ODBST Risk Management Policy

ODBST Level 1 Statutory Policy:	**ALL** Schools require this policy with **no changes** allowed to core text. No changes are necessary to personalise this with school name and branding, as this is a Trust level policy for use, without change, by all schools, **except** where a school contact is required as identified in the content of the policy. LGBs will **note** adoption in LGB meetings. Review will take place at Trust level, and schools will be notified of updates and review dates as necessary.
Other related ODBST policies and procedures:	
Committee responsible:	FRAPP
Approved by:	FRAPP
Date Approved:	7th February 2024
Review Date:	Spring term 2027

Risk Management Policy

Risk is inherent in everything academy trusts do to deliver high quality services. Risk management is an essential part of governance and leadership and an integral part of business planning and decision-making processes. ODBST considers risk management in terms of the ICAEW four lines of defence concept:

- **1st line of defence** – management and staff who own and manage risk on a day-to-day basis.
- **2nd line of defence** – the board who oversee the effectiveness of the risk management framework.
- **3rd line of defence** - the internal scrutiny function who provide independent assurance on the overall effectiveness of risk management and controls.
- **4th line of defence** - assurance from external independent bodies such as the external auditors and other external bodies.

It is a requirement of the Academies Financial Handbook (AFH) that:

- Academy trusts must manage risks to ensure their effective operation and they must maintain a risk register (part 2).
- The trusts management of risks must include contingency and business continuity planning (part 2).

ODBST Risk Register Requirements

All ODBST Schools must have a Risk Register which is reviewed and updated at least once a term. The local governing body must review and agree the register *at least annually*. Each term a copy of the school's risk register must be sent to the ODBST Chief Operating Officer so the risks can be understood. All schools must use the format given to them by the Trust.

1.What is Risk Management?

Risk management involves the identification, measurement, management, monitoring and reporting of threats to an academy trusts business objective. Such threats can arise from a wide variety of sources such as litigation relating to safeguarding failures, financial uncertainty from a falling roll, security risk from inappropriate access to data, property risk from fire or flood, accidents resulting in injury, natural disasters, and of course a global pandemic. School leaders identify risks and implement appropriate mitigating control measures as part of normal business, for example managing the risks associated with school trips.

Risk management is not about adding new processes, but ensuring processes are integrated in the management and operation of businesses. Effectively managing risk informs business decisions, enables a more effective use of precious resources, enhances strategic and business planning and strengthens contingency planning.

Trust has responsibility for overseeing risk management within the institution as a whole. The oversight of the risk register, lies with the ODBST's Board of Trustees, the board has appointed the Finance Resource Audit Pay and Personnel (FRAPP) committee to coordinate this work in accordance with the Academy Financial Handbook (part 3) to:

- direct the trust's programme of internal scrutiny
- ensure that risks are being addressed appropriately through internal scrutiny

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

The Trust carries out this responsibility through its Senior Leadership Team and Trustee board meetings. The ODBST has identified the Chief Operating Officer as being responsible for risk management on a day-to-day basis. However, the Trust-wide risk register is reviewed and updated on a monthly basis and it is a standing item of all Committees.

The policy should be read alongside the ESFA good practice guide on internal scrutiny and reference can be made to the publication The Orange Book - Management of Risk - Principles and Concepts helpful, in particular page 38 which provides examples of risk categories.

2. Steps to developing a risk management process

2.1 Risk Framework

Risk management processes follow steps shown in the diagram and combine to make up an overall risk framework. It is important to take a balanced view to managing opportunity and risks, to make the process meaningful.

Academy trust risk management framework

2.2 Identification

At the risk identification stage, all potential events that are a threat to the achievement of business objectives (including not capitalising on opportunities) are identified, defined and categorised. To get maximum benefit from this stage if risks are identified in a "top-down" as opposed to "bottom up" way. Events that appear to be negative, but which do not have any direct impact on business objectives, may not be risks at all.

To ensure all major risks are identified it is helpful to consider the various types of risk and there are several different ways to categorise them. Understanding the type of risk being faced can also help determine what action is best to take. A common approach is to consider risks under the following categories:

- **Internal risks** - these are risks over which the academy trust has some control, by managing them through internal controls/ additional mitigating actions. Examples of such risks include health and safety risks, data security.
- **External risks** - this focuses on big external events/perils and then considers how to make the academy trust more resilient to such events. Examples of such risks include a pandemic and extreme weather.
- **Strategic risks** – these are risks to the achievement of the academy trust's core objectives. For example, the risk of high staff turnover.
- **Project risks** – risks associated with any critical projects the academy trust may be involved in. For example, slippage on the delivery timescale for a new building.

