Education & Skills
Funding Agency

Guidance

Academy trust risk management

Updated 31 July 2019

Contents

1. What is risk management?
2. Steps to developing a risk management process
3. Common pitfalls
4. Conclusion
5. Acknowledgements

1. What is risk management?

Risk management involves the identification, measurement, management, monitoring and reporting of threats to an organisation's business objectives. Such threats could arise from a wide variety of sources, including financial uncertainty, IT security, management errors, accidents, natural disasters, and so on.

We all manage risk on a daily basis: thinking about what we want to achieve, assessing the likelihood of it happening, what might stop it from happening, and, if things go wrong, how big the "loss" might be. The discipline has reached its peak in financial services where fund managers take informed gambles on what might happen to investments and whether it is worth hedging against loss. Unfortunately, much risk management language has been so highly influenced by this legacy that it can seem abstract, but it does reinforce an important feature of risk management: it concerns the maximisation of gain as much as the minimisation of loss. Risk elimination can lead to the elimination of reward too, either by the total avoidance of exposure or the prohibitive cost of prevention. Nevertheless, school leaders identify risks and chose appropriate mitigation approaches as part of normal business, whether this is to do with developing plans for dealing with an influenza pandemic, school trips or even something as mundane as keeping pupils off the playing fields during wet weather.

2. Steps to developing a risk

management process

Risk management plans may differ in terms of sophistication, with many academy trusts having developed a risk management policy that informs the plan, but most follow broadly the same steps that combine to make up the overall framework:

Academy trust risk management framework

2.1 Identification

At the risk identification stage, all potential events that could adversely influence the achievement of business objectives (including not capitalising on opportunities) are identified, defined and categorised[1]. This is best done as a joint effort and with the focus on things that could adversely affect business objectives and so academy trusts may 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.

2.2 Measurement

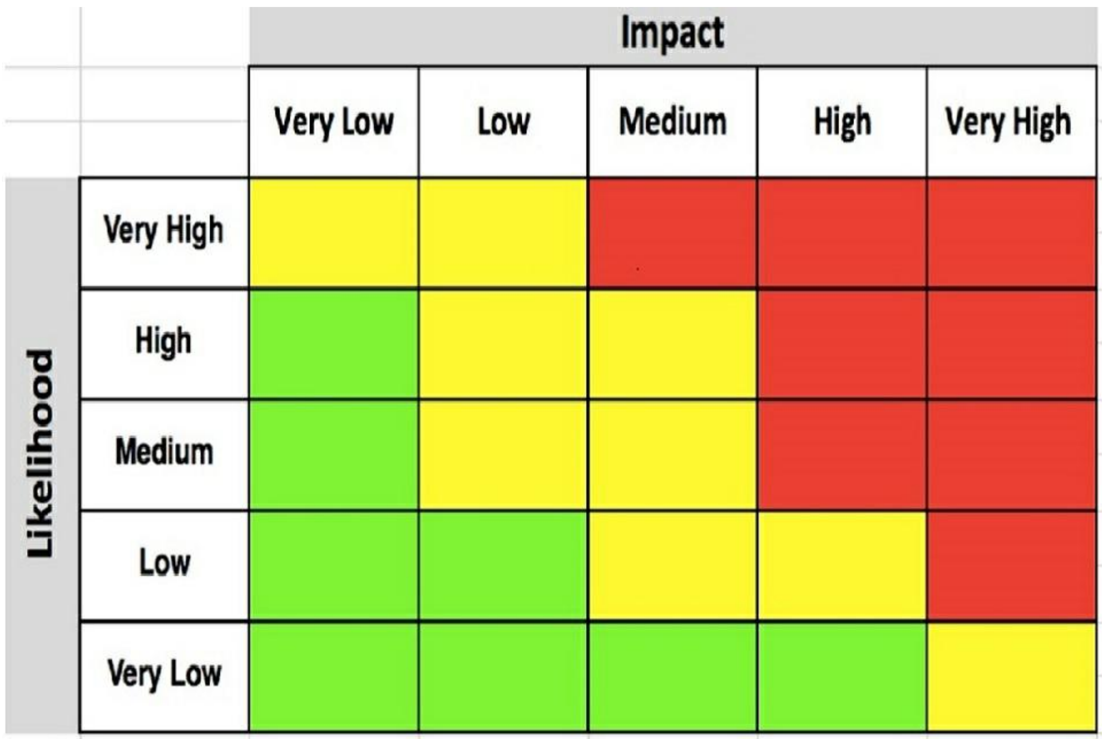
This consists of assessment, evaluation and ranking:

- The aim of **assessment** is to understand better each specific instance of risk, and how it could affect business objectives. Academy trusts 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, but, in an education context, a rational approach could be to simply assess each on a H/M/L scale

- **Evaluation**: the combination of the respective scores for each risk's likelihood and impact respectively to derive a single risk score reflecting its overall level of threat. Risks could be evaluated as H/H, H/M, L/H and so on
- **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



Academy trust risk matrix

It is common practice to use 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 your risk register to identify which risks fall below the academy trust's level of tolerance, and which need to be managed actively.

2.3 Management (control)

Once risks have been assessed, evaluated and ranked, academy trusts will need to ensure there are appropriate plans to manage them. These plans include preventative controls, mitigation processes and contingency plans in the event that risks materialise. The approach taken will depend substantially on the academy trust'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

Consideration of these factors may generate disagreement owing to differing views of risk, so it is important that discussion involves debate and challenge. Trustees may feel more comfortable when there is greater control of risk, but the academy trust's resources and capacity must determine controls. Excessive control may be stifling as well as expensive and controls and resources will directly affect how assured trustees feel about risks. For instance, trustees may prefer that the risk of inappropriate procurement would be reduced by having every purchase order over £100 signed off by the accounting officer, but would this be the most appropriate use of the time of the most highly paid member of staff in the academy trust, especially if effective and cheaper alternatives exist?

Once the academy trust has established its risk tolerance and capacity, it can move onto developing a risk control strategy. Again, there are various ways to do this and no one way is "right", but one easy-to-follow approach is to consider the **"4 T's"**:

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, academy trusts may decide to end an established after school club if it is impractical to get suitably qualified staff to cover it

Some risk experts suggest a fifth “T”: “take advantage”, in recognition that the uncertainty attaching to risk sometimes offers opportunities as well as threats. For example, the risk that 30 pupils apply for a place on a residential trip when the academy trust has only reserved 25 places. In such cases, it may be logical to maximise the likelihood of the risk and to “mitigate” the consequences, for example, by contacting other schools to see if they have any untaken places.

2.4 Monitoring

The risk register (sometimes called a risk log) is central to risk monitoring[2]. As risks are identified, they should be logged on the register and relevant control measures documented. Risk registers come in various formats and no particular version is recommended. However, some elements should always be included:

- Risk category – does each risk fall under the category of IT, finance, HR, premises, and so on? Categorisation helps tease out other likely risks as well as potential duplication
- Risk description – a brief description of the potential risk, i.e. the event itself rather than its consequences
- 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 could be scored H/M/L (as above) or using another method
- The estimated impact of the risk if it materialised. This too should be scored.

- Risk ranking – this is the overall magnitude or the level of the risk. It is a combination of likelihood and impact and so reflects its position on the risk matrix (as above) and, if appropriate, its “traffic light” rating
- Control measure – which of the 4Ts we have opted for, and why
- 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[3]
- 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
- Residual risk – 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

2.5 Reporting

The board (including any relevant sub-committee such as the finance or audit committee) should set out how and when it wants to receive information about risks. This reporting should provide reliable, current, complete and timely information, reflecting different risk types as well as emerging issues. The best way to do this may be to receive the risk register and probe academy trust management as to whether the various scores, rankings and control measures remain appropriate.

The interval at which the board should review the risk register is a matter for the board, though at least one detailed review a year is essential. Boards may decide that it is appropriate to review the register at every meeting, though this may result in a diminution in impact if it comes to be regarded as a bureaucratic necessary evil or routine box ticking exercise. The periodicity of review can be kept flexible, with boards opting for more frequent review during periods of heightened risk.

Trustees should consider “stress testing” the supposed controls and mitigations to ensure that they do not exist on paper only. For example, trustees (or the internal scrutiny function) could ask their IT provider to produce their SIMS backup data from off-site storage on disk within contract time and quality requirements.

Academy trusts must have an internal scrutiny function (internal audit, responsible officer, and so on) in place and it may be that it is appropriate for this function take ownership of the risk register and periodic reporting to the board. The register also provides a rational basis for the internal scrutiny function’s work programme.

Boards should keep their own risk appetite under review and should consider the ongoing appropriateness of its risk management approach. Unforeseen events will materialise periodically, and, when this happens, the board should consider the extent to which the risk was identified and measured and whether or not the chosen control measure was appropriate.

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”?
- **Ignoring known risks**: known 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 the tone at the top?
- **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. 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 has sufficient time to dedicate to the role and has adequate influence within the academy trust, and/or designate one of the trustees as their “risk champion”
- **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. Ideally, risks should be identified by senior people, taking into account trust-wide issues, and then the operational implications and control measures derived from them.
- **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 may not be fully bought-in to the discipline’s potential. Any programme of internal scrutiny not basing its planning on the risk register is likely to be missing an opportunity to add value

4. Conclusion

Risk management is not about creating excessive paperwork, but rather about identifying appropriate measures to control risks in your academy trust. Most academy trusts are probably already doing this instinctively, or as the result of legal requirements (such as fire safety risk assessment) but a risk management plan helps you decide whether you have covered everything you need to. There is no “one size fits all” to implement risk management, and it must be tailored to fit the size, complexity and particular challenges facing each academy trust.

However, even for a small academy trust the process needs to be reasonably formal, documented and provided with appropriate resources.

Individual risks should not be looked at entirely in isolation from each other and should always be linked to higher-level business objectives. If trustees take a holistic view of risk management then appropriate processes can then be embedded in both day-to-day operations and governance.

5. Acknowledgements

Special thanks to: Maxine Adams, Chief Finance & Operations Director, Apollo Partnership Trust; Chair, Leicestershire Academies Group.

ESFA Finance & Assurance Steering Group, WG3.

ESFA will review and update this guide by March 2021.

---

1. The Academies Financial Handbook (2018 edition, section 2.6.1) requires that business continuity risks must be managed. ↩
2. The Academies Financial Handbook (2018 edition, section 2.6.1) states that trusts should maintain a risk register. ↩
3. The Academies Financial Handbook (2018 edition, section 2.6.1) states that trusts must plan for contingencies. ↩