someone suitably qualified and experienced and able to draw on technical expertise as required.

3.2.6. The committee's oversight must extend to the financial and non-financial controls and risks at constituent academies and must ensure information submitted to the DfE, ESFA and other external bodies that affects funding, including but not limited to pupil number returns, is complete, accurate and in compliance with funding criteria and submitted in a timely manner.

3.2.7.6 The academy trust must establish an audit and risk committee, appointed by the board which should meet at least three times a year.

3.2.8. The audit and risk committee **must**:

3.2.8.1. oversee and approve the trust's programme of internal scrutiny

3.2.8.2. ensure that risks are being addressed appropriately through internal scrutiny

3.2.8.3. report to the board on the adequacy of the trust's internal control framework, including financial and non-financial controls and management of risks.

3.2.9. Employees of the trust should not be audit and risk committee members, but the accounting officer and chief financial officer should attend to provide information and participate in discussions.

3.2.10. The chair of trustees should not be chair of the audit and risk committee. Where the finance committee and audit and risk committee are separate, the chair should not be the same.

3.2.11. Where the audit and risk committee are combined with another committee, employees should not participate as members when audit matters are discussed.

4. Definitions

4.1. **Trust** means all academies within the Ormiston Academies Trusts, as well as central leadership and support services.

4.2. **Executive Leadership Team** means the Chief Executive Officer ("CEO") and the direct line management reports of the CEO (the "Executive Team Members").

4.3. **Trust staff** means all permanent employees of the Trusts, as well as temporary employees, fixed term contractors and agency staff.

4.4. **Risk** is the threat of an outcome adversely or positively affecting the trust's ability to achieve its objectives and successfully execute its strategies.

$$Risk = Likelihood \times Impact$$
Both Likelihood and Impact are scored on a scale of 1-5.
Maximum risk score is therefore 25.

4.5. **Risk exposure** means the severity of the combination of the probability of a risk event occurring and the magnitude of its impact. This is also referred to **Gross risk** – the level of risk before considering the effect of any preventative or mitigating action – either existing or planned controls.

4.6. **Net risk** refers to the level of risk after considering the effect of any existing controls and their effectiveness i.e., the situation as it is at the current time.

4.7. **Probability** means the likelihood of a particular outcome occurring (including a consideration of the frequency with which the outcome may arise). **Likelihood** is the probability of occurrence of an impact – how likely is the event to happen and the risk – considering the control mechanisms that are in place.

The assessment of probability should depend on factors such as history, current circumstances, and the nature of controls in place. The Trust uses the following descriptors:

4.8. **Impact** means the evaluation effect of result of a particular outcome occurring.

4.9. **Control mechanisms/ measures –** the process, policies and procedures used to govern the Trust (and academies) or any additional controls or mitigating actions taken to deal with the situation. A judgement must be made by the risk owner as to the numerical reduction to the gross risk (risk exposure) score to produce the net risk score.

4.10. **Risk Mitigation** involves development of mitigation plans designed to manage, eliminate, or reduce risk to an acceptable level. Once a plan is implemented, it should be continually monitored to assess its efficacy with the intent of revising the course of action if necessary.

4.11. **Risk Register** means a document which sets out identified risks, their risk exposures, mitigating controls and assessment of control effectiveness.

4.12. **Risk Scoring Matrix (or Risk Matrix)** is a matrix that is used during risk assessment to define the level of risk by considering the category or probability (or likelihood) against the impact (or consequence) severity. This is a simple mechanism to increase visibility of risks and assist management decision making. An example is shown in appendix 3.

4.13. **Risk Tolerance** means the level of risk with which the organization is willing to operate, given current constraints. This reflects the intention to optimize the delivery of strategic objectives with consideration to all constraints including the need to ensure long-term financial viability of the Trust.

4.14. **Risk Management** is the process of identifying, evaluating, and controlling risks and is a key element in the framework of academy governance.

4.15. **Risk Owner** - A named individual staff member, who is closely involved with the risk, can monitor it, initiate action if the risk becomes more serious, or escalate to senior management if necessary.