Whilst risk management assessment at board level will focus on the highest priority risks, which will have the greatest impact on the trust, there is also a need for school leaders to assess operational risks. In a trust with multi academies, local governance can play an important role in working with the trust leadership team to identify these risks and ensure plans are in place to minimise any impact on the academy trust and its pupils. The (Finance Resource Audit Pay and Personnel) FRAPP committee's role is to oversee that all categories of risk are identified and must extend to ensuring the risks at constituent academies are being assessed and addressed appropriately.

2.3 Measurement
Once risks have been identified it is important to measure them to give a standard for comparing the risks consistently. Measurement consists of assessment, evaluation, and ranking.

The aim of **assessment** is to understand better each specific instance of risk, and how it could affect business objectives. ODBST and its academies should estimate:

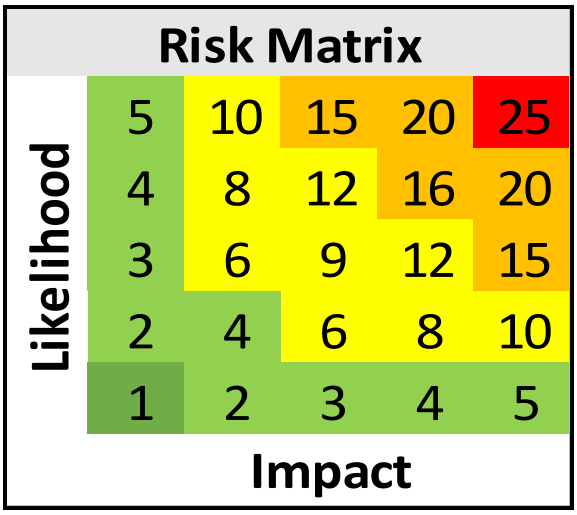
- the likelihood (or probability) of it occurring, and
- the impact (or severity) if it did occur

There are various ways to assess likelihood and impact. AT ODBST a scoring approach should be used, using a range of 1 to 5 for each. For example, a score of 5 for likelihood would denote an extremely likely event and 5 for impact would denote a critical level of damage.

Evaluation: the "r scores" for each risk's likelihood and impact respectively are combined to derive a single risk score reflecting its overall level of threat. Risks could be evaluated using a range of 1 to 5 would generate a numeric score with the minimum being 1 (1x1) and the maximum being 25 (5x5).

Ranking: once the scores for likelihood and impact have been combined into a single risk score, they can be plotted on a risk matrix. The matrix is simply a grid showing high likelihood/high impact risks to the upper right and low likelihood/low impact risks to the lower left.

ODBST Risk Tolerance Grid



Colour key when you compare likelihood against impact

Red: critical risk
Amber: high risk
Yellow: medium risk
Green: Low risk

Schools should be aware that risks which are of very low likelihood and very high impact will be ranked in the same position as a risk with very high likelihood and very low impact. However, as the former could be catastrophic for the trust, if realised, they should be prioritised accordingly.

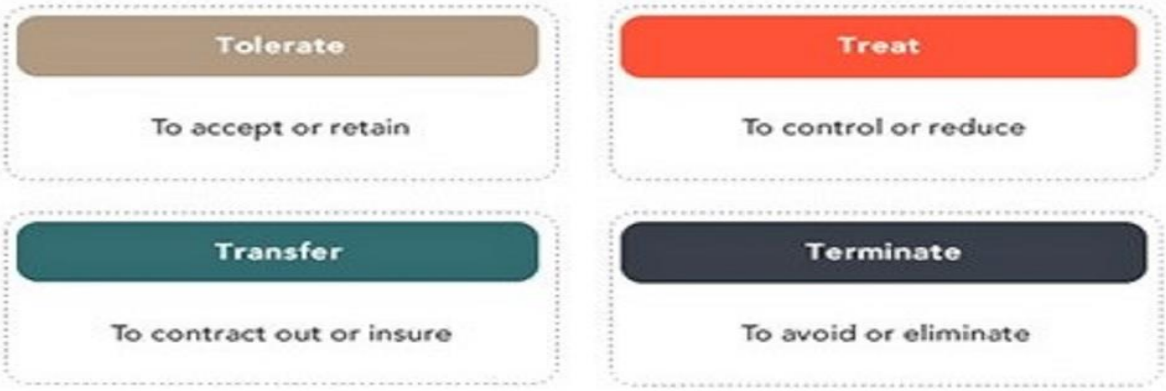
ODBST also uses a traffic light system (sometimes called a RAG-rating) for an intuitive representation of the ranking of risks. The matrix also provides a reference for the risk register to identify which risks fall outside the academy trust's level of tolerance, based on its risk appetite, and which need to be managed actively.

