Community Southwark

Assessing and Managing Risk

Risk management is the identification, assessment, and prioritisation of risks followed by coordinated and economical application of resources to minimise, monitor, and control the probability and/or impact of unfortunate events or to maximise the realisation of opportunities.

No matter what we do in life, there will always be a certain level of risk, and it is no different for organisations. Organisations face varying levels of risk on a daily basis, if left unmanaged these risks could severly damage, if not close, the organisation.

The Voluntary and Community Sector (VCS) has been searching for sustainable and innovative ways to remain strong and resilient, carrying out key objectives to make a positive difference for beneficiaries. While this search may not be new in itself, the intensity of it has certainly increased during these tough times. It has been a time full of economic and policitical uncertainty with many changes coming in a relatively short space of time: gift aid changes, CRB/DBS changes, funding cuts, introduction of payment by results, bedroom tax, welfare reforms, elections, personalisation and so on. And more change is due to come throughout 2015/16 and 17.

The sector may not have control over the political and fincancial environment in which we operate but we do have control over how we run our organisations and how we meet the challenges ahead. By understanding uncertainty and managing risks we can be better placed to work through difficult times and build more resilient services.

Risk management does not have to be a negative process; it can be a useful management tool and a way to measure performance and provide more to your beneficiaries. Knowing what risks you are exposed to and the controls that you have in place allows you to make informed choices about activities.

This fact sheet will explain some approaches to risk management, the various roles and responsibilities within the risk management system and gives you the tools necessary to manage the risks that you are responsible for. It also provides guidance on how you might want to assess the controls that you have in place to manage risks, ensuring that they are the right controls and that they are working.

What is risk?

Risk is the quantifiable outcome of uncertainty and therefore manageable. By looking at the uncertainities surrounding issues and turning them into quantifiable senarios, an organisation can measure the risk involved with certain activities and decide which risks are too big to take, which you have no choice but to manage and which are simply part of the job.

The Charity Commission use the term ‘risk’ to ‘*describe the uncertainty surrounding events and their outcomes that may have a significant impact, either enhancing or inhibiting any area of the charity’s operations.’*

Risks fall into two main categories, strategic and operational. Strategic risks are those that affect your medium to long term strategic goals and objectives. Operational risks are those that are encountered in the daily course of work.

Risk = event or action which may have an impact on the achievement of objectives.
Can be strategic or operational:

- **Strategic** – affect ability to achieve medium to long term strategic goals and objectives
- **Operational** – encountered in daily course of work.

Below are some examples of risks under both categories:

Strategic risks

- **Political** – a change in approach from national or local government which affects our ability to deliver our objectives
- **Economic** – affecting the ability to meet financial commitments (including internal budgetary pressures, adequacy of insurance cover, macro level economic changes, investment decisions)
- **Social** - relating to change in demographic, residential or socio-economic trends
- **Technological** – associated with the ability to deal with pace of change and consequences of internal technological changes
- **Legislative** – current or changes in national or EU law
- **Environmental** – associated with environmental policies and practice and dealing with environmental consequences of progressing strategic objectives
- **Competitive** – affecting the competitiveness of services, including the ability to deliver value for money
- **Beneficiaries and stakeholders** – failure to meet current or changing needs and expectations. Hazards that can impact upon reputation or goodwill

Operational risks

- **Professional** – associated with the particular nature of your business unit
- **Financial** – associated with financial planning, accounting and reporting, control and delegation
- **Legal** – relating to possible breaches of legislation
- **Physical** – connected to protection of property and assets and health and safety
- **Contractual -** failure of contractors to deliver services or products to agreed cost / specification
- **Reputational** – relating to the organisation's reputation and the public perception of the organisation's efficiency and effectiveness
- **Technological** – relating to reliance on operational equipment
- **Environmental** – associated with pollution, noise or energy efficiency of day to day operations
- **Human Resources** – relating to recruitment and retention, health, safety and welfare of people, sickness rates and personal development
- **Processes** – inspection compliance, project management, performance management etc.