4.16. **Trust Risk Champion** – a member of the executive with day-to-day responsibility for the oversight of risk for the Trust.

4.17. **Academy Risk Champion** and **Head Office Risk Champion** – A named individual who is ultimately responsible for the review and completion of the risk register. In academies, this ultimately sits with Principal, but can be delegated to a member of SLT.

4.18. **Control Owner** - A person or entity with accountability for ensuring that the control activity is in place and is operating effectively. The control owner does not necessarily perform the control activity, however, if not conducting the control, they should have a level of oversight of its performance.

4.19. **Process owners** "own" the processes within which the controls are embedded. Control owners "own" the responsibility to execute the controls. Process owners both execute controls (as a control owner) AND supervise and monitor the execution of controls (by designated control owners).

4.20. **Assurance** is an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management and control processes for an organization.

4.21. An **Assurance Map** is a structured means of identifying and mapping the main sources and types of assurance in an organisation across the four lines of defence and coordinating them to best effect. An example of an assurance map is provided in appendix 4.

4.22. **Four Lines of defence** (also known as the three lines of defence when excluding external audit and as referred to in the Orange Book) refers to the underlying idea that in any organization, management seeks to achieve its aims by establishing systems and processes to manage its main risks. Depending on the organization and its objectives, these systems and processes can be developed in different ways and the evidence of the operation of the controls will vary. This means that the level of assurance derived by management from the operation of controls will also vary. Ideally, the various controls combine to provide management with sufficient (quantity) and appropriate (quality) evidence of controls in place to manage the organization's main risks. More information on Lines of Défense are provided in Appendix 2a and Appendix 2b.

5. The Trust's policy on Risk Management

Risk Appetite

5.1. The Trust will develop and maintain a Risk Appetite Statement to describe the Trust's attitude to accepting risk in each category of principal risk.

5.2. The Trust Board will review and approve the Risk Appetite Statement on an annual basis, or more frequently as necessary to reflect any significant change in the content within which the Trust operates.

Risk Management Framework

5.3. The Trust aims to adopt, as far as possible within budgetary constraints, a "Three Lines of defence" approach to risk management, as references in HP Government's publication, "The Orange Book: Management of Risk – Principals and Concepts (2020). An overview of such a framework is illustrated in Appendix 1.

5.4. The Trust will adopt a continuous, cyclical approach to risk management processes, as illustrated in the diagram in Appendix 2, extracted from HM Government's The Orange Book: Management of Risk – Principles and Concepts (2020).

Identification of risks

5.5. The Trust will, embed risk management to ensure that it is an integral part of all organizational activities to support decision-making in achieving its objectives. As such, the Trust will on a regular and on-going basis, consider the nature of the risks that it faces as an organization – alongside and integrated with the following processes: setting strategy and plans; evaluating options and delivering programmes, projects, or policy initiatives; prioritizing resources; supporting effective and efficient operations; managing performance; managing assets; and delivering improved outcomes.

5.6. To identify risks, we will encourage and support the use multiple identifying tools and techniques. For example: Documentation reviews; Information Gathering; Brainstorming; Interviewing; SWOT analysis; Horizon scanning; Checklist analysis; Risk registers etc.

5.7. Consideration will be given to a full range of factors that may result in a risk occurring, as well an internal factor, including factors which may change over time.

5.8. There are numerous ways in which organisations categorise risks and failure to manage these may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, stakeholder, and operational consequences. For example:

   5.8.1. *Strategic* - 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).

   5.8.2. *Governanc*e – Risks arising from unclear plans, priorities, authorities, and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

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

   5.8.4. *Legal* – 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 those 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).

   5.8.5. *Property* – 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.

   5.8.6. *Financial* – 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.

   5.8.7. *Commercial* – 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.

   5.8.8. *People* – 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.

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

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

5.8.11. *Security* – Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

5.8.12. *Project/Programme* – 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.

5.8.13. *Reputational* – 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

5.9. At Ormiston Academies Trust, we have developed a framework where risks are grouped and considered as follows:

5.9.1. **Duty to our key stakeholders**, including parents and communities, for the safety and welfare of children, and for their educational (academic and personal development) outcomes.

