CROSSHALL JUNIOR SCHOOL

RISK REGISTER

CROSSHALL
JUNIOR ACADEMY TRUST

PUBLISHED: AUTUMN 2018
REVIEW DATE: SUMMER 2019

CROSSHALL JUNIOR SCHOOL LIMITED – RISK REGISTER
Autumn 2018

Overview

The Risk Register was reviewed by the Chair of Governors for approval by the Finance, Resources and Personnel Committee.

Review Procedure

Each of the risks were reviewed in turn and rated in terms of likelihood and impact, e.g. 5 (high) to 1 (low).

With the list of key risks and responses agreed, it is then time to identify any controls that exist to mitigate the risks. The controls identified need to be assessed to determine whether they are an appropriate mitigation of the risks identified. The value for money of the chosen responses needs to be considered, i.e. it is as important to avoid over-control of minor risks as under-control of serious risks.

It is likely that the assessment of controls will produce a list of actions required to produce an acceptable internal control system. Clear responsibilities should be allocated to these actions along with a deadline for the action to be completed and a scheduled date for review.

A risk register pro-forma was completed and circulated to the FRP Committee. The FRP members should be able to provide further confirmation that the understanding of the risks and controls within the organisation is accurate.

A final version of the register will be circulated to all members of the academy so that they are aware of the risk management policy and the controls in place to limit exposure to risk.

The risk register is reviewed **annually**, bearing in mind that the key risks faced by the academy may change and that the adequacy of the internal control system requires regular re-assessment.

There is a requirement to provide a report on risk management in the Trustees' Report in their annual account.

Categories of Risk

The table below offers a summary of the most common categories of risk. The table does **not** claim to be comprehensive - some organisations may be able to identify other categories of risk applicable to their work.

Category of Risk	**Illustration / Issues to Consider**
External Risk – arising from the external environment, not wholly within the organisation's control, but where action can be taken to mitigate the risk	
1. Political	Possible political constraints such as change of government or EU exit
2. Economic	Economic factors such as interest rates, exchange rates, inflation
3. Socio Cultural	Demographic change affecting demand for services; change of stakeholder expectations
4. Technological	Obsolescence of current systems; procurement and best use of technology to achieve objectives
5. Legal / Regulatory	Laws and regulations which impose requirements (e.g. health & safety and employment legislation)
6. Environmental	The need for buildings to comply with changing standards (e.g. energy efficiency); the need for disposal of rubbish and surplus equipment to comply with changing standards
Operational Risk – relating to delivery of current activities, and building capacity and capability	
7. Operations	Overall capacity and capability to achieve objectives; procedures employed
8. Service/Project Delivery	Failure to deliver the agreed service
9. Resources: Financial Physical Human Information	 Availability and allocation of funding; poor budget management Security against loss, damage and theft of physical assets, and fraud including identification of areas which can be insured Availability, retention, skills and capacity of staff Adequacy of information for decision making; security of information against loss, damage, theft and fraud
10. Relationships	Threats to relationships with delivery partners; customer satisfaction; accountability (particularly to Parliament)
11. Reputation	Confidence and trust which stakeholders have in the organisation
12. Governance	Propriety and regularity; compliance with relevant requirements; ethical considerations
13. Scanning	Failure to identify threats and opportunities
14. Resilience	Capacity of accommodation, systems and IT to withstand adverse impacts and crises; contingency planning and disaster recovery (e.g. fire, flood, failure of power supply, failure of transport systems)
Change Risk – created by decisions to pursue new endeavours beyond current capability	
15. Public Sector Targets	New targets challenge the organisation's capacity to deliver
16. Change Programmes	Programmes for organisational or cultural change threaten current capacity to deliver as well as providing opportunity to enhance capacity
17. New Projects	Making optimal decisions/prioritising between new activities that are competing for resources
18. New Policies	Policy decisions creating expectations where the organisation has uncertainty about delivery

Assessing Risk Appetite

Defining "Risk Appetite"

Risk appetite is the amount of risk to which the organisation is prepared to be exposed before it judges action to be necessary. Even risk as opportunity is surrounded by threats which potentially limit ability to exploit the opportunity, and for which an appetite in relation to the opportunity benefit has to be assessed.

Risk appetite is also about comparing the cost (financial or otherwise) of constraining the risk with the cost of exposure should the risk become a reality, and finding an acceptable balance. The fact that the resources available to control risks are likely to be limited means that value for money decisions have to be made – what resource cost is it appropriate to incur to achieve a certain level of control in respect of the risk? Apart from the most extreme circumstances it is unusual for good value for money to be obtained from any particular risk being completely obviated with total certainty.

Some risk is unavoidable, and not within the ability of the organisation to completely manage it down to a tolerable level. In these cases the organisation needs to make contingency plans.

Risk appetite may be very specific in relation to a particular risk, or it may be more generic in the sense that the total risks which an organisation is prepared to accept at any one time will have a limit.

Features of Identifying the Risk Appetite

In consequence every organisation has to identify its risk appetite. Decisions about response to risk have to be taken in conjunction with an identification of the amount of risk that can be tolerated. Any particular organisation is unlikely to have a single risk appetite.