Risk Category Examples from the Charity Commission guidance ‘Charities and Risk Management’ (CC26)

Risk category	Example
Governance risks	• Inappropriate organisational structure • Trustee body lacks relevant skills or commitment • Conflicts of interest
Operational risks	• Lack of beneficiary welfare or safety • Poor contract pricing • Poor staff recruitment and training
Financial risks	• Inaccurate and/or insufficient financial information • Inadequate reserves and cash flow • Dependency on limited income sources
External risks	• Poor public perception and reputation • Turbulent economic or political environment • Changing government policy
Compliance with law and regulation	• Acting in breach of trust • Poor knowledge of legal responsibilities of an employer • Poor knowledge of regulatory requirements

What is risk management?

Risk is considered to be an event or action which may have an impact on the achievement of objectives. Risks do not have to be negative, they can be positive. Risk management should be used to manage the negative effects of risks while also attempting to maximise the positive opportunities.

Risk management is the process by which risks are identified, evaluated and controlled. The process of risk management does not seek to fully eliminate all risks, as this cannot be achieved. Rather, it acts to reduce the risk that is left over after we insert controls (this is called the ‘residual risk’) to an appropriate level with which the organisation is comfortable.

The responsibility for the management and control of the charity rests with the governing body and therefore they must be involved in the key aspects of managing risk – particularly setting the risk appetite of the organisation (what level of risk is acceptable for the charity), setting the expectations for the risk management process and considering the results. Trustees do not need to do the process themselves. If there are staff, then trustees are likely to delegate elements to them. However, trustees must be involved to such a degree that they can make the statement in the annual report to say that risks are managed.

Reporting in its trustees' annual report on the steps a charity has taken to manage risk helps to demonstrate the charity's accountability to its stakeholders including beneficiaries, donors, funders, employees and the general public.

The underlying premise of risk management is that every organisation exists to provide value for its stakeholders. All organisations face risks and challenges from both internal and external factors and influences. The key task for management is to determine how much risk is acceptable for the organisation and what impact will it have on the organisations objectives. Note that the

Commissions' definition states that risk may in fact enhance a charity's operations, so it is important to look at which risks are worth taking for the good of the charity.

Therefore, as part of your risk management process, your organisation will need to decide what your 'risk appetite' and ' risk tolerance' are. These are moving concepts and will of course be unique to every organisation. By understanding the level of risk you organisation is willing to accept in pursuit of its objectives (risk appetite) and the level beyond which the organisation will not accept exposure to the risk under any circumstances (risk tolerance), your organisation will also be able to identify the opportunities that have inherent risk but are still worth doing in furtherance of your objectives.

Knowing your risk appetite and tolerance will come down to the risk culture of your organisation. '*Risk culture is a term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose, in particular the employees of an organisation. This applies to all organisations from private companies, public bodies, governments to not-for-profits.*

An effective risk culture is one that enables and rewards individuals and groups for taking the right risks in an informed manner' (The Institute of Risk Management – IRM)

There are plenty of risk management tools out there, but what they all have in common is being a systematic way to map out the uncertainties facing your organisation so that you can plan for change, opportunities and the day-to-day running of the organisation in order to meet the objectives of your organisation.

To put it simply risk management is expecting (and planning for) the unexpected.

Why should you manage risk?

Effectively managing risks helps us to achieve our objectives, which is the reason that we exist, by:

- Identifying risks that prevent you from accomplishing your objectives
- Identifying opportunities that you can take advantage of in order to deliver more for your beneficiaries

Charities are required by law to make a risk management statement in their trustees' annual report, confirming *that '…the charity trustees have given consideration to the major risks to which the charity is exposed and satisfied themselves that systems or procedures are established in order to manage those risks'* (Charities (Accounts and Reports) Regulations 2008)

The Charity Commission advises that charities consider risk and its management in a structured way if a positive risk management statement is to be made.

Benefits of managing risks

- An increased focus on what needs to be done to achieve your objectives
- More satisfied stakeholders
- Better management of change programmes
- Better able to support innovation

- Reduction in complaints
- Great control of insurance costs
- Quality improvement
- Enhanced ability to justify and rationalise our actions
- Protects our reputation
- Reduces the risks of mistakes
- Allows us to think more strategically about the future rather than ‘fire-fighting’

What do we need to do in order to manage risk effectively?

You should start by spending some time thinking about your assurance framework. Ensure that you are very clear about the following:

- What is the organisation’s appetite for risk? In other words, what is the amount of risk (financial, reputation, health, etc) that is acceptable to the organisation. This allows staff to understand the significance of the risks faced. They can then make more informed decisions about whether controls are worth it, when to report to trustees, whether to take risks in this area at all, etc.
- The roles within the organisation to manage risk- clearly document these roles and make sure everyone understands this
- Who owns the controls? They will be the people responsible for checking and providing assurance they are the right controls, that they are working and that you know what risk still remains after the controls are in place. They will provide annual assurance that the controls are working – this is call an ‘Annual Assurance Statement’.
- What are the expectations if controls are not working?

The boards role in managing risk

The board has a key role in managing risk: it is the board who are ultimately responsible for safeguarding the Mission of the organisation and so must understand the risks that could threaten that. The board must ensure that a process for managing these risks is put in place **before** they happen.

Some key questions for the board are:

What can go wrong? Risks that apply to all organisations i.e. health and safety etc. Unique risks which apply to your organisation e.g. specific funding, litigation etc.

What will we do to prevent it? Review your premises, processes, operations etc. to identify risks and fix things that are fixable. Mitigate risks where possible e.g. introduce checks, sign off processes and training. Review risks at regular intervals – at least annually.

Trustees are ultimately responsible but don’t want a long list of every little risk, therefore it is a good idea to have someone in the organisation who will be responsible for checking the more every day risks. Make a trustee responsible for checking on the bigger risks and discuss as a whole board regulalry.

What will we do if it happens? Scenario planning and stress testing to develop strategies in advance.

If you are not sure about risk in your organisation, try asking the board the following questions:

- What are our top risks?
- How often do we assess risk?
- How effective are we at managing risk i.e what are the results?

- Do we have organisational blind spots e.g. culture?
- How do we articulate risk appetite?
- How effective is risk reporting?
- Can we respond to extreme events?

How can we manage risk?

In order to manage risk effectively it is important to ask yourselves key questions in four main areas:

1. **Identify** - what might stop us delivering our strategy?
2. **Rate and score** – if we did NOTHING what is likelihood that this happens? What would the impact be?
3. **Controls** – what do we currently do to stop this happening? What level of risk remains and is this good enough?
4. **Actions** – if it's not good enough what do we need to do next?

Once you have identified various risks it is worth scoring them to find out which are high and which are low, in both likelihood of happening and in the impact they would have if they do happen.

You can then decide which controls you need to put in place for each risk. A risk register can help you to keep track of the risks and whether or not the controls are working.

But remember, you don't want pages and pages here. So some low risks won't make it; for example, petty cash is a risk, however, simple controls such as limiting how much is in the office, having to sign for it, having a policy on who can take petty cash and for what etc. should limit the risk considerably and therefore it is unlikely to make it onto the register.

Losing core funding from your single biggest funder would be a much higher risk and would therefore go on the register and be carefully monitored to ensure actions are being taken to deal with this.

Don't forget to monitor the actions taken, and change them if they are not working.

10 Top Tips for managing risk

1. Managing risk is just what we do – petty cash, supervisions, HR processes – if these are relevant, up-to-date and useful then risk can be easily managed.
2. Risk is not always internal – PESTLE and many other planning tools can be used to help you identify risks (as well as opportunities) over which the organisation has no control such as changes in policy or government, technology and law. Recognising how they affect your organisation and your beneficiaries will help you to identify the risks involved.
3. Recognise the controls – be sure you know what controls are in place and why. If something isn't working, change it.
4. Build it into schedules and meetings – spend some time thinking about and discussing risk, new risks will appear throughout the year and should be dealt with as they arise not months.
5. Discuss biggest risks and critique and challenge – are these risks still so big? Should they be moved down? Have the controls and actions worked? Are they high risks in themselves or is it that the organisation is highly risk adverse?
6. Recognise your own style and weaknesses and give it to someone else! – Risk management does not have to fall to one person, think about who is best placed to take an overarching role in its management and delegate monitoring particular controls to those working in each area.

7. Make register a useful tool – don't write everything down and lock it away. Create a risk register that really supports you to keep track of the risks, the controls in place, the lead person etc. and update it as risks move up or down.
8. Risk is not always bad – it is easy to assume risk is bad but risks also come with good opportunities for example a small organisation with no staff is awarded a large contract; they now have to manage the money, employ staff etc. all of which is risk. Or joining a consortium is a risk but the opportunities it presents may far outweigh the 'risks'.
9. Identify your risk culture – take a look at IRM's guidance on understanding risk culture and take some time to think about the risk culture of your organisation. Do you need to make any changes?
10. Take a look at the controls you already have in place – does anything need updating? Are they relevant and helpful?

Below is one suggested process to manage risk. There are lots of ways to do this and the example below can be simplified – what's important is that your organisation is thinking about risk and managing it:

Six steps to managing risk

1. Identify your risks
2. Analyse – how likely are they to happen and what would the consequences be?
3. Evaluate – What is the overall risk?
4. Mitigate – what can you do to reduce the risk and does it need escalated?
5. Assurance – testing your controls
6. Monitor and report – who needs to know about the risks and how do you monitor them?

Step 1: Identify risks

When thinking about risks, you should consider what the project, service, unit, etc is vulnerable to – what could we suffer, a failure to deliver, a loss, a shortfall, a barrier to achieving the objective?

Write down all of these risks.

Step 2: Analyse risk

Once you know what your risks are, consider:

a. how likely is this to occur (likelihood)
b. what would the consequences be if the failure happened – how big a problem would that be (impact)?

Once you know the risk, the likelihood of that risk occurring and the potential impact you can develop your risk 'score'.

You risk score is calculated by multiplying the likelihood by the potential impact:

Likelihood x Impact = Risk score

Use the tables below **(add table numbers)** to help you calculate how likely things are to happen and the potential impact.

a) Identify likelihood

Likelihood Table

The following can be used as a guide for determining likelihood. However this tool has limitations as likelihood and frequency of events tend to vary between disciplines and functional areas so you will have to make a judgement – it is important to check this judgement with others who understand the area that you work in.

	Expected or actual frequency experienced
Rare (1)	May only occur in exceptional circumstances; simple process; no previous incidence of non-compliance
Unlikely (2)	Could occur at some time; less than **25%** chance of occurring; noncomplex process &/or existence of checks and balances
Possible (3)	Might occur at some time; **25 –50%** chance of occurring; previous audits/reports indicate non-compliance; complex process with extensive checks & balances; impacting factors outside control of organisation
Likely (4)	Will probably occur in most circumstances; **50-75%** chance of occurring; complex process with some checks & balances; impacting factors outside control of organisation
Almost certain (5)	Can be expected to occur in most circumstances; more than **75%** chance of occurring; complex process with minimal checks & balances; impacting factors outside control of organisation

The above definitions are intended as a guide, and a degree of flexibility may be appropriate in their application.

b) Grade the impact

Grading of the impact is less straightforward, since there are a variety of impact types which a risk may have, for example reputation or financial. To provide guidance, a description has been provided for some of the more common impacts, as set out on the following page. It should be noted that an impact may occur in only one of these categories, and a grading does not indicate that all impacts will arise. In cases where other impact types arise, the gradings must be interpreted appropriately.