5.9.2. **Organisational effectiveness**, including all aspects of people management - the ability to structure our organization and attract, recruit, develop and retain staff that meet the current needs and aspirations of the organisation, and **efficient delivery** through robust organizational management processes and systems (governance, information, data, technology, and processes) integrated across all functions. Together, a collaborative, forward-thinking, transparent, and supportive organization that seeks to have as positive an impact on as many children as possible by sharing and embedding what is best and, in doing so, achieving more together.

5.9.3. **Trust viability** where success is measured by the strength of the Trust's strategic, financial, and structural integrity and through its ability to demonstrate added value to the academies and communities that they serve – where the Trust is the sum of its academies, and the academies reflect the strength of the Trust.

5.9.4. **Compliance** with laws and statutory guidelines.

5.10. We believe that, by taking this approach, we will deliver on our strategy in a sustainable manner and achieve our mission.

5.11. Across these four groups, we have created 12 risk headings and it is at this level that we have delegated ownership to trustee committees and executives. However, the Board of Trustees is ultimately accountable for ensuring that risk is managed. Supported by the Audit & Risk Committee, they will review the risk policy annually. At the same time, as part of an annual Trust level strategy and risk review, they will review the risk heads to ensure that these effectively

capture the breadth of strategic risks facing the trust and adequately act as a framework for capturing detailed risks at an operational level.

5.12. The executive risk register (consolidated view of HO and academy risk registers) will be reviewed termly

Risk Heading	Delegated executive and risk owner	Governance forum
Trust Strategy, growth, transformation, and stakeholder engagement (Trust Governance)	Chief Executive Officer	Full Board
Child welfare and protection	National Director of Education	Education Committee
Educational standards and pupil outcomes	National Director of Education	Education Committee
People Management (recruitment, performance management, development, well-being, pay and remuneration)	National Director of HR National Director of Teaching & Training	People Committee
Pupil Numbers (and associated data)	National Director of Education	Education Committee and Finance Committee
Financial Management (Including Value for Money)	National Director of Finance	Finance Committee
Estates Management (including Health and safety)	National Director of Estates and Technology	Finance Committee
Technology Management (Incl. Cyber security and GDPR)	National Director of Estates and Technology	Finance Committee
Trust (incl. Academy, Programme and Project) Governance	National Director of Finance	Audit & Risk Committee
Information	National Director of Finance	All committees
Operations (Processes incl. oversight of projects)	National Director of Finance	All committees
Legal and Compliance with Statutory and Trust Policies.	National Director of Finance	Audit & Risk Committee

Risk Register

5.13. To identify, evaluate and proactively manage risk, we have developed a risk register that meets the needs of our organization.

5.14. Within the risk register, each of the risks are categorized under the ten risk headings noted above so that they can be grouped and reviewed by the relevant executive, academy SLT and governance forum.

5.15. Each entry in the risk register gives details of the risk and is evaluated using a scoring system which takes account of:

- The probability of the risk materializing
- The potential impact it would have
- The risk-mitigating measures and controls currently in place across the trust.

5.15. The assessment of probability should depend on factors such as history, current circumstances, and the nature of controls in place. The Trust uses the following descriptors:

Likelihood score	Descriptor	Description
1	Rare	Can't believe this will ever happen.
2	Unlikely	Do not expect this to happen but it is possible
3	Possible	May occur occasionally
4	Likely	Will probably occur but it is not a persistent issue
5	Almost certain	Likely to occur on many occasions, a persistent issue.

5.16. Impact should be considered by sub-entity (i.e., academy, function, programme) in addition to at trust level because the sum of many small risks can be significant at a trust level.

5.17. Assessment should follow the guidance below noting that this is guidance only and other factors should be considered as appropriate.