2.4 Management (control)
Once risks have been assessed, evaluated and ranked, appropriate plans to manage them are required. These plans include preventative controls, mitigation processes and contingency plans, if risks materialise. The approach taken will depend substantially on ODBST and the School's risk appetite and risk capacity:

- **Risk appetite** – the amount of risk the academy trust is willing to accept in the pursuit of its objectives
- **Risk capacity** – the resources (financial, human, and so on) which the academy trust is able to put in place in managing risk

Once the risk tolerance and capacity have been decided, a risk control strategy needs to be made. One easy-to-follow approach is to consider the **"4 T's"**. Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits from the achievement of objectives against the costs, efforts, or

disadvantages of proposed actions.



Academy trust risk tolerance grid

- **Tolerating** risk is where no action is taken. This may be because the cost of instituting controls is not cost-effective or the risk or impact is so low that they are considered acceptable. For instance, the academy trust may decide to tolerate the risk of contracting with a supplier with a poor credit rating provided the goods/services could be obtained relatively easily from someone else.
- **Treating** risk involves controlling it with actions to minimise the likelihood of occurrence or impact. There may also be contingency measures to reduce impact if it does occur. For instance, an academy trust may decide to train more than the statutory minimum of staff as paediatric first aiders and to put in place a rota for first aid cover during lunchtimes.
- **Transferring** risk may involve the use of insurance or payment to third parties willing to take on the risk themselves (for instance, through outsourcing). An academy trust may decide to take out insurance to mitigate the risk of the excessive costs of supply staff in the event of extended staff absences.
- **Terminating** risk can be done by altering an inherently risky process to remove the risk. If this can be done without materially affecting operations, then removal should be considered, rather than attempting to treat, tolerate or transfer. Alternatively if a risk is ranked highly and the other potential control measures are too expensive or otherwise impractical, the rational decision may well be that this is a process the academy trust should not be performing at all. For instance, an academy trust may decide not to contract with a related party to eliminate reputational risk.

There is also a fifth **“T”**, **“take advantage”**, in recognition that the uncertainty attached to risk sometimes offers opportunities as well as threats.

2.5 Monitoring

Monitoring should be ongoing and continuous as this supports understanding of whether and how the risk profile is changing. Monitoring also provides assurance on the extent to which the mitigating actions and controls are operating as intended and whether risks are being managed to an acceptable level.

The risk register is central to risk monitoring. As risks are identified, they should be logged on the register and the associated control measures documented. A risk register should be a ‘live document’ and should be an on-going process. Risk registers come in various formats and no particular version is recommended.

However, some elements should always be included.

- **Risk category** – risk should be categorised under, for example, IT, finance, HR, premises to facilitate their effective management. Categorisation helps tease out other likely risks as well as potential duplication.
- **Risk description** – a brief description of the potential risk, namely the event itself, for example "a cyber-attack on the trust's IT systems" and its consequences "students cannot access their saved work".
- **Risk ID** – a unique number used to identify and track the risk.
- **Business objective threatened** – a description of the relevant business objective that the risk would affect if it materialised.
- **The estimated likelihood that the risk will occur**. This should be scored using the number method.
- **The estimated impact of the risk if it materialised**. This too should be scored or assessed
- **The gross risk score** - this is the combined score of the estimated likelihood and impact, without control measures being implemented. It is also known as the inherent risk.
- **Control measures** – which of the risk treatment option(s) (the T's) have been opted for and the rationale for the decision. Also, what the proposed actions are, including timescales for implementation and resources required.
- **The net risk score** – the risk that remains after control measures have been put in place. This is essentially a re-assessment of likelihood and impact assuming that control measures are in place. It is also known as the residual risk.
- **Risk ranking** – this is the overall level of the residual risk, it reflects its position on the risk matrix and, if appropriate, its "traffic light" rating. It may be helpful to use a series of arrows to indicate the direction of travel of the risk ranking after each review i.e. up, down or static.
- **Risk trigger** – what is the event that would trigger implementation of contingency plans?
- **Contingency plan** – an action plan to address the risk if it does materialise and what plans are in place to mitigate the risk. It is a requirement of the AFH (part 2) that the trust's management of risks must include contingency and business continuity planning.
- **Risk owner** – the person responsible for deciding whether the risk trigger needs to be activated and managing the control measures and contingency plans. This should always be in identifiable individual who will ensure effective communication where necessary.
- **Date of last review** – this is an indication of when the audit and risk committee or the board last reviewed the risk. It may be that the risk climate has changed, and the risk level is of a sufficient level that it can be retired from the register. A date supports regular monitoring of risk.
- **Current status of risk** – this should include any comments that will support the review of the risk at the appropriate time.
- **Risk retired date and rationale for retiring risk** – this is an important element as it is an audit of any risks that have been considered by Trustees and later retired with the rationale. These can be hidden from any live document but should still be recorded.