Impact table

The following is a guide to determining impact or consequence. The definitions will be different in the various business units and areas so this is just a guide.

	Expected or actual impact experienced
Insignificant (1)	Very little impact or impact is at everyday level which is easily absorbed by organisation.
Minor (2)	Small amount of impact which is normally dealt with at the team level. No reputational damage expected.
Moderate (3)	Impact may require an increased level of attention and create organisational delays or underacheivement of targets. Senior management level involvement needed.
Major (4)	Prolonged suspension of work which severely delays reaching targets and rganisational objectives. Possibility of loss of funding. Board level involvement needed. Possibilities of reputational damage.
Catastrophic (5)	High level of impact which may mean a failure to meet organisational objects and run efficiently. High reputatuional damage

Example Impact Table

Level and descriptor	Health Impacts	Critical services interruption	Organisational outcomes/ objectives	Reputation and image per issue	Non-compliance	Financial cost/loss
Insignificant (1)	First aid or equivalent only	No material disruption	Little impact	Non-headline exposure, not at fault; no impact	Innocent procedural breach; evidence of good faith; little impact	<£100
Minor (2)	Routine medical attention (up to 2 wks incapacity)	Short term temporary interruption – < 1 day	Inconvenient delays	Non-headline exposure, clear fault settled quickly; negligible impact	Breach; objection/complaint lodged; minor harm with investigation	<£1,000
Moderate (3)	Increased Level medical attention (2 wks to 3 mths incapacity)	Medium term Temporary suspension – Backlog cleared by additional resources	Material delays; marginal underachievement of target performance	Repeated non-headline exposure; slow resolution; Board / Leadership Team enquiry/briefing	Negligent breach; lack of good faith evident; performance review initiated	<£10,000
Major (4)	Severe health crisis (incapacity beyond 3 mths)	Prolonged suspension of work – Additional resources required; performance affected	Significant delays; performance significantly under target	Headline profile; repeated exposure; at fault or unresolved complexities; Board / Leadership Team involvement	Deliberate breach or gross negligence; formal investigation; disciplinary action; Board/Leadership Team involvement	<£100,000
Catastrophic (5)	Multiple severe Health crises/injury or death	Indeterminate prolonged suspension of work; non performance	Non achievement of objective/ outcome; performance failure	Maximum high level headline exposure; severe board criticism; loss of credibility	Serious, wilful breach; criminal negligence or act; prosecution; dismissal; severe board criticism	<£1000,000

Step 3: Evaluate

Once risks have been graded, they may be reflected on a risk scoring grid. Plotting the impact and likelihood on the grid allows you to asses the overall risk. This is a risk scoring grid (the colour coding is explained below, under “risk classification”).

When a risk is amber or red on your risk register, use the escalation process.

	Consequence / Impact				
Likelihood	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Rare (1)	Low (2)	Low (3)	Low (3)	Moderate (4)	Moderate (5)
Unlikely (2)	Low (2)	Low (4)	Moderate (6)	High (8)	High (10)
Possible (3)	Low (3)	Moderate (6)	High (9)	High (12)	Extreme (15)
Likely (4)	Moderate (4)	High (8)	High (12)	Extreme (16)	Extreme (20)
Almost certain (5)	Moderate (5)	High (10)	Extreme (15)	Extreme (20)	Extreme (25)

For grading risk, the scores obtained from the risk matrix are assigned grades as follows

Risk classification	
1 - 3	Low risk. Risks where any action to further reduce the level of risk would be inefficient i.e. the cost in time or resource outweighs any potential impact of the risk materialising. Such risks include infrequent events with low impact. These risks are being effectively managed.
4 - 6	Moderate risk. Risks which can be reduced within a reasonable timescale, in a cost effective manner. Any mitigating actions must be monitored and recorded. Moderate risks are coloured yellow on the scoring grid
8 - 12	High risk. Risks which have a serious impact, and detrimental effect on the achievement of objectives. Action plans should be developed to reduce the level of residual risk, and reviewed periodically. High risks are shown as orange on the scoring grid
15 - 25	Extreme risk .