Impact score	Description
1	• Financial net impact of less than 0.2% of turnover [For 21/22 – this will 0.2% of £225m or ~ £0.5m for Trust level risks]. *For academies – please use 0.2 % of local academy turnover.* • No other significant impacts.
2	• Financial net impact of less than 0.2% of turnover [For 21/22 – this will 0.2% of £225m or ~ £0.5m for Trust level risks]. No other significant impacts. *For academies – please use 0.2 % of local academy turnover.*

	• No regulatory consequences. • Adverse publicity locally or in sector publications (e.g., TES) • Minor injury.
3	• Financial net impact of 0.2% - 0.5% of turnover [For 21/22 – this will be 0.5% of £225m or ~1.25 for Trust level risks]. Academies – use 0.2 – 0.5% of local academy turnover. • Addressable regulatory consequences. • Adverse publicity in national newspapers. • Major injury.
4	• Financial net impact of 1% of turnover. turnover [For 21/22 – this will be £2.25m for Trust level risks]. Academies – use 1% of local academy turnover. • Substantial regulatory consequences. • Major sanction by ESFA. • Significant/ major national adverse publicity. • Death of an individual or several major injuries.

5.18. This produces a "net residual" score that is deemed either acceptable or unacceptable. If unacceptable, then details of further risk-mitigating actions are included in the risk register, including deadlines for implementation.

5.19. Where the need for risk mitigating measures (in place or to be acted on) is highlighted, then the management of both is included within the objectives of the relevant executive, academy SLT and subject to regular review and appraisal.

5.20. The risk register is a "living document" held on a shared site accessible by the appropriate stakeholders. It is the responsibility of each risk owner to monitor on an on-going basis and to update the risk register and highlight these changes to the executives and Board as appropriate.

5.21. The risk register is formally reviewed on a termly basis (three times per year) by the Executive Committee at Head Office and by SLT at the Academy, in line with the financial planning cycle. Scores may be adjusted, and risks added or removed.

5.22. Where further actions are required, these are shown on an action tracker (held within the same file) with a cross reference to the relevant risk. The action tracker is reviewed monthly by the executive team and Senior Leadership Team, to ensure all risk mitigation actions are acted on promptly.

5.23. The risk register is administered and monitored by OAT's Head of Compliance and Reporting and overseen by the National Director of Finance.

Assessment of risk exposure

5.24. The Trust will evaluate the risk exposure of all risks identified using a consistent framework across the Trust.

5.25. Sometimes a risk may be evaluated as having a high exposure and/ or inadequate mitigating internal controls. In such cases, reporting of these risks must be escalated to the Executive

Leadership Team, to be reflected on the top Trust-level Risk Register, as reviewed regularly by the Executive Leadership Team, until such time as the risk exposure is reduced and the mitigating controls are assessed as at least adequate.

Risk treatment: planning and implementation of risk response plans

5.26. Depending on the results of evaluation risk exposure, the Trust will plan and implement appropriate and cost-effective risk response plans.

Monitoring and review of risk management

5.27. The Trust will, on a regular and ongoing basis, reconsider the risks identified, re-evaluate risk exposure and review the risk response plans as required.

5.28. Risks and corresponding controls relevant to the Terms of Reference of Committees of the Trust Board may be delegated to those Committees of the Trust Bboard for monitoring, by the Risk & Audit Committee and will then be reported to those Committees for scrutiny in terms of evaluating the effectiveness of mitigating controls.

5.29. The Committee meeting minutes from each of the Committees of Trust Board, relating to scrutiny of delegated risks and controls, will be reported to the Risk & Audit Committee for oversight and the Risk and Audit Committee will make recommendations where required to other Committees and/ or Trust Board.

Internal Scrutiny

5.30. The Trust will engage at least one appropriately qualified and independent firm to provide bought-in internal audit services.

6. Record keeping

6.1. The Trust will retain records evidencing compliance with this policy, as set out in the Trust's Data Retention Policy. This will include records of Risk Registers and minutes of meetings.

6.2. From January 2022, all academy level risk registers will be stored on Governor Hub.

7. Roles and Responsibilities

7.1 The trustees of the Trusts, as charity trustees, have ultimate accountability for the Trust's proper management, which includes management of risk.

7.2 The Trust Board is accountable for overseeing risk management across the Trust as a whole.

7.3 The Trust Board has delegated responsibility for oversight and scrutiny of the Trust's risk management policy and procedures to the Audit & Risk Committee. The Trust Board will approve the appointment of internal auditors.

