Ormiston Academies Trust

Risk Management policy

Policy version control

|  |  |
| --- | --- |
| Policy type | Mandatory |
| Author  In consultation with | Natalie Slayman-Broom, Director of Strategy  Jo Dawson, National Director or Finance and Strategy. Claire Lovell, Head of Compliance and Reporting. Sunita Yardley-Patel, Head of Governance Audit & Risk Committee |
| Approved by | Executive team – November 2023 |
| Trust Board approval | December 2023 |
| Release date | December 2023 |
| Review | Policies will be reviewed in line with OAT's internal policy schedule and/or updated when new legislation comes into force |
| Description of changes | * Policy re-written. Treat as new. |

Contents

[1. Policy statement 3](#_Toc151362886)

[2. Scope and purpose 3](#_Toc151362887)

[3. Risk management objectives 4](#_Toc151362888)

[4. Risk management strategy 4](#_Toc151362889)

[5. Roles and responsibilities 5](#_Toc151362890)

[6. Risk management and the link to internal controls 7](#_Toc151362891)

[7. Risk register location 8](#_Toc151362892)

[8. Training 8](#_Toc151362893)

[9. Risk management statement and risk framework 8](#_Toc151362894)

[10. Trust matrix and risk notes 9](#_Toc151362895)

[11. Risk reporting 11](#_Toc151362896)

1. Policy statement
   1. The trust board and executive committee believe that sound risk management is integral to good management and governance. They recognise that risk management must form an integral part of their decision making and their strategic and operational planning.
   2. The members and trust board, supported by the audit and risk committee, are accountable for risk management and for maintaining a sound system of internal control. This system supports the achievement of policies, aims and objectives and the embracing of opportunities, whilst safeguarding against threats to all assets (including human and non-material) for which it is responsible.
   3. The trust board acknowledges that risk cannot be entirely eliminated, however, they hold the CEO to account for putting in place appropriate mitigation to ensure risk is not damaging.
   4. The risk management process informs the agenda setting of the Trust Board and, where appropriate, the Trust’s sub-Committees.
   5. The trust board delegates the function of overseeing risk management to the audit and risk committee. This committee holds the executive to account for ensuring that the trust meets all aspects of statutory compliance. They are aided in this function by internal audit.
   6. The trust board recognises that opportunities to further the trust’s mission will always have associated risks. The trust board recognises that not capitalising on emerging opportunities may, in itself, adversely influence the achievements of the trust.
   7. In managing risks and opportunities, the trust board will assess the appropriateness and strength of plans to manage them. New opportunities will always be discussed, debated, and challenged, and considered in light of the risk capacity of the trust.
   8. This policy is written in accordance with the Department for Education guidance and in line with OAT’s belief that ‘we achieve more together.’
2. Scope and purpose
   1. The policy explains the trust board’s approach to risk and how responsibilities for risk management are delegated. The policy explains how the risk register is created and the way in which it is used by the executive and the trust board to identify, measure, manage, monitor, and report risk.
   2. The trust board has overall responsibility for the risk management process and the CEO has the delegated responsibility for risk management and is supported in this by the executive team.
   3. Risk is managed by everyone daily and school leaders constantly assess situations. The trust board is particularly concerned with risks and opportunities that can have a high impact (positive and/or negative) on the running of the trust and the meeting of its objectives and mission.
3. Risk management objectives
   1. The objectives for managing risk across the trust are:

* To comply with risk management best practice.
* To ensure risks facing the trust and individual academies are identified and appropriately documented.
* To provide assurance to the trust board that risks are being adequately controlled, and / or identify areas for improvement.
* To ensure action is taken appropriately in relation to accepting, escalating, mitigating, avoiding, and transferring risks.

1. Risk management policy
   1. This policy aims to:

* Outline the roles and responsibilities for risk management.
* Identify risk management processes to ensure that all risks are appropriately identified, controlled, and monitored.
* Ensure appropriate levels of training and awareness throughout the trust.
  1. In its annual consideration of the risk register, the Trustees should consider:
* The effectiveness of the overall approach to and policy for risk management and whether changes or improvements to processes and procedures are necessary.
  1. As part of the review, the following should be considered:
* Whether the policy effectiveness could be improved to further meet the needs of the trust.
* Whether risk management continues to be linked to the achievement of the trust’s objectives.
* Whether risk review procedures cover fundamental strategic and reputational, operational, compliance, financial and other risks to achieving the trust’s objectives.
* Whether risk assessment and risk-based internal control are embedded in on-going operations and form part of its culture
* Whether there have been changes in the nature and extent of fundamental risks and the trust’s ability to respond to changes in its internal and external environment since the last assessment
* The scope and quality of management’s on-going process of monitoring the system of internal control, including such elements as the effectiveness of assurance functions.
* The extent and frequency of reports on internal control to the trust board and whether this is sufficient for the trust to build up a cumulative assessment of the state of control and effectiveness of risk management.
* The incidence of any fundamental control failings (risk events) or weaknesses (near misses) identified at any point within the year and the impact that they have had or could have on the trust.
* The effectiveness of the trust’s public reporting processes

