



RISK MANAGEMENT

Iceland 
Liechtenstein
Norway

**Active
citizens** fund

This material is created as part of the Next Gen initiative. Next Gen is a joint initiative of the Active Citizens Fund Operator in Bulgaria and the Active Citizens Fund Operators in Slovakia and Lithuania to enhance the capacity of young leaders of civil society organisations. The Active Citizens Fund Operator in Bulgaria is the Open Society Institute - Sofia Foundation in partnership with Workshop for Civic Initiatives Foundation and Trust for Social Alternative Foundation.

Sofia 2024

This material is created with the financial support of the Active Citizens Fund Bulgaria under the Financial Mechanism of the European Economic Area. The entire responsibility for the content of the document carried by the Active Citizens Fund Operator in Bulgaria and under no circumstances can be taken to reflect the official opinion of the Financial Mechanism of the European Economic Area.

RISK MANAGEMENT

The trustees of an organisation are responsible for safeguarding its assets - including its reputation - and board members are responsible for good and lawful governance. In recent years, increasing attention has been given to risk assessment and risk management - identifying the things that can go wrong, what the likelihood of this happening is, how serious it could be if it did happen, what has already been done to limit the likelihood of it happening and to limit the negative impact if it does, and the further steps that can or should be taken.

Risk assessment and risk management are not highly specialised disciplines requiring a high level of technical skills. As with most aspects of good governance, they are rooted in the everyday exercise of common sense. They are closely linked to planning (see Resource Material 14) and change management (Resource Material 16).

Legal requirements

Duty of care

Everyone has, by unwritten laws, a duty of care to take reasonable steps to ensure that no one suffers injury, illness or death, or property damage or other financially measurable loss, because of something that could have been foreseen and prevented. The Board has this duty in relation to employees, volunteers, service users, members of the organisation, members of the public, anyone else with whom the organisation comes into contact and the organisation itself. Individual employees, paid or voluntary, have a duty to the service users they work with, other employees and others with whom they come into contact.

Failure to exercise a duty of care is negligence. The person who was injured or suffered harm or loss can sue the person who failed to follow safety rules. Public/civil liability insurance or professional indemnity insurance can cover situations where the organisation has to pay compensation in cases of negligence.

The legal basis for assessing all types of risks is enshrined in this duty of care.

Law on non-profit legal entities

Not-for-profit organisations are responsible for safeguarding their organisation's assets, which include not only its funds and property but also its reputation. They must also make sure that the assets of the organisation are used to achieve its objectives, in accordance with its constitution. Even when an organization is not for the public benefit, the board as a whole is responsible for safeguarding the organization and ensuring the proper use of its assets.

The Trustees' responsibilities are:

- to focus primarily on major risks - the things that keep them awake at night - and to make sure that there are appropriate procedures in place to mitigate those risks;
- ensure that the council and/or staff consider other risks - the more routine or day-to-day care - and put in place appropriate procedures in place to prevent them.

Scope of risk

People often think of risk only in terms of health and safety, or of disasters such as fire, flood or computer failure, or in relation to financial risks such as fraud. However, risk management is much broader and includes anything that could have a significant impact on an organisation's strategic and operational management, its capacity to do its job or its reputation. The latter - reputational risk - is often overlooked but should always be considered.

The lists given below are not exhaustive but are a starting point for considering risk. Another approach is described in the risk management standards freely available on the Bulgarian Institute for Standardisation (BIS) website.

Risks in strategic and operational management

Most strategic and operational management risks can be anticipated and steps can be taken to likely mitigate or influence them.

Examples of these risks are:

- non-compliance with the objectives set out in the organisation's constitution by the board and/or officers, or even ignorance of constitutional requirements;
- failure to set and/or adhere to the organisation's strategic objectives or failure to regularly review these objectives;
- pressure to act outside the spirit and values of the organisation (or lack of agreement about what its spirit or values are);
- board members do not understand their role and the board as a whole lacks the necessary skills, knowledge and experience to carry out its duties effectively;
- conflicts within the board or staff team, or between the board and staff, preventing the organization from operating effectively;
- lack of clear separation between the roles of council and officers;
- inadequate reporting and communication between and within council and officers (see Resource Material 5);
- lack of consistent succession planning for key board members and/or staff;
- key councillors or officers unable to carry out their duties, possibly due to unexpected illness or departure;
- failure to comply with charity law and/or trading law (if applicable) and other legal requirements.

Operational risks

Operational risks relate to the capacity of the organization to perform its activities and services. While some are unpredictable, most can be anticipated and steps can be taken to mitigate their likelihood or impact.

Operational risks include:

- Lack of adequate funds or other resources (equipment, premises, etc.) to carry out the activities, arising from poor financial planning and monitoring, unsuccessful fundraising or other reasons;
- risks to resources (theft, breakage, misuse, spoilage or depreciation);
- Lack of sufficient staff (paid or voluntary) to carry out the work, or staff without adequate training or support;
- Inability to underwrite contractual terms or those for donations;
- Invalid, inadequate, inappropriate, unenforced and/or unworkable policies and procedures (see Resource Material 21);

Risk assessment of future projects:

- Inability to respond to complaints or concerns of service users, donors/service purchasers or others;
- the constant drive to develop new activities or refraining from giving sufficient attention to the development of new activities;
- Inability to adapt to the changing needs of service users, donor/user demands, political and environmental changes, technological changes and other pressures;
- Inability to plan adequately for disasters such as theft, fire, flood, equipment failure, loss of information, in case an employee or user does something that damages the organization's reputation;
- success risk - the possibility that the organization will be destroyed by its own success.