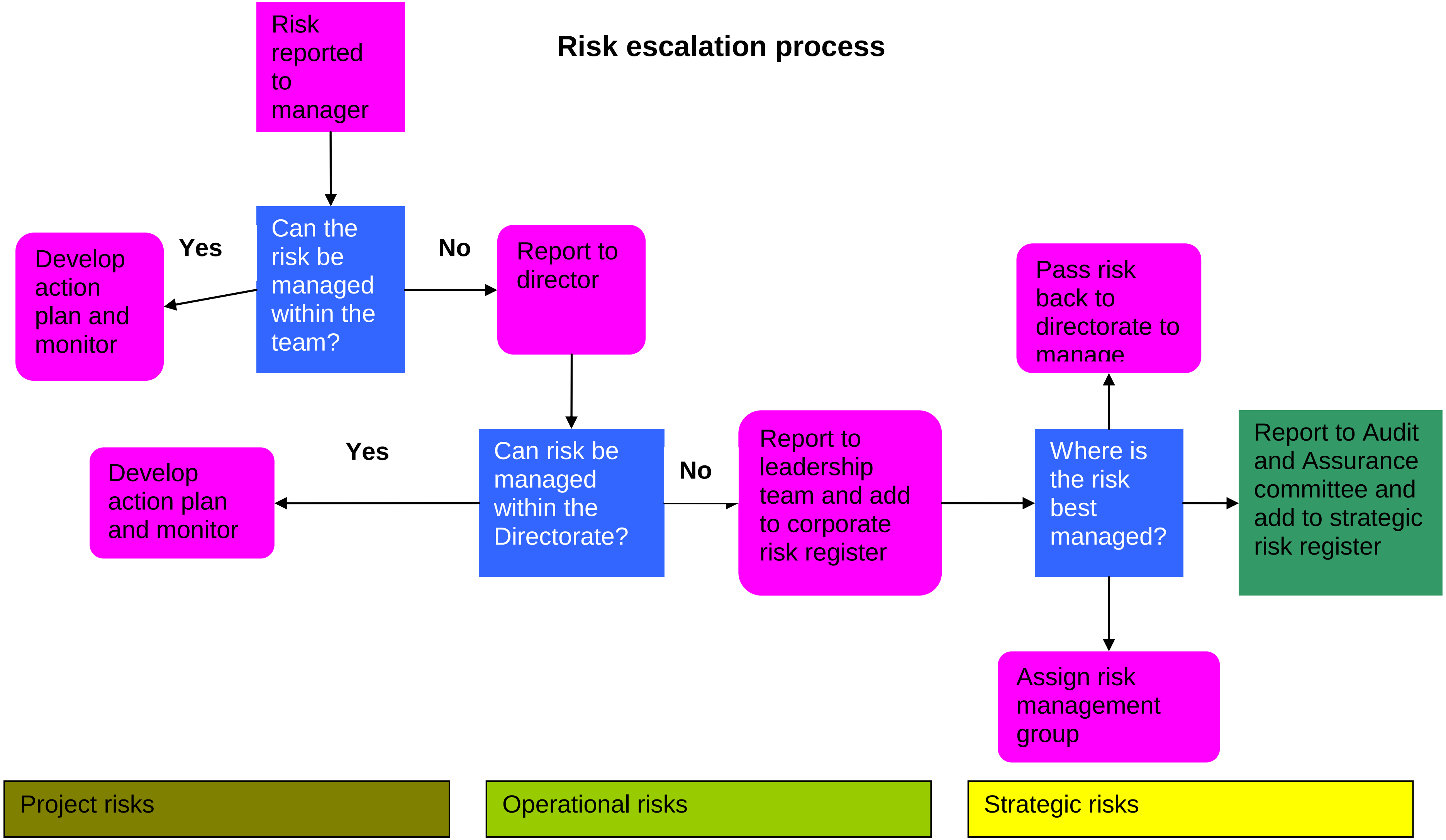
Step 4: Mitigate risks

The level of each identified risk must be transferred or controlled to a satisfactory level. This will involve people who own the risk and control working together to consider the controls in place to mitigate or reduce the risk. This might include enforcing existing controls, introducing new controls, contingency planning, stopping the activity, accepting the risk, insuring against the risk or contracting out the risk.

Any choice to accept risk at the directorate or corporate level should be backed up with realistic contingency plans and agreed by the Leadership Team and the Board of Trustees.

Once you know the controls that are in place you can assess the residual risk, ie, the risk that is left over. If it is above acceptable levels, consider whether you need to escalate the risk. See the figure below for the escalation procedure

Risk escalation process



Risk reported to manager

Can the risk be managed within the team?

Yes

Develop action plan and monitor

No

Report to director

Can risk be managed within the Directorate?

Yes

Develop action plan and monitor

No

Report to leadership team and add to corporate risk register

Where is the risk best managed?

Pass risk back to directorate to manage

Report to Audit and Assurance committee and add to strategic risk register

Assign risk management group

Project risks

Operational risks

Strategic risks

Updated: April 2016

Step 5: Assurance

Once the key business risks have been identified, assessed and are subject to controls throughout various parts of the business, it is important to obtain confirmation that these activities are being performed as expected and that the risk and control scoring is valid. Risk owners will be asked to provide annual assurance during their appraisal that the appropriate controls are in place. Internal audit can also be asked to review the controls and provide assurance.

Step 6: Monitor and reporting

Relevant information for each key risk should be seen by the right people at the right time across the organisation.

Register Activity	Strategic risk register	Corporate risk register	Business Unit/Directorate register	Programme/project