1. Roles and responsibilities
   1. The trust board, being the principal policy making body, has overall accountability for managing risk. They:

* Consider the tone and culture of risk management within the trust.
* Determine the appropriate risk appetite and whether the trust is “risk taking” or “risk averse” at any given time in relation to capacity. The risk register will support this judgement and a decision will be taken as to whether the trust has the capacity to manage further risk, or, if by not taking an opportunity, a risk is presented (e.g., growth)
  1. Additionally, the trust board determines which risks are acceptable and which are not. To achieve this, the trust board will:
* Set and regularly review the trust’s approach to risk management and the risk appetite. It will communicate this approach (and any changes).
* Set standards of conduct expected of staff, including associated behaviours, and ensure all aspects of compliance are adhered to.
* Set and approve the framework for managing risk, including the key categories of risk.
* Approve major decisions affecting the organisation’s risk profile or exposure.
* Ensure risk management is included in the development of business plans, budgets, projects, and programmes and when considering strategic decisions.
* Satisfy itself that fundamental risks are being effectively managed and there are clear lines of accountability.
* Provide oversight of risk identification, management, and mitigation within the organisation, monitoring the management of fundamental risks through the audit and risk committee, external consultants, and any other relevant parties, and making recommendations as required.
  1. The audit and risk committee takes responsibility for reviewing the effectiveness of financial and other risk management activity within the trust in detail. In doing so, it supports the trust board through oversight of financial and other controls, escalating key risks to the Board for further review as required. To achieve this, members of the sub-committee will:
* Understand the trust’s business strategy, operating environment, and associated risks.
* Understand the framework for risk management and assurance.
* Critically challenge and review the risk management and assurance framework and all controls.
* Understand how risks and opportunities support the key business objectives and the trust’s mission.
* Work with the executives in identifying annual internal audits in relation to risk.
* Review the risk register at every meeting.
* Recommend any amendments of the risk register to the trust board and authorise who is overseeing the risk register from the executive.
* Focus on the top-10 risks faced by the trust at every meeting and review the update from the Executive.
* Review the full register and compliance on an annual basis.
  1. The sub-committees to the trust board take responsibility for monitoring risks pertaining to their own area of responsibility per the terms of reference for each committee.
  2. The CEO is the accounting officer and has delegated responsibility for risk management. In conjunction with the executive team, the CEO is responsible for:
* Evaluating and reporting to the trust board whether the trust values, leadership style, opportunities for debate and learning, and human resources policies support the desired risk culture, incentivise expected behaviours and sanction inappropriate behaviours.
* Anticipating and considering emerging risks.
* Assessing the likelihood and impact of existing and potential key risks.
* Implementing corrective actions in response to significant risks, learning from any previous mistakes, and ensuring any business continuity plans are sufficiently robust to cope with high level risk.
* Engaging senior managers in the assessment and recording of risks.
* Delegating oversight of risk management and reporting to the audit and risk committee on an annual basis to a member of the executive team.
* Ensuring the responsible executive has adequate resources, including access to training.
* Ensuring the expected values and behaviours are communicated and embedded at all levels of the trust through regular training.
* Ensuring risk is an integral part of appraising option choices, evaluating alternatives and making informed decisions so that risk management is integral to all decision making.
* Accurately reporting to the audit and risk committee and the trust board on current and future risk.
* Producing a report for the trust board four times a year that addresses the top current and future risks identified by the Executive, supported by the audit and risk committee.
* Ensuring the language of risk management is used at every level of the trust and that risk management is part of the trust’s culture, not an add-on process.
  + 1. Where there is a disagreement with regards to the scoring of risk, or any related matter, at an executive level this should be escalated to the chair of the audit and risk committee – this can be actioned by either the CEO, a member of the executive team or a member of the governance and compliance teams.
  1. The director of strategy:
* The director of strategy has overall responsibility of the maintenance of the corporate risk register and leads on the engagement of ongoing risk oversight and quarterly reviews of the corporate risk register.
* They are responsible for updating this policy.
* They will work with the executive team to escalate breaches of risk limits immediately to the trust board.
  1. Internal committees:
* Internal committees take responsibility for reviewing risks under their remit and discussing these regularly ahead of the quarterly updates.
  1. Risk owners:
* Individual risk owners will be identified by the executive team, based on their area of expertise and risks that fall within their day-to-day management. The corporate risk owners will primarily be made up of Executives and Trustees. They will be responsible for:
* Supporting the process of identification, mitigation and reporting of risks in line with agreed systems and timelines
* Escalation of risks in line with organisational processes
* Updating their risks ahead of the quarterly risk meetings
  1. Head of reporting & compliance:
* The head of reporting & compliance is responsible for monitoring the overall risk process and managing the interdependency between this and work performed around process and controls improvement together with internal audit plans.
  1. Head of governance:
* The head of governance is responsible for ensuring that risk management is built into governance at all levels via standard agendas, governance calendars and associated training.
  1. The local governing body:
* Inviting the principal to start the meeting by highlighting the academies main strategic priorities and any risks that may prevent the academy from delivering these and it’s mor detailed academy development plan.
* Considers the main risks faced by the academy and how those are being managed, by reviewing the full academy risk register annually and reviewing the top ten rated risks and any risks that have moved (increased, decreased or closed) since the previous review, on a termly basis.
* Reviews safeguarding data at every meeting and challenges safeguarding procedures.
* Scrutinise the annual external safeguarding review.
* Has a named governor for safeguarding.
* Review other compliance information, such as Health and Safety information, as appropriate.
* Scrutinise the annual external safeguarding review.
  1. Academy principals, supported by operations, finance leads and business managers, are responsible for:
* Implementing policies on risk management and internal control at a local level.
* Identifying and evaluating fundamental risks faced by their institution.
* Assisting the executive team and internal auditors to undertake reviews of risk management and the effectiveness of the systems of internal control, where appropriate.
* Keeping informed, and escalating any risks to the Executive, allowing them to be accessed and communicated as appropriate.
* Embedding risk management as part of the systems of internal control.
* Ensuring the school’s SLT is reviewing and updating the risk register on an ongoing basis.
* Sharing the risk register with the head of reporting & compliance and education directors on a quarterly basis for feedback.
  1. Where there is a disagreement with regards to the scoring of a risk or any related matter, this should be escalated to the executive responsible for risk to resolve.