Financial risks

Every organization is aware of the possibility of not having enough resources to do what it wants to do or what it is obliged to do. But a much wider range of financial risks need to be addressed, such as:

- Inadequate financial procedures: budgeting, fundraising, or revenue generation strategies; cash flow planning, financial statements, monitoring and reporting, actions to address cash flow shortfalls and variances from budget (see Resource Material 23);
- Inadequate procedures to limit the risk of fraud or financial mismanagement and to increase the likelihood of it being recognized if it occurs;
- over-reliance on a few sources of funds;
- setting an insufficient price (for goods or services to be sold or provided under contract) or using insufficient funds (donations) and so having to subsidize - or setting too high a price or bidding for too much, and ending up with no sale, contract or donation;
- inability to use restricted funds (donations or grants received for specific purposes) as required;
- invalid or inadequate reserve policies (explaining why the organization needs reserves, how much should be set aside as reserves, and how reserves should be stored or invested);
- inability to meet long-term financial obligations such as redundancy pay, pension contributions, and loan repayments.

Environmental and external factors

These are the most difficult risks to predict as they are beyond the control of the organization. To some extent, they can be anticipated by careful examination of political, economic, social and technological factors as well as environmental and reputational factors.

These factors typically include:

- changes in the public image of the organization or its field of activity, such as the type of activity suddenly becoming fashionable or going out of fashion, or a serious negative advertising campaign being carried out for another similar organization;
- likely or possible changes in political control and/or policy at local, regional, national or supranational level;
- changes in the organization's markets: its service users, customers, donors or service purchasers;
- competition with fewer or more organizations offering similar services;
- demographic and other social changes in the communities served by the organization and among the organization's supporters, such as more children, an aging population, more refugees and those in need of shelter;
- environmental changes, such as new roads dividing or bringing communities together, new housing developments attracting more people;
- technological changes, such as the rapid shift to mobile phones and electronic communication in the late 1990s and early 2000s.

Regulatory risk

Regulatory risk arises from a failure to understand, follow and comply with legal and regulatory requirements. They coincide with many other risks - of strategic management, operational management, reputation - but they need to be considered separately to make sure nothing is missed.

Consideration of regulatory risk should include:

- the object and powers of the organisation, as set out in the constituent instrument;
- constitutive rules, standing orders and other internal regulations concerning the membership of the organisation and its governing body, meetings and other administrative matters;
- requirements imposed by donors through the terms and conditions for donations or purchases of goods and services in the contractual terms;
- lease requirements and other legal agreements;
- duty of care to the organisation's service users, employees and other associates, other organisations with which they are in contact, its members and the organisation itself;
- Non-Profit Legal Entities Act if the organization is registered as a non-profit legal entity;

- Commercial Act, Social Assistance Act or Social Services Act if the organisation is registered as a company or as a non-profit legal entity (NPO);
- Labor Code if the organization has employees working under contract with the organization;
- Occupational Health and Safety Act;
- Data Protection Act if the organisation collects, holds or uses information about individuals;
- Copyright and Related Rights Act, relating to copyrights, patents, trademarks, use of the organization's name and logo, use of the organization's research, etc.;
- Provisions for specific types of services, such as legal and financial advice, work with children or vulnerable adults, or international work.
- The summary in Resource Material 3 provides a starting point for considering regulatory risk.

The process

The steps in the risk management process are:

- Recognise the hazard: in relation to a particular activity, service, duty, process, equipment, premises, etc., identify what is dangerous or risky and what can go wrong;
- Assess the risk: through discussion with people involved in the work and others with relevant experience, find out what they think about the likelihood of the risk occurring and how serious they think the effect will be if it does (see below);
- Determine the level of risk: based on probability and potential impact, determine whether the level of risk is low, medium or high;
- Clarify the risk culture and risk tolerance levels: in relation to these specific risks, determine whether the organisation is risk averse or risk averse (see below);
- Consider existing control measures: consider what procedures are already in place to mitigate such likelihood of mitigating the negative impact itself;
- Determine the residual risk: taking into account existing control measures, assess whether the residual or net risk is high, medium or low;
- set priorities: based on an acceptable level of risk and the level of residual risk, determine which risks are high priority and which are lower priority;
- devise an action plan to change what has been done or how it has been done to reduce risk.

Who should participate

There is a risk that only managers, or only finance and health and safety staff, are involved in risk assessment. The people who are directly involved in the work often know best what level of risk they can take and usually know best what are the ways to reduce the risks to themselves and others.

Risk assessment and management should involve relevant board and senior management team members, paid and voluntary staff and, if appropriate, people from outside the organisation with specific risk management experience in this area of work. A board member or manager should be appointed as the risk lead/risk manager to coordinate risk-related work.