2.6 Reporting and scrutiny

Risk information should be clear and provide key information on the significant business risks. The information should support ODBST in assessing whether decisions are being made within their risk

appetite, to review the adequacy and effectiveness of internal controls, to reprioritise resources, improve controls and to identify emerging risks.

For this process to be effective it is important that the number of risks reported is a manageable number. If too many risks are reported the process may become more difficult to manage and may lose focus.

Local governing bodies review of the risk register should be at least annual as required by the AFH (part 2).

Risk management is as much about ensuring that the control environment remains effective to manage the risks that are already known, such as through testing of the controls. Risks will materialise if controls only exist on paper.

3. Common pitfalls

- **Reporting too many risks**: academy trusts can fall into the trap of tracking too many risks or ones that substantially overlap. The board should clarify the number of risks they are able to oversee, maybe prioritising their "top 10". Other "divisional" risks may be delegated and managed locally?
- **Ignoring known risks**: risks are sometimes ignored because of organisational politics or the preferences of a dominant personality. Are you ignoring the elephant in the room because of an issue?
- **Overreliance on subjective judgement**: one person's risk is another person's opportunity and individual perceptions influence the way risks are assessed. Potential risks should be discussed with the aim of reaching a common understanding of what they are and how they should be dealt with.
- **No real buy-in at a senior level**: the person who administers the risk management framework may not have the seniority to have an impact or the capacity to fulfil the role effectively. As a result, risk management may not get the required attention and the process may decline into a tick-box exercise. Academy trusts should ensure that the person appointed is sufficiently senior to have adequate influence and has sufficient time to dedicate to the role, and/or designate one of the trustees as their "risk champion". The FRAPP committee role is to ensure the risk management framework in place is effective.
- **Risks not linked to strategic objectives or only captured bottom-up**: commonly risks are captured from the bottom up and this can leave them disassociated from strategic objectives. As a result it may be almost impossible to see what impact risks are going to have on the academy trust's goals at a higher level. Although ultimate responsibility for risk management lies with the board, everyone in the academy trust has a role to play in identifying risks to business goals.
- **Over-complexity**: endless discussions about methodology and terminology, which leave no time left to address the risks themselves, are symptomatic of an over-engineered approach
- **Not using the output**: it has been said that all management is risk management. Whether or not this is so, organisations that put the review of risks as the last item on meeting agendas run the risk of an unexpected event having a significant negative impact on a business-critical system. Furthermore, good risk management will inform a sound programme of internal scrutiny reviews, which should focus on areas of risk.

Appendix A

What should be considered?

1. **External risks** - exist outside of the school/trust and are largely beyond the organisation's control.
2. **Internal Risks** - exist inside the school/trust and arise during normal operation
3. **Governance specific risk** - can be external or internal. They relate to the ability and capacity of the governing board to provide robust accountability, oversight and assurance for the performance of the school/trust.

External Risk

Types of risk	Examples
Economic	funding conditions and allocations n rising costs
Political	• a change of government • policy or political landscape
Social	• pupil demographic change • changing social climate
Technological	• obsolescence of externally sourced IT equipment/services • changes to technological requirements
Legal	• changes to the law • consequences of non-compliance
Environmental	• pandemic • transport infrastructure

Internal Risk

Type of risk	Examples
Strategic	• clarity of vision • capacity to plan effectively
People	• recruitment and retention • moral
Compliance	• effectiveness of adopted policies • procedures and the management of compliance
Operational	• premises management • technological failure • cyber attack

Governance Risk

Types of Governance risk	Examples
Recruitment	• recruiting for defined skill sets • recruiting from diverse backgrounds
Structural	• issues arising from size and constitution • delegation of function
Competency	• understanding of roles and responsibilities • effective leadership of the board
Support	• clerking/governance professional arrangements • external advice, support and training
Relationships and behavioural	• Commitment • working relationship between the governing board and headteacher