Guide on Business Resilience for NGOs

Erasmus+

CASSANDRA
KEEP YOUR BUSINESS GOING

Copyright

Liabilities

Clarification of Terminology

The simultaneous use of male and female forms of speech has been avoided for reasons of better readability. All personal designations are equally applicable to both genders.

A CASSANDRA PROJECT OUTPUT

Prepared by TOURNIS CONSULTING LP

In cooperation with

CPMS and emcra GmbH

AUGUST 2017

“We must free ourselves of the hope that the sea will ever rest. We must learn to sail in high winds.”

Aristotle Onassis

CASSANDRA Project Partners

emcra GmbH
Hohenzollerndamm 152,
14199 Berlin
Germany
Tel: +49 30 31801330
Email: info@emcra.eu

Tournis Consulting LP
Noti Botsari 9-11,
11741 Athens
Greece
Tel: +30 2102526321
Email: info@tournis-consulting.com

CPMS
Volonaki 14,
1045 Nicosia
Cyprus
Tel: +357 70003232
Email: info@cpms.org.cy

T-SOFT
Novodvorska 1010/14,
14201 Praha 4
Czech Republic
Tel +42 0261710561
Email: info@tsoft.cz

IBWF e.V.
Potsdamer Straße 7,
10785 Berlin
Germany
Tel: +49 30 53320645
Email: ibwf@ibwf.org

LVH
Mitterweg 7,
39100 Bolzano
Italy
Tel: +39 0471323200
Email: info@lvh.it

1. Table of Contents

Icons

Definition

Information

Attention

More information

2. The CASSANDRA Project

This guide is a product of the CASSANDRA project. “CASSANDRA” is an acronym for “Continuity And Security for SMEs Active in Neutralising Dangers and Risks affecting their Activities”. The aim of the two-year project (2015-2017), which is funded as part of a "Strategic Partnership" within the EU “Erasmus+" programme, is to improve the business resilience of SMEs. This specific version is a side-product of the project and focuses on the resilience of non-governmental organisations and bodies (NGOs).

2.1. NGOs[1]

In general

Non-governmental organisations, commonly referred to as NGOs, are nonprofit organisations independent of governments and international governmental organisations (though often funded by governments) that try to improve the lives of other people through humanitarian, educational, healthcare, public policy, social, human rights, environmental, and other activism and services. They are thus a subgroup of all organisations founded by citizens, which include clubs and other associations that provide services, benefits, and premises only to members.

According to the Council of Europe Recommendation CM/Rec(2007)14 on the legal status of NGOs in Europe, NGOs are voluntary self-governing bodies or organisations established to pursue the essentially non-profit-making objectives of their founders or members. They do not include political parties. NGOs encompass bodies or organisations established both by individual persons (natural or legal) and by groups of such persons. They can be either membership or non-membership

[1] http://www.associationline.org/guidebook/section/standards/action/read/chapter/2, https://rm.coe.int/16807096b7 (legal status of NGO in Europe), https://en.wikipedia.org/wiki/Non-governmental_organization, http://www.3sektorius.lt/docs/NGOGuidelinesforGoodPolicyandPractice_2013-01-17_15_21_00.pdf, http://164.100.133.129:81/eCONTENT/Uploads/CONCEPTS_AND_FUNCTIONS_OF_NGO.pdf, http://ec.europa.eu/social/main.jsp?catId=330.

based. NGOs are bodies or organisations that can be either informal or with a legal nature.

In the same recommendation several important areas of NGO operations are described. These areas are:

- Objectives,
- Formation and membership,
- Legal nature,
- Management,
- Fundraising, property and public support,
- Accountability and
- Participation in decision making.

The CM/Rec(2007)14 recommends that the governments of member states adjust their relevant legislation, policies and practice by the minimum standards set out in this recommendation and take these standards into account by monitoring the commitments they have made. They are also to ensure that these recommendations and the accompanying explanatory memorandum are translated and disseminated as widely as possible to NGOs and the public in general, as well as to parliamentarians, relevant public authorities and educational institutions, and used for the training of officials.

Types

NGO types can be understood by their orientation and by the level on which they operate.