1. Risk management and the link to internal controls

* The trust’s system of internal control incorporates risk management. It encompasses various elements that, together, facilitate an effective and efficient operation, enabling the trust to respond to a variety of risks.
* Attached to fundamental risks, are a series of policies that underpin the internal control process. The policies are reviewed by the trust board. Written procedures support the policies where appropriate.
* Risk owners are expected to monitor, manage, and mitigate identified risks on an ongoing basis. In doing so they will be guided by adherence to organisational policies and managerial oversight. The risk owner must assess all risks. Any risks scored at a rating of 13 or above must be escalated to the Executive as soon as they are identified.
* The trust board will receive further assurance through the external audit processes including reviews of probity, and effectiveness of internal controls.
* Each risk should have assigned internal controls or plans within the mitigating actions to implement internal controls. It is the responsibility of the risk owner to check at least once a year that these controls are sufficient and effective. The internal audit function sits within the remit of the head of reporting & compliance who reports into the CFO.
* Every academy within the trust must hold its own risk register. This must be always kept updated and available to the executive team. The responsibility for this lies with the principal, although principals may delegate the updating of the register to a member of their SLT. Principals will discuss the register formally with their line-manger on a quarterly basis and at any point where there is a need for an update. Principals should proactively flag any emerging risks to the relevant function as appropriate. Education directors should proactively support principals to mitigate any emerging risks – this includes collaborating with other functions as appropriate.