Risk management is not a one-off task or something that is only done once a year. It is an ongoing process. It may be more sensible to set up an adaptive programme to assess the main areas of risk on a regular basis, for example a board meeting held once a year may look at financial management process risks, another meeting may look at client and service user risks, another meeting may look at premises and equipment risks. Only in this way is the board entitled to state in its annual report that it has considered the main risks to the organisation and has put in place appropriate systems to mitigate those risks.

In day-to-day work, the relevant staff must carry out regular risk monitoring. Of course, when an organisation starts a new activity or service, has new equipment, uses new premises (even on a one-off basis) or starts doing things in a new way, a risk assessment should be carried out and the necessary procedures put in place.

Culture of safety

Risk assessment and management is often done in a purely mechanical way, just ticking tasks off the list. Lists of issues can be very useful, especially for people who have not done this before, but they may not include one essential step: to determine the acceptable level of risk in the organisation in relation to each individual risk area. Bringing clarity to an organisation's safety culture is an essential part of risk management.

Imagine, for example, two community groups wanting to build a playground on a wasteland. One group wants to build an amusement park with lots of facilities for teenagers to encourage them to try new activities and test the limits of their courage. They realise that some children may fall and of course the organisers are trying to reduce the risk of serious injury if this happens. But they believe that it is only by taking risks, and perhaps by falling, that children can find out where their capabilities lie. This group takes risks in terms of their activities.

The other group is preparing a very different playground. They just want nice, safe swings and slides, and a low climbing frame. They know that children can hurt themselves - by running in front of the swings, for example - but they will do their best to achieve safety on the playground, perhaps by building a fence in front of the swings. This group is much more risk averse about their activities.

In terms of finance, however, the first group may be much more risk averse. They are reluctant to start work on the site until they have a 100% guarantee of costs and running

costs in the first year. The second group, meanwhile, is much more open to taking financial risks. They want to start with the necessary procedures with the landowner, hire designers to build the site and landscape architects, start the construction work and buy the equipment with only a 75% guarantee of the capital costs and no guarantee that they will be able to cover the running costs in the first year.

Many disagreements and conflicts arise in an organisation because the people working in it have different views on acceptable levels of risk. It is not hard to imagine the disconnect if the first group turns out to have a risk-averse IP and treasurer, or if the second group turns out to have an adventurous IP and a very cautious treasurer.

Discussions about levels of acceptable risk and reaching agreement should form the main part of all decisions about new activities or services, new approaches to fundraising and advertising, strategic planning, project planning, financial planning and policy development, and verification.

Risk management strategies

It is very important to remember that risk management is not risk avoidance. It is about recognising, assessing and managing risk - limiting the likelihood of its occurrence to a level acceptable to the organisation and reducing the negative impact if it cannot be avoided. Organisations that seek to avoid risk altogether will stagnate.

Ways to overcome the risk include:

- Risk avoidance: don't take risks;
- Risk mitigation: limit what is done or do it differently;
- improving controls: better policies and procedures, training, monitoring, statistics;
- Risk insurance: it will not prevent the risk from occurring, but it will limit the impact on the organisation and/or the person who is injured or otherwise harmed;
- transfer the risk to someone else: hire a contractor for this part of the work;
- Share the risk with others: create a joint venture;
- And finally, accept the risk. Nothing is ever exempt from risk.

In relation to the playground mentioned above, if board members are concerned (and they should be) about the risk of children being hurt, they should decide to avoid the risk by opting out of having the playground built. But that creates another risk - the lack of a place for children to play, and in their view that is not an option. They can mitigate the risk by consulting a specialist about the right equipment, by choosing reliable suppliers, by employing good staff and perhaps, initially, by limiting the types of activities on the site.

They can ensure good control by providing appropriate health and safety training, first aid and training in the use of all equipment on site; planning realistic on-call rotas so that there are always enough staff prepared for contingencies when the minimum numbers are not present; and properly recording all damage, no matter how minor. They can take out public liability insurance to pay the damages if someone is injured and the organisation is accused of negligence.

If all this seems too overwhelming, they can subcontract a specialist to manage the site or some of the activities, such as the children's football team. Or make the playground a limited company or partnership between themselves, a local sports club and a local adolescent/under 5 organization. However, sub-contracting and joint stock companies bring with them their own risks (see Resource Material 20).

Finally, if it does not want to reject the idea of the site, the board must agree that the organisation has considered the risks and has taken, or will take, appropriate measures to mitigate them.

Risks and risk mitigation measures must be subject to regular monitoring.

List of risk management questions

Do board members understand their duty to recognise, assess and manage the risks faced by the organisation?

Do all board members understand at least some of the potential risks that it organization faces?

Does the council or staff receive adequate information to help them understand and consider the risks and options when they have to make a decision about doing something different, doing something new, or doing something with financial or legal implications?

Do they specifically discuss the risk and reflect the results in the minutes?

Is the necessary attention being paid to developing a shared approach to different aspects of risk?

When something goes wrong, is there an emphasis on learning from the incident rather than criticising and blaming?