By orientation:

- *Charitable orientation* often involves a top-down paternalistic effort with little participation by the 'beneficiaries'. It includes NGOs with activities directed towards meeting the needs of poor people.
- *Service orientation* includes NGOs with activities such as the provision of health, family planning or education services in which the programme is designed by the NGO and people are expected to participate in its implementation and in receiving the service.
- *Participatory orientation* is characterised by self-help projects where (local) people are involved particularly in the implementation of a project by contributing cash, tools, land, materials, labour etc. In the classical community development project, participation begins by defining a need and continues into the planning and implementation stages.
- *Empowering orientation* aims to help poor people develop a clearer understanding of the social, political and economic factors affecting their lives and to strengthen their awareness of their own potential power to control their lives. There is maximum involvement of the beneficiaries with NGOs acting as facilitators.

By level of operation:

- *Community-based organisations* (CBOs) arise out of people's own initiatives. They can be responsible for raising the consciousness of the urban poor, for helping them to understand their rights in accessing needed services and for providing these services.
- *City-wide organisations* include organisations such as chambers of commerce and industry, business coalitions, ethnic or educational groups and associations of community organisations.
- *National NGOs* include national organisations, professional associations and similar groups. Some have state and city branches and assist local NGOs.

- *International NGOs* range from secular agencies such as Ducere Foundation and Save the Children, SOS Children's Villages, OXFAM and CARE to religiously motivated groups. They can be responsible for funding local NGOs, institutions or projects and for implementing projects directly.

Strengths and Weaknesses of NGOs

NGO Strengths:

- The majority of NGOs are small and horizontally structured with short lines of communication and are therefore capable of responding flexibly and rapidly to customers' needs and to changing circumstances. They are also characterised by a work ethic conducive to generating sustainable processes and impacts.
- NGOs' concern is that they often maintain a field presence in remote locations, where it is difficult to keep government staff in post.
- One of NGOs' main concerns has been to identify the needs of their customers because they are spread all over the country. They have therefore pioneered a wide range of participatory methods for this diagnostic process and, in some contexts, have developed and introduced systematic approaches for testing new technology.
- NGOs have also developed innovative dissemination methods that rely on customer-to-customer contact, whether this is on a group or individual basis.
- In some cases, NGOs have developed new technologies or management practices. More often, however, they have sought to adapt existing technologies.
- One of the main strengths of NGOs has been their work in group formation. This has been in response to perceived needs at several levels:

(1) To meet the technical requirements of certain types of innovation.

(2) To manage common property resources.

NGO Weaknesses:

- NGOs' small size means that their projects rarely address the structural factors across society. Small size, independence, and differences in philosophy also obstruct learning from each other's experience and the creation of effective forums, both at a national and at a local level.
- Some ‘fashionable’ locations have become so densely populated by a diversity of NGOs that problems have arisen not merely of competition for the same clientele, but of some undermining the activities of others.
- NGOs have limited capacities for technological development and dissemination and limited awareness of how to exercise effective demand from government services.
- Some NGOs are more accountable to external funding agencies than to the clientele they claim to serve. Donor pressure to achieve short-term impacts, combined with a lack of cross-learning, has led in some cases to the promotion of inappropriate technology.
- Many NGOs place great emphasis on voluntarism. Whilst such concepts as ‘volunteer extension workers’ have great intuitive appeal and reflect widely commendable values, they are sometimes promoted at the expense of financially sustainable alternatives.
- NGOs usually cannot pay anywhere near as high wages as for-profit organisations can, meaning that they often lose star employees to the private sector.
- NGOs also have to keep facilities and equipment to the minimal needed to get work done - a reason why they try to get as much as possible donated, so they cannot be accused of spending money on ‘overheads’ rather than clients.
- NGOs also are bound by their mission - they cannot engage in activities that do not support their mission, whereas a for-profit can do whatever it wants to make a profit.

Approach of this guide

For the purposes of CASSANDRA and this guide, we focused our efforts exclusively on supporting the needs and requirements of NGO entities (organisations, associations and bodies).

The use of the term NGO (and NGOs) in the rest of this document refers to these entities and to the operations and services they offer.

3. Introduction

This Guide focuses on and has been written for NGOs. It aims to support the needs of NGOs in the specific area of Risk Management (including Information Security and Business Continuity concerns), and to help NGOs achieve an improved level of resilience in accordance with their individual needs, capabilities and invested effort and resources.

The CASSANDRA approach assists those involved in the entity strategy, management and operations of NGOs (that is the owners, members and/or managers) in a refined, simple, straightforward and practical way. It helps them to acquire the necessary awareness and knowledge of risk management, to understand in context how resilience management relates to their specific entity needs and, as a further step, to use the material and methodology provided in order to construct and implement an effective risk management strategy (also including issues of business continuity and information security), which is founded on informed decisions and a fit-for-purpose approach.