1. Risk register location
   1. The executive risk register for the trust is located on GovernorHub (Quarterly update). A life copy is maintained on the OAT central teams’ site and accessible by the relevant members of staff.
   2. The risk registers for each academy should be located on GovernorHub.
2. Training
   1. Any new member of staff must undergo risk training as part of their induction.
   2. New senior managers must undertake training on the evaluation, recording and escalation of risks as part of their induction.
   3. To ensure that all principals understand their responsibilities, they will be supported to effectively manage risk with training provided as needed.
   4. Responsibility for ensuring that appropriate training is provided sits with the executive, supported by internal auditors and the head of governance. The training for the risk management framework is a key part of this policy and the procedures for the trust.
3. Risk management statement and risk framework
   1. The organisation will maintain a risk register covering key corporate risks, which will be updated each quarter. The detailed register considers risks according to the following categories:
      1. Strategic e.g., growth/pupil numbers and demographics; strategic planning.
      2. Compliance and regulatory risk e.g., introduction of new legislation.
      3. Financial (incl. liquidity) risk e.g., inflation, interest rates.
      4. Operational risk e.g., breakdown of normal ways of working (Health & Safety, Information, Data & Technology (Cyber, GDPR), governance, processes, and people management).
      5. Reputational e.g., education quality and standards; safeguarding; student experience; stakeholder management.
   2. Whilst the full risk register will be available to the trustees, a summary of key risks will be presented to the audit & risk committee and trust board. It is the responsibility of each sub-committee of the trust board to monitor the detailed risk register for any emerging risks and flag these to the trust board if these are not included within the summarised risk register.
4. Trust matrix and risk notes
   1. Risks are assessed in terms of likelihood and potential impact. The risk register includes relevant risk mitigation and actions required and records the resulting retained risk. At each review, trustees consider the level of retained risk and decide whether this is acceptable. All major projects must include consideration of the key risks involved and will be expected to have their own risk register.
   2. Risks are scored in the following way:

* provide a score of 1-5 for the perceived impact of the risk (I)
* provide a score of 1-5 for the likelihood that it happens (L)
* multiply the two numbers together to create a risk rating (IxL)
* add the weighting of Impact to ensure this is differentiated enough (+P)
  1. 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 | Event is expected to occur less than once in 100 years. |
| 2 | Unlikely | Event may occur once in 50 years. |
| 3 | Possible | Event is likely to occur once in 10 years. |
| 4 | Likely | Event is likely to occur once every few years. |
| 5 | Almost certain | Event is likely to occur multiple times within a year, indicating a persistent issue. |

* 1. Impact should be considered by sub-entity (i.e., academy, function, programme) in addition to trust level, as the sum of many small risks can result in a significant risk at trust level.
  2. Assessment should follow the guidance below noting that this is guidance only and other factors should be considered as appropriate.

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | No consequence | | |
| 2 | Financial net impact of less than 0.2% of turnover or £0.5m for trust level risks. *For academies – please use 0.2 % of local academy turnover.*  No other significant impacts. | | |
| 3 | Financial net impact of less than 0.2% of turnover 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. | | |
| 4 | Financial net impact of 0.2% - 0.5% of turnover or £1.25m for trust level risks. *Academies – use 0.2 – 0.5% of local academy turnover.*  Addressable regulatory consequences.  Adverse publicity in national newspapers.  Major injury. | | |
| 5 | Financial net impact of 1% of turnover or £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. | | |
| **Score** | | **Risk description** | **Action requirement** |
| 17-25 | | High risk | Risk will be actively managed with control measures |
| 11-16 | | Medium | Take appropriate action to reduce risk if possible |
| 10 and below | | Low risk | Risk has low priority and actively monitored |

* 1. The risk response is based on the rating. The following two responses are used:

**TREAT** – specific action is required to contain the risk to an acceptable level.

**TOLERATE** – exposure to risk may be tolerated without any further action.

Each element of risk will be reviewed, and updated where relevant, on a 3-monthly basis.

The risk register will form a standing agenda item at all trust board meetings. The risks will be highlighted on an exceptions’ basis, and these will be presented to the relevant meetings as appropriate.

The members and trustees of OAT are accountable for all risks. Additionally, the risk register states who the identified “risk owner” is, to identify roles within the governance structure.

1. Risk reporting
   1. OAT’s committees will regularly review their agreed risks as a standing agenda item, paying particular attention to the internal controls and risk scoring. This review will help to inform quarterly risk review meetings and help drive the agenda for the committee, particularly for risks that are showing higher than tolerance levels.
   2. The trust board will have a standing agenda item at each meeting on the risk review and each committee will review the corporate risks assigned to them as outlined in their terms of reference at each meeting.
   3. A risk review will be a standing agenda item at the audit and risk committee. The committee will review both the risks relevant to them as stated in the terms of reference, and general oversight of all the risks.
   4. Risks that breach their limit will be escalated immediately to the trust board via email with an explanation of the risk, the breach of tolerance and the mitigating actions being taken to bring back down within tolerance.
   5. All risks other risk metrics that remain within tolerance and guidelines will be tracked and monitored by the trustees through the risk review and risk appetite RAG-rating.