What is recorded?	Risks so significant they could materially impact achievement of objectives or even our survival Normally arise from strategy, are external and beyond our control, are pervasive across organisation.	Records the lower level risks that affect high level strategic priorities and cut across organisation.	Business Unit risks that are not large or significant enough to be recorded on the corporate or strategic registers	Programme or project risks.
Who maintains	Sufficiently senior member of staff	Sufficiently senior member of staff	Head of directorate	The programme or project lead
Who owns the risks for monitoring	Each risk has a risk owner at Leadership Team level	Each risk has a risk owner at Senior Management Level	Head of Directorate although each risk may have management owner	The programme or project lead
When is the content reviewed	- Leadership Team reviews and updates quarterly as part of performance monitoring - Audit and Assurance committee review quarterly -Trustees discuss and update annually	- Leadership Team review quarterly as part of performance monitoring -Audit and Assurance committee review twice a year -Trustees review annually	As the directorate decides	Quarterly by programme lead or sponsor
When is it reported on	-Exception reporting (when the status of a risk changes) - Quarterly from Leadership	-Exception reporting (when status of a risk changes) - Quarterly from Leadership	- Directorate decides - Where a risk is red or amber the LT will decide whether it	- Exception reporting - Twice a year to CEO as part of performance

	Team to Audit and Assurance as part of performance monitoring - Annually to trustees	Team to CEO as part of performance monitoring -To Audit and Assurance Committee twice a year -Trustees annually	needs to be reported on and recorded on the corporate register	monitoring
Assurance on controls	Provided from Leadership Team annually to trustees	Provided from directors to Leadership Team annually	Provided from individual Director to CEO annually in appraisal	Provided from Programme lead to CEO annually in appraisal
Other features	No more than 10 risks at any one time			