The tolerable extent of risk will vary according to the perceived importance of particular risks. For example, tolerable financial loss may vary in accordance with a range of features including the size of the relevant budget, the source of the loss, or associated other risks such as adverse publicity. Where a particular risk can give rise to a number of effects, an effect of quite large financial loss may be acceptable whilst an associated effect of damage to health and safety may not be tolerable at all. Both the risk framework and the control responses therefore have to be considered in detail to identify the appropriate balance of potential realisation of risk against the costs of limiting that risk.

The most significant issue is that it is unlikely, except for the most extreme risks, that any particular risk will need to be completely and absolutely obviated. Identification of risk appetite is a subjective (rather than an objective or scientific) issue but nevertheless is an important stage in formulating the overall risk strategy.

Risk Responses

Responses to risk can be divided into four response categories:

Transfer For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks of risks to assets.

Tolerate The exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the response may be toleration. This option may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

Treat By far the greater number of risks will belong to this category. The purpose of treatment is not necessarily to obviate the risk, but more likely to take control action to contain the risk to an acceptable level. Such controls can be **corrective, detective, directive or preventive** (see glossary)

Terminate Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in the public sector when compared to the private sector; a number of activities are conducted in the public sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved.

Take the Opportunity This option is not an alternative to those above; rather it is an option which should be considered whenever tolerating, transferring or treating a risk. There are two aspects to this. The first is whether or not at the same time as mitigating threats, an opportunity arises to exploit a positive impact. The second is whether or not circumstances arise which, whilst not generating threats, offer positive opportunities – for example a drop in the cost of goods or services might free up resources for redeployment.

Risk Register - Strategic and Reputational Risks

Category	Sub Category	Specific	Likelihood of Occurring (5=High, 1=Low)	Impact if Occurs (5=High, 1=Low)	Response (Transfer, Tolerate, Treat, or Terminate)	Control Procedures and Target Date
Strategic Risk	**Charitable Objects Risk**	Charity receives unfavourable OfSTED report	1	3	Treat	School Improvement Plan; OfSTED Action Plan; external school improvement advisor; governors informed of/and monitor priorities and impact
	Natural Disaster Risk	Risk of the impact an uncontrollable event will have on the charity e.g. fire, flood	1	5	Transfer / Treat	Regular Fire Drills; insurance; LA and Critical Incident/Business Continuity plans
	Technology Risk	Information security risk	4	4	Treat	Computer Use Policy; IT Network Manager; social networking protocols
		Virus risk / corruption of data risk	2	2	Treat	Virus Protection; technical support
		IT systems out of date / no longer supported	4	1	Treat	Budget priority; continuous monitoring of IT
Public Profile Risk	**Fraud Risk**	Fraud discovered at the Charity attracts bad publicity	1	3	Treat	Financial protocols; external audit; Responsible Officer; Fraud Policy

Risk Register - Operational Risks

Category	Sub Category	Specific	Likelihood of Occurring (5=High, 1=Low)	Impact if Occurs (5=High, 1=Low)	Response (Transfer, Tolerate, Treat, or Terminate)	Control Procedures and Target Date
Human Resources Risk	**Management Risk**	Key person loss / succession risk	2	5	Treat	Succession plan; appraisals
	Staff Risk	Recruitment risk (recruiting someone unsuitable to work with children)	1	5	Treat	Training (GB and staff); DBS checks
		IT Technical capability risk	1	4	Tolerate	IT training for staff
	H & S Risk	Fatality/injury to pupil/third party	1	5	Tolerate	Insurance; risk assessments

Risk Register - Financial Risks

Category	Sub Category	Specific	Likelihood of Occurring (5=High, 1=Low)	Impact if Occurs (5=High, 1=Low)	Response (Transfer, Tolerate, Treat, or Terminate)	Control Procedures and Target Date
Fixed Asset Risk	**Fraud Risk**	Risk that assets are misappropriated	1	3	Tolerate	Asset checks; office systems
Funds Risk	**Level of Funds**	Risk that fund levels are too high / low	2	4	Tolerate	Keep updated with information from government

Glossary of Risk Terms

Assurance	gaining (independent) confirmation that the organisation's governance, risk management and internal control framework is appropriate, adequate and achieving the effects for which it has been designed
Corrective Control	a control designed to correct undesirable outcomes
Detective Control	a control designed to detect undesirable outcomes which have arisen
Directive Control	a control designed to ensure a particular outcome
Embedding Risk Management	ensuring that the risk management strategy is reflected in the objectives and function of every level of the organisation
Exposure	the consequences, as a combination of impact and likelihood, which may be experienced by the organisation it a specific risk is realised
Horizon Scanning	systematic activity to identify changes in risk as early as possible
Inherent Risk	the exposure arising from a specific risk before any action has been taken to manage it
Internal Control	any action taken within the organisation to manage risk, including the impact if the risk is realised and the frequency of it
Impact	the evaluated effect or result of a particular outcome actually happening
Likelihood	the evaluated probability of a particular outcome actually happening (including a consideration of the frequency with which the outcome may arise)
Preventive Control	a control designed to prevent an undesirable happening
Residual Risk	the exposure arising from a specific risk after action has been taken to manage it
Risk	uncertainty of outcome, whether positive opportunities or negative threats, arising from a combination of impact and probability, including perceived importance
Risk Appetite	the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time
Risk Assessment	the evaluation of risk with regard to the impact if the risk is realised and the likelihood of the risk being realised

Risk Management	all the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress