

IRM Charities SIG Risk Management Maturity Framework

	Conscious	Developing	Proficient	Expert
Level	<p>Aware of risk management through Charity Commission and other guidance but unsure how to 'make it happen'.</p> <p>Planning is a repeated exercise based on previous years as no one has time to consider further.</p> <p>Objectives and targets are often missed as senior management are diverted to deal with unplanned events.</p>	<p>Aware of the need for good risk management but not yet fully committed to the concept.</p> <p>Risks are considered on occasions as part of planning by some but others are unenthusiastic.</p> <p>Objectives and targets are not always achieved as senior management are diverted to deal with unplanned events or unenthusiastic about using a risk based approach.</p>	<p>Risk management is established and becoming mainstreamed and less noticeable as a separate activity.</p> <p>Risks are considered as part of planning but not fully explored.</p> <p>Objectives and targets are usually achieved. Contingency plans for key risks are generally in place, resulting in minimal disruption when unwanted events occur.</p>	<p>Risk management is embedded at all levels within the organisation on a consistent basis.</p> <p>Risks are fully explored as part of the planning process.</p> <p>Objectives and targets are nearly always fully achieved and the organisation is rarely surprised by unplanned events. Contingency plans exist for key risks and any surprises are normally external in origin.</p>
Knowledge and skills	<ul style="list-style-type: none"> Staff, managers and leaders are aware of need to do risk management, but do not understand why or how. Risk management may be seen as a separate discipline not connected to business planning or day-to-day decision making. It's perceived as a distraction. There is no one or few within the organisation who understand risk management. 	<ul style="list-style-type: none"> Managers and leaders understand the theory and processes behind formal risk management. They know a risk policy and guidance exist, but may think of risk as a compliance tool, not as a tool for real organisational improvement. Key staff have read the risk policy and guidance. Staff and managers understand some of the organisation's key risks and risks to their area. 	<ul style="list-style-type: none"> Training has been provided to managers and leaders who know how to identify, assess, address, monitor and report risk in a consistent way in line with policy. Managers throughout the organisation know what is expected of them to manage risks and there's real ownership of risks and actions. There's a real belief that risk management can help and add value. An understanding of upside risk is beginning to be shown. 	<ul style="list-style-type: none"> Leaders seek out and demand quality risk information as part of decision making processes. Training and refresher training is available so that staff and key volunteers understand risk management and know what is expected of them. Risk management is seen as fundamental to "the way we do things around here" within an established Risk Culture. Understanding of upside risk is widespread.
Possible behaviours	<ul style="list-style-type: none"> Senior management do not yet see the benefits of risk management. Staff, managers and leaders are not yet taking action to identify and control risk across the organisation or in high risk areas. Policies and standards have not been developed. Without this staff decide for themselves what level of risk taking is acceptable. Little attention is paid to risk mitigation actions. Risks often occur which should have been foreseen and recorded on the risk register. There's no structured approach to learning lessons for future work. 	<ul style="list-style-type: none"> Senior management give passive support to risk management or can be unsupportive or hostile. They rarely lead by example. Risk management often involves a junior team member creating a risk register document which then collects dust and is rarely updated. Progress against planned risk mitigation actions is often not satisfactory. There's no routine analysis for future projects. 	<ul style="list-style-type: none"> Senior management are visibly giving direction on the oversight and management of risk, using basic risk information – including the defined risk appetite - to inform decision-making and generally promoting and supporting the concept. Managers act as role models and lead on risk management, regularly checking that risks are being managed and discussed with relevant people. Discussions about risk are becoming increasingly more mature and widespread and this is evidenced in minutes and notes. There's open communication internally on risk. The policy and processes are used and adhered to in everyday activities. Progress against the planned risk mitigation actions is usually satisfactory. There is communication of lessons learned. 	<ul style="list-style-type: none"> Trustees and senior management demonstrate top-down commitment to risk management, leading by example. People adhere to policies and processes and use them appropriately. Application is widespread at all levels of the business, with regular updating, active feedback and learning. Risk management is used to spot opportunities as well as threats. Agreed risk responses are effectively carried out and monitored for all risks, including emerging risks. Responses can cope with any scenarios. Risk-based reporting and decision making is routine. Frontline, leadership and risk experts collaborate and communicate. Risks are explicitly discussed at all levels in the organisation. The effectiveness of risk management is regularly reviewed. Lessons learned are implemented and learning from experience is a routine part of the process.
Systems, Policies & Processes	<ul style="list-style-type: none"> Someone may have risk management allocated to them but as part of a larger remit and without any supported learning. Pockets of operational risk management such as Health & Safety may be being addressed. Training is not considered or available. There's no formal risk policy or processes– some places are too risk averse while others take excessive risks. Risk registers may have been produced, but only as a one-off exercise. Risks in the risk registers are not clearly defined in all cases and/or risk owners have not been allocated. Contingency plans do not exist where they are needed. There is no approach to escalating risks from the frontline. It's done on an exceptional basis as the result of a crisis. 	<ul style="list-style-type: none"> There may be a central risk manager who is the organisation's expert or the responsibility may be assigned to a junior member of staff as part of a wider remit. There is no or only limited experience of using risk management. There are no risk champions across the organisation or other indicators of a risk management culture. Some staff have attended training but the person allocated responsibility for risk management is normally called on to support management. Risk Management Policies and standards are not consistently used or fully adhered to. Application is patchy with different groups doing different things – there's no cohesion between groups. There are risk registers at directorate level which are typically compliance focussed documents, updated only when required. Risk is not routinely a standing item at management, team, project or programme board meetings. Risk management is partially effective and works in some specific areas where it has been embraced. There's evidence of some risks being escalated in accordance with the policy in areas where risk management has been embraced. 	<ul style="list-style-type: none"> Accountability for management of key business risks is clearly defined and captured in role descriptions/personal performance targets. Risk appetite begins to be considered. There's a formal organised and updated training programme. There's an accepted policy for risk management and evidence that the defined risk appetite is often referred to in decision-making. Risk management is part of the business planning and performance process and organisational monitoring processes such as management reporting, performance management and individual objectives, all focus on risk. Risk registers exist at corporate and directorate level and are regularly updated and used at management meetings throughout the organisation. Contingency plans are in place where needed. Risk is a standing item at management meetings throughout the organisation. Managers regularly discuss risk with their staff and share and discuss critical cross-cutting risks. A visible process is in operation for escalating risks from the frontline to directorate and corporate level. No one is blamed for escalating a risk and good risk management is recognised positively in personal appraisal discussions. Business continuity planning is in place and all units have workable, up to date and tested Business Continuity (BC) plans. Information risks are identified and mitigating actions are in place. 	<p>As "proficient" but with the following additions:</p> <ul style="list-style-type: none"> Senior management is actively engaged in the process of identifying risk and setting the organisation's risk appetite. Personal performance objectives include targets for risk management and proactive risk management is encouraged and rewarded. Mission, business planning and core risks are explicitly linked. Longer term risks are integrated into the strategy and business planning functions. Training is actively encouraged. Sustained regular discussions on risk are long established and routine throughout the organisation. Risk management adapts proactively to internal and external changes. Risk management is a dynamic and living approach that is constantly referred to and where necessary updated Strategic risks are taken into account and give direction to the business planning and policy making mechanisms. Information is safeguarded at all levels of the organisation.