7.4   Responsibility for recommending an appropriate Risk Management Policy and Procedures is delegated to the Trust's executive Team.

7.5   Within the Executive Team, a Trust Risk Champion will be identified who will oversee, co-ordinate and direct the risk management procedures across the Trust.

7.6   Within the Trust central management team, the Trust Risk Champion will be supported by an appropriate member of the Senior Leadership Team in the co-ordination, including training, of risk management across the Trust.

7.7   The relevant personnel, together with their contact details, are included within the Principals Handbook and Centrals Teams documentation and shared via the Trust intranet site.

7.8   Although certain activities and responsibilities are delegated, the level of Trustee involvement must be such that Trustees can make the required assertions relating to risk in the Trust's annual report.

7.9   All senior staff are responsible for encouraging good risk management practice within their areas of responsibility.

7.10   All Trust staff are responsible for complying with internal control procedures as applicable to their role.

7.11   Responsibility for adhering to this Policy, implementing the Procedures and therefore for the identification and evaluation of risks, implementation, and monitoring of risk response plans, is delegated to the Trust's Executive Team for the Trust as a whole, to the Principals for their individual academies and to functional leaders for Trust functional oversight and central support services.

Academy Level Risk Management

7.12   The Principal will be accountable for managing the academy level risks and will have overriding control of the academy risk register and its completion within the academy. However, the Principal may delegate responsibility for ensuring that the risk register is maintained correctly to a senior staff member who demonstrates the appropriate skills and behaviours. This individual will be known as the Academy Risk Champion.

7.13   The Principal should notify the Head of Compliance and Reporting of the name and role of the person who is responsible for performing this task so that appropriate training and support can be provided as necessary.

7.14   Each risk on an academy risk register should be assigned to a member of the academy SLT. This individual will be referred to as the 'Risk Owner'.

7.15   The risk register should be updated on an on-going basis and reviewed as an SLT on a termly basis to provide local oversight of how operational risks are being managed. The risk register should be maintained in line with guidance provided on the instructions tab of the risk register template.

7.16   As mentioned in 5.24, the Principal, in conjunction with the Risk Champion, is responsible for escalating risks to the relevant Executive assigned to that risk. The Head of Compliance and Reporting should also be copied into this email for monitoring purposes.

7.17   The full academy risk register should be shared as part of the LGB paperwork and pre-read by the LGB with any concerns being raised within the LGB. Within the principal report to the LGB, the principals should summarise the top 10 risks at an academy level and highlight all changes between versions including progress made with regard to mitigating actions. The LGB should look for evidence of assurance that the mitigating actions are in place and effective. It is at the discretion of the LGB if they wish to discuss risks in optional sub-committees.

7.18   LGBs should formally review the full academy risk registers annually and review on a termly basis the top ten rated risks and any risks that have increased, decreased, or closed since the previous term.

7.19   Additionally, on an on-going basis, LGB's should support their academy Principal in identification and evaluation of risks by raising any concerns they have with the Principal, particularly relating to risks and risk factors which may be particularly relevant in the context of the academy and its local context.

7.20   If a Governor needs to escalate a certain risk, this should be emailed in the first instance to the Head of Governance with the Head of Compliance and Reporting copied in. This will then be escalated to the appropriate Regional Director, the Trust Risk Champion and the relevant Functional Executive for further investigation and monitoring.

Monitoring of academy risk registers, consolidation, and escalation

7.21   The Risk Champion at each Academy is responsible for sending the reviewed and updated risk register to the Head of Compliance and Reporting on a termly basis. The Head of Compliance and Reporting will feedback and provide challenge, where necessary on the risk register.

7.22   Termly the Head of Compliance and Reporting will then consolidate the top ten rated risks per academy and a consolidated version of this will be presented to the Regional Directors and Executive.

7.23   Termly, a report will be prepared by the Head of Compliance and Reporting and presented to the Audit and Risk Committee, highlighting the key rated risks noted at academy level, and the impact these have, if any on the Consolidated Trust risk register.

7.24   The Audit and Risk Committee will review, for accuracy and completeness, the Consolidated Trust risk register with consideration to assurance provided by external and internal information (e.g., internal audit and external audit report), external risk factors etc.

7.25   The Chair of the Audit and Risk Committee is responsible for presenting the risk register to the Board of Trustees on a termly basis.

7.26   The Board is responsible for reviewing this in detail in the context of performance against strategy on an annual basis.

8. Reporting and Consequences of Non-Compliance

8.1. All Trust staff are responsible for escalating known or suspected instances of non-compliance to appropriate management, ultimately to the policy owner and/ or the Risk Champion.

9. Policy Status

9.1. This policy does not form part of any employee's contract of employment.

10. Related Policies & Documents

10.1. This policy is related to the following other Trust policies:

    10.1.1. Scheme of Delegation (and Decision-Making Framework)

    10.1.2. Records Retention Policy

11. References/ suggested reading

8.1 [The Orange Book (publishing.service.gov.uk)](publishing.service.gov.uk)

8.2 [Assurance mapping: a vital tool | Assurance practical guidance | ICAEW](ICAEW)

8.3 [Academy_trust_handbook_2021.pdf (publishing.service.gov.uk)](publishing.service.gov.uk)

Appendix 1
Risk Management Framework [Source: The Orange Book]

Risk Management Framework
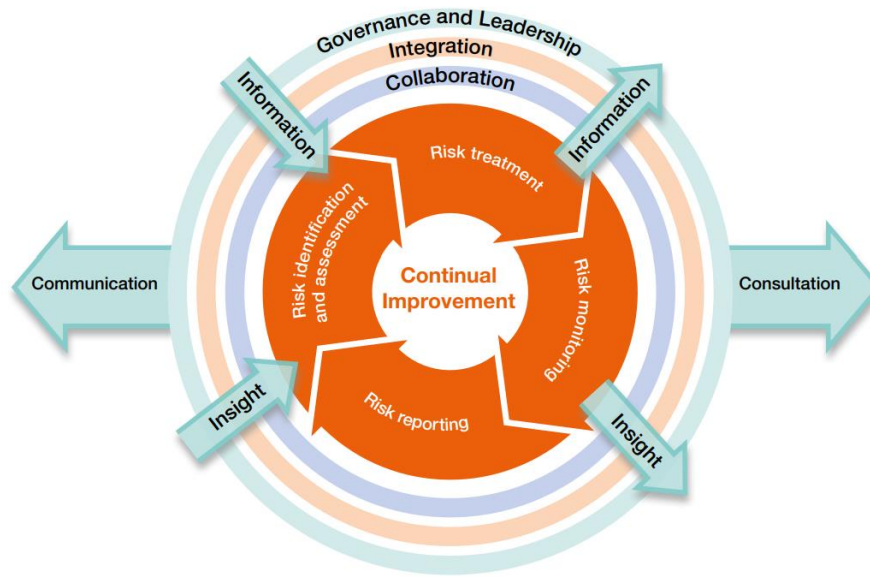
Appendix 2a

4 lines of defence as presented by the ICAEW (Institute of Chartered Accountants of England and Wales)

Line	Consists of:
1	Management policies Control frameworks and controls Management review processes
2	Control self-assessment mechanisms, ie independent of management review processes Risk reviews Compliance reviews Group legal Group insurance Board review processes
3	Internal audit
4	External audit Other independent assurance