4. NGOs in risk

4.1. What is risk?

Risk is a common term that all kinds of people use every day. Definitions usually refer to a combination of the likelihood that an event will take place and the associated consequences (impact) that such an event would have. For the purposes of this guide:

> Risk is a current possibility (uncertainty) that may become a reality in the future and, if it occurs, may have a positive or negative consequence (impact) on/for your business / organisation[2, 3].

You may also see the term 'risk' used in several different contexts, for example:

- Risk in *Probability* ("There is a 30% probability that our team will win the game today.") (Extra question: How confident are you in the probability value?)
- Risk as *Uncertainty* about an event and its impact ("If there is an earthquake the building might suffer damages.")
- Risk as *Uncertainty* about the extent of an event's impact ("As a result of the strike we may lose between €20,000 and €40,000.")
- Risk as *Variance* from a forecast ("We expected to pay €10,000 in promotional expenses, but the final cost rose to €25,000.")

Risks (the impacts that uncertainties may have in a given set of circumstances) should be important to you because they may significantly impact your ability to meet objectives both in your own life and in the life of an NGO. These consequences (financial, reputational, legal etc.) may vary from being insignificant to threatening your life or NGO operation. They can be organised into different categories, such as financial, reputational, operational etc.

[2] ISO Guide 73:2009, definition 1.1.
[3] Principles of Risk Management, CRMI, the National Alliance for Insurance Education and Research, 2014.

4.2. ‘And there was risk’

Risk is everywhere and in everything. You cannot do anything without encountering risk[4]. Even doing nothing is risky!

Living itself involves risk. There are risks attached to eating (e.g. eating well means good health, eating carelessly increases the risk of disease, eating too little to keep weight under control can create a risk of vitamin deficiencies or anorexia) and risks attached to working (e.g. accidents that occur whilst traveling to and from work, accidents at work and work-related illnesses). Regular exercise may lead to good health, but it increases the risk of having an accident and breaking an arm or a leg. Not exercising or moving at all removes the risk of a broken leg but introduces the risk of a heart attack.

NGOs (whether active in humanitarian, educational, healthcare, public policy, social, human rights, environmental, and other areas to effect changes in line with their objective) are also a part of life that naturally fits in the same picture. Their existence intrinsically involves risk, which is why every year founders, donators and volunteers finance numerous new NGOs, at the same time as other NGOs are being closed down. In spite of this, the management of many NGOs invest and operate as if there is no risk at all, the so-called ‘not to me’ and ‘not me’ syndromes.

Risk may be introduced either as a result of your own activities, decisions and actions (e.g. changing your member fees, inadequately maintaining your ICT systems etc.) or as a result of external factors that arise in the wider societal environment (e.g. competition, legislation, financial stability in a country, end of a crisis related to the scope of an NGO etc.) or in the physical environment (earthquakes, flooding etc.).

[4] B. L. Cohen and I. S. Lee, “A Catalog of Risks”, Health Physics, 36, 707 (1979).

4.3. Positive and negative risks

Risks can be both positive and negative at the same time. Starting an NGO and opening a site or an office introduces us more fully to the world of risk.

POSITIVE RISKS (Opportunity Risks)	NEGATIVE RISKS (Losses Risks)
Having positively risked your effort and the money or effort invested in your NGO, you expect to receive a good return, to achieve your entity's objectives and to see strong revenues or an increase in membership in the years ahead if you manage it correctly. The closure of a local 'competitor' is a positive risk which creates an opportunity, provided you are resilient enough to adapt and support the sizeable number of new areas (those served or supported by the closed 'competitor') without compromising your quality or operating capacity. If you are not well prepared enough or do not respond well enough, this opportunity may turn into a disaster that results in the loss of your existing members or donors or volunteers base as well.	Negative risk exposures, such as computer failures and hacking, human errors, stronger than estimated competition and environment problems or natural disasters (e.g. flooding), may drive your NGO to bankruptcy if not treated properly.

Every NGO needs to be capable of managing the risks it faces and ensuring the best possible outcomes for both positive risks (achieving maximum success and securing the greatest advantage) and negative risks (minimising the exposure to and consequences of these risks). Moreover, every NGO must be able to respond to and deal effectively with new risks or environmental changes (whether simply potential risks or incidents that have actually happened and direct threaten its survival).