Appendix 2b

3 lines of defence as presented in Annex 2 of the Orange Book.
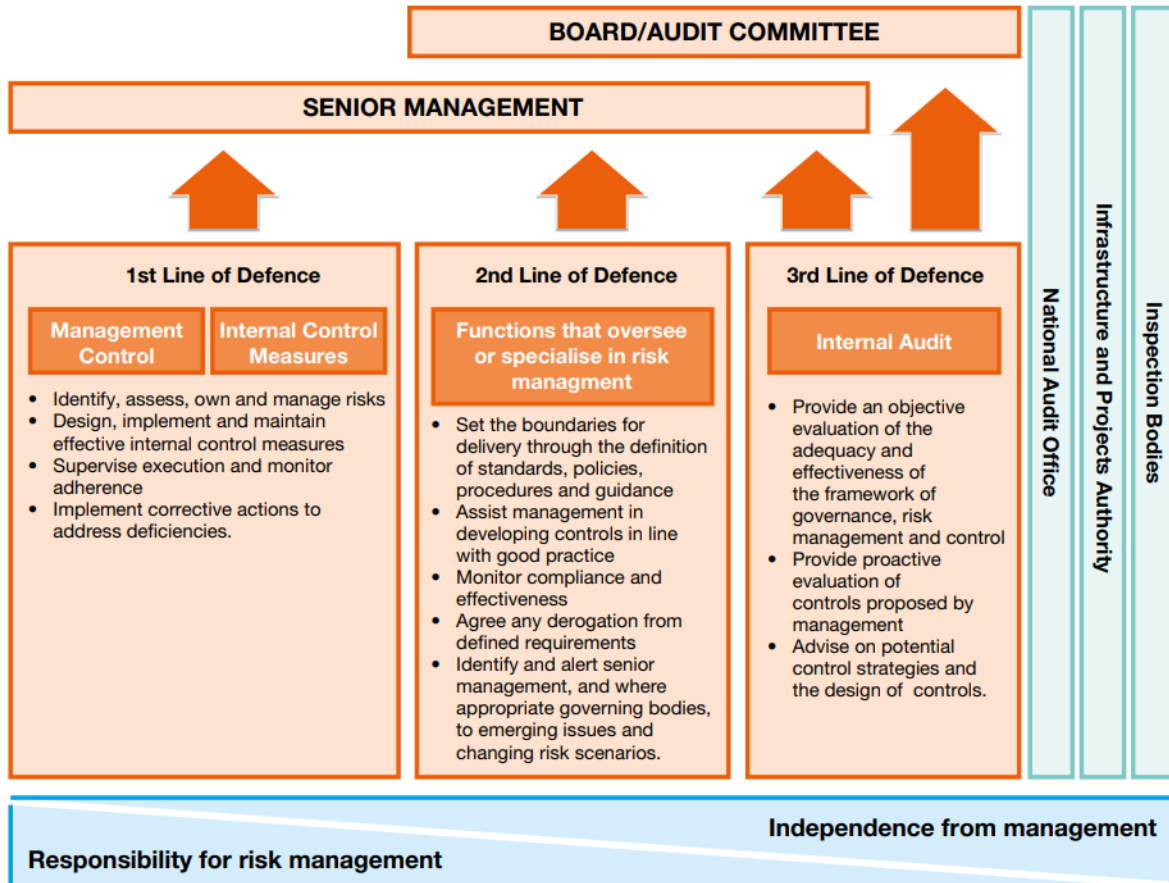
Appendix 3

Risk scoring matrix

		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	**5 Almost certain**	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

1 A standard risk matrix

Appendix 4

Example of a simple assurance map [Source: ICAEW/ technical/ audit and assurance]

	1st Line		2nd Line				3rd Line	4th Line	
	Control Framework	Management Review	Control Self Assessment	Risk and Compliance review	Group Legal	Board Review	Internal Audit	External Auditors	Other Third Party
Financial Reporting	Green	Green	Yellow	Yellow	White	Yellow	Green	Green	White
Financial Controls	Green	Green	Yellow	Yellow	Red	Yellow	Green	Yellow	White
Legal	Orange	Orange	White	Yellow	Green	Orange	Orange	White	White
IT	Orange	Orange	Yellow	Red	Yellow	Red	Orange	White	White
Treasury	Yellow	Yellow	Red	Yellow	Green	Yellow	Red	Orange	White
Tax, Pension and Insurance	Yellow	Yellow	Red	Red	Orange	Orange	Red	Orange	White
Human Resources	Yellow	Red	Red	Yellow	Yellow	Yellow	Orange	White	White
Fraud	Yellow	Orange	Yellow	Red	White	Orange	Orange	Orange	White
Health & Safety	Yellow	Yellow	Yellow	Yellow	Orange	Red	Orange	White	Green

KEY

Green	Yellow	Orange	Red	White
High Assurance	Medium Assurance	Low Assurance	No assurance - but should be assurance in this area	Not Applicable