In other words, NGOs must raise their level of business continuity and capacity for "resilience".

4.4. Risks do not discriminate

No NGO founder, owner, member or manager wants to see their organisation closed down by a fire or earthquake, or the resignation of a key member (or even key employee), or the inability to deal with an unexpectedly large number of new members or volunteers or donors, or the unrecoverable loss of key ICT systems and data, or the leakage of privileged information, or any other negative incident, whether natural or man-made.

Unfortunately, most people who are involved in NGOs (including their managers) end up having the 'typical approach' to this:

- This will never happen to me!
- Where is the threat? I do not see any threats!
- Our organisation does not handle sensitive information.
- We are a small entity, risks and threats are for big organisations!
- Why would anyone want to hurt our organisation?
- I can deal with anything!

> Organisations, irrespective of their size and complexity, no matter where they are located, what they do, or how they perform, are directly exposed on an ongoing basis to significant risks and threats which, if not carefully treated in advance, may threaten the safety of their premises and the people in them, drive their beneficiaries or donors away, jeopardise their revenues, destroy their reputation and, as has often been the case, close them down.

In the case of natural disasters (flooding, earthquakes, avalanches etc.) or large fires, all organisations and businesses in that area will be affected, regardless of whether they are large, small, tiny, for profit or not-for profit. Equally, a strike by drivers in the transportation sector will - at a local and national level - hinder or block all transfer of goods, materials or people, equally affecting all types of organisations, whether large corporations or tiny NGOs.

In other words, risks and threats do not discriminate between large organisations and small ones. Small entities are just as likely as big ones to be hit by computer viruses, information hacking, loss of key personnel, fires or earthquakes or any other form of failure or disaster. In actual fact, small NGOs are far more vulnerable than bigger companies or organisations because they usually have either a lack of awareness about risks in their operational environment (“I do not see any threats.”) or tend to be overly optimistic about their exposure to risk (“It will not happen to us.”) or have few or no extra resources to counter risks.

4.5. How exposed are NGOs to risks and threats?

A survey, carried out by the Business Continuity Institute for the year 2015[5], exposed the risks and threats that businesses fear most:

[5] Horizon Scan 2015 Survey Report – BCI, 2015.

TYPE OF RISK OR THREAT	CHANCE OF OCCURRENCE
Cyber Attack	82%
IT and Telecommunication Systems unavailable	81%
Data leakage	74%
Utilities unavailable (power, water etc.)	57%
Adverse weather conditions	52%
Disruption in procurement	48%
Security incidents	48%

Although specific statistics solely for NGOs are not available, we have every reason to believe that an average NGO is little different than a typical business entity in relation to its preparation status against risks.

It is possible to identify three distinct categories of threats linked to the above input.

THREAT	**FIRST**	The first category includes some of the threats and risks that are feared most, such as those linked with information systems and security or the use of computer technology. This could be in connection with specialised applications (in the retail or printing market), or standard office technology (Word processor, email or internet browser). Although NGOs are not always computerised, they all depend to a greater or lesser extent on technology, just as with any other business. Where NGO personnel, members, volunteers or employees use computers to communicate with beneficiaries, customers, suppliers or banks, the information on their computers may be confidential (e.g. bank account details for suppliers and employees, sensitive personal data from partners and their own business, etc.).

CATEGORIES	SECOND	A second important category of threats and risks is the availability of networks (IT and telecommunication networks etc.) and utilities (electricity and water supply etc.) to support the day-to-day operations. The risk of having any of these services unavailable is crucial for the work of most NGOs and usually requires: (a) Identifying alternative ways of working in case of such an incident. (b) Communicating and exchanging information with the relevant authorities in order to estimate the downturn time and to plan accordingly.
	THIRD	A third category of risks and threats includes all risks that may reduce or remove any of an NGO's resources, assets or services. These could include the loss of offices due to a fire or earthquake or flood, the unavailability of key personnel, the loss or death of a board member, adverse weather conditions, failure of computer systems or communications, or loss of critical data. It may be necessary to have a contingency plan in place for the above risks.

4.6. Are NGOs prepared for risks and threats?

Although specific statistics solely for NGOs are not available, we have every reason to believe that an average NGO is little different than a typical SME in relation to its preparation status against risks. Few NGOs are usually prepared to deal with how their operations will respond if a risk or a threat becomes a reality. The most common reasons for a failure to plan and prepare are a lack of awareness or understanding, a lack of adequate finances and a lack of resources, particularly in terms of time and skill, both of which are scarce for most NGOs and are usually reserved for crucial tasks and activities at the core of their activities.

NGO people and managers are usually unfamiliar with threats and risks. They find these issues complex, technical and confusing, and, because they have far more pressing priorities, they tend to ignore anything that is not directly involved with the objectives and growth of their organisation. These risks are therefore often either overlooked or completely ignored.

Some of the major disruptive consequences of any incident on an organisation are:

a) Loss of productivity (they may not be able to operate for days or weeks)

b) Beneficiary dissatisfaction (beneficiaries will seek the services of other NGOs)

c) Volunteer, donors and partners withdraw (lack for extra funds and work to fund and restart the same effort from scratch again)

d) Increased costs (including wages, rebuilding expenses etc.)

e) Loss of revenue (inability to provide their services and keep donors, members and funding from grants going).

In light of this, it is doubtful that an average NGO will be able to overcome these consequences and return to normal conditions, unless they have completed serious preparation for the most likely threats and risks in advance.

5. What is resilience?

Put simply, resilience is the adaptive capability of an organisation to withstand and recover from loss, and to bounce back in the face of stress, complexity, chaos and ever-changing environments and situations[6].

For the purposes of this guide:

Resilience management is the adaptive capability of NGOs to control their exposure to risks and threats; to prepare for and be able to recover successfully from mistakes, disasters and crises; and to respond effectively to negative and positive incidents, environmental changes and new opportunities.

Changes, whether sudden or gradual, may occur because of any factor or reason. These changes doubtless have real or potential consequences for an organisation's property or operations. Changes could be made necessary by risks and threats, new opportunities, and external or internal events, whether locally, nationally or globally.

Resilience is not a state but a dynamic ability that is acquired and cannot be measured. The factors that may improve an organisation's resilience are different for each organisation.

Improving the resilience of an organisation requires the active management of exposures to threats and risks in all areas of the organisation's life, both internal and external (e.g. health and safety, physical security, information systems security, financial management, member management, etc.). It also requires an increased ability to respond effectively to unfamiliar or unplanned incidents (e.g. disasters, failures, crises etc.).

[6] ISO/DIS 22316 Societal Security – Guidelines for organizational resilience.

6. Improve your resilience with CASSANDRA

6.1. Can there ever be a risk-free environment?

Of course not! We live in an ever-changing world where nothing remains static. Every change that is induced or imposed (whether by us or others or nature itself) creates new risks and alters the extent of existing risks.

You can, however, work through the following three stages:

(a) Identify your risks and work consistently to have them under control in accordance with your current abilities.

(b) Monitor your environment and adapt promptly to any changes.

(c) Improve your ability to respond effectively to incidents or sudden emergences of risks and to handle crises effectively.

This guide and the CASSANDRA approach are designed to help your oranisation gain control of your risks. The only limit is the extent to which our human nature plays a role.

6.2. How does the Cassandra project respond to the needs of NGOs?

CASSANDRA key output was designed to support Small and Medium Enterprises (SMEs) resilience management. CASSANDRA's integrated approach comprises of[7]:

- A **Quick Check** tool to show you quickly a whole range of concepts and ideas for dealing with risks and improving resilience which are all tailored to your business.
- An **Online Course** to take you through the resilience management process, help you understand how to identify your particular threats and risks, evaluate potential implications and provide a clear route into taking the appropriate actions and implementing the best solutions. Most importantly, all this can be done without even leaving your office (or from home), since this is a work-based learning course!

[7] See www.cassandra-resilience.eu

- A **Guide for SMEs** (which is supported by the use of the above online course) that offers a powerful and informative presentation of the background that an SME owner or manager needs to understand before effectively implementing resilience management in an individual business context. This is done through a practical and structured approach and is supported by examples, techniques and templates.

The principles of resilience management (and the methodology to be followed) are exactly the same in the case of both SMEs and NGOs.

Typically, you may use the above tools to help you understand the overall resilience management approach and methodology, and then use this guide especially for the needs for your NGO.

This CASSANDRA output is designed specifically for NGOs. When it comes to **resilience management**, NGO managers require step-by-step professional support in an accessible format. This support should be **simple** but concise, **practical** but comprehensible, **oriented around implement-tation**, **adapted to their specific environment and needs**. **It should also** include a clear methodology and **practical steps** about what to do, what to achieve and how to be both efficient and effective.

6.3. Your benefits ('What's in it for you?')

There is a long list of benefits for any organisation that decides to **improve its capacity for resilience** by using CASSANDRA. Here are just a few:

- Increase the awareness and maturity of founders, managers, members, volunteers, and employees
- Achieve stability and secure your organisation's future
- Enhance your organisation's ability to adapt to a changing environment
- Ensure the safety of employees, beneficiaries and customers
- Protect your organisation's assets
- Minimise exposure to threats and risks and reduce insurance costs
- Minimise the possibility of your operations being interrupted
- Minimise your dependence on key people
- Minimise delays and evaluate the importance of existing procedures and operations
- Minimise negative legal consequences by meeting insurance, legal and regulatory requirements
- Protect your organisation's reputation and brand image
- Manage and recover from crises that threaten to disrupt your organisation's operations, thereby minimising all kinds of losses
- Maximise your possibility of succeeding in the future

And much more!

7. Starting the project for your organisation

7.1. Decision-making

The following two simple questions will show you the value of CASSANDRA and help you make up your mind about implementing it:

- Do I want my organisation to be prepared to deal successfully with risks, uncertainties and unexpected incidents in the days to come?
- Do I want a more resilient organisation as a result of just a few hours of effort?

If your answer is YES, then **YOU HAVE ALREADY UNDERSTOOD THE VALUE OF THIS PROJECT AND HAVE DECIDED TO START IT**!

We can assure you that the results will far exceed and remunerate the time and resources that you invest.

7.2. How do you use CASSANDRA to implement resilience management in your organisation?

For best results, we advise that NGO managers use **the online course, the quick check, the guide for SMEs and this guide in parallel**.

One common way of doing this is to:

1. **First visit the quick check tool**. This will introduce you to the basic concept of risk and resilience management in a few minutes.
2. **Focus primarily on the online course.** Each section of the course is based on and refers to a specific chapter or chapters in this guide. It is therefore **strongly recommended** that you **use the guide in parallel** with the course**.** Work step by step through the course, pausing after each chapter to read the relevant areas in the guide. There you will find detailed information that is not provided in the online course, as well as relevant tables and templates that can be used during actual implementation.
3. Implement resilience management in your organisation **whilst reading through the online course and guide for SMEs in parallel with this NGO**

guide. Alternatively, you could first read the course and the guide for SMEs and then start your implementation using this NGO Guide.

A minimum approach would be to read only this NGO guide and to implement the steps which it presents.

7.3. How long will your project last?

When it comes to decision making, time and effort are key factors. A project for an NGO will typically require:

1. **A big smile and a commitment to progress** (it only takes a few seconds to dream of a safer future for your organisation)
2. **Some project preparation** (this only lasts a few minutes)
3. A few hours to **run the project, along with an awareness and willingness to learn** (i.e. using the quick check tool and reading through this guide). You can divide this time over several weeks (this would typically take 1-3 hours per week for 4-5 weeks, although it may differ, depending on the size and complexity of an organisation and its work load).
4. **A conscious effort to implement the decisions made** during the project and time to follow up the results of its implementation. The amount of effort required (in total between a few hours and a few working days) depends to a large extent on the starting point of each organisation. This includes time spent buying and installing equipment and solutions, for example buying a fire extinguisher for the office, or buying and installing a backup system for the IT systems if this is not present, or buying and implementing antivirus software. This also includes the time it takes to prepare the organisation's disaster recovery plan and ensure that appropriate insurance coverage is in place.
5. Once the above cycle has been fully carried out, **a follow-up status assessment**, lasting about 1 hour every 3-4 months, might be required. **An end-to-end review assessment** of a few hours once a year will also be necessary.

On average, you will not need more than **a couple of hours each week over a few weeks to strengthen your organisation's preparation and greatly improve its resilience**. The results will fully justify the effort you invest.

7.4. Who ought to be in charge of the resilience management project?

NGO managers or those in charge of their operations are usually best suited to run the project.

They are the key individuals with a bird's eye view of all areas within their entity. They know their organisation's history and future objectives, its commitments and risk exposures, its members, beneficiaries and customer relations, as well as the economic, social, political and technological environment that their organisation operates in.

They should also be able to demonstrate managerial skills and lead authoritatively, particularly when it comes to making important decisions and implementing necessary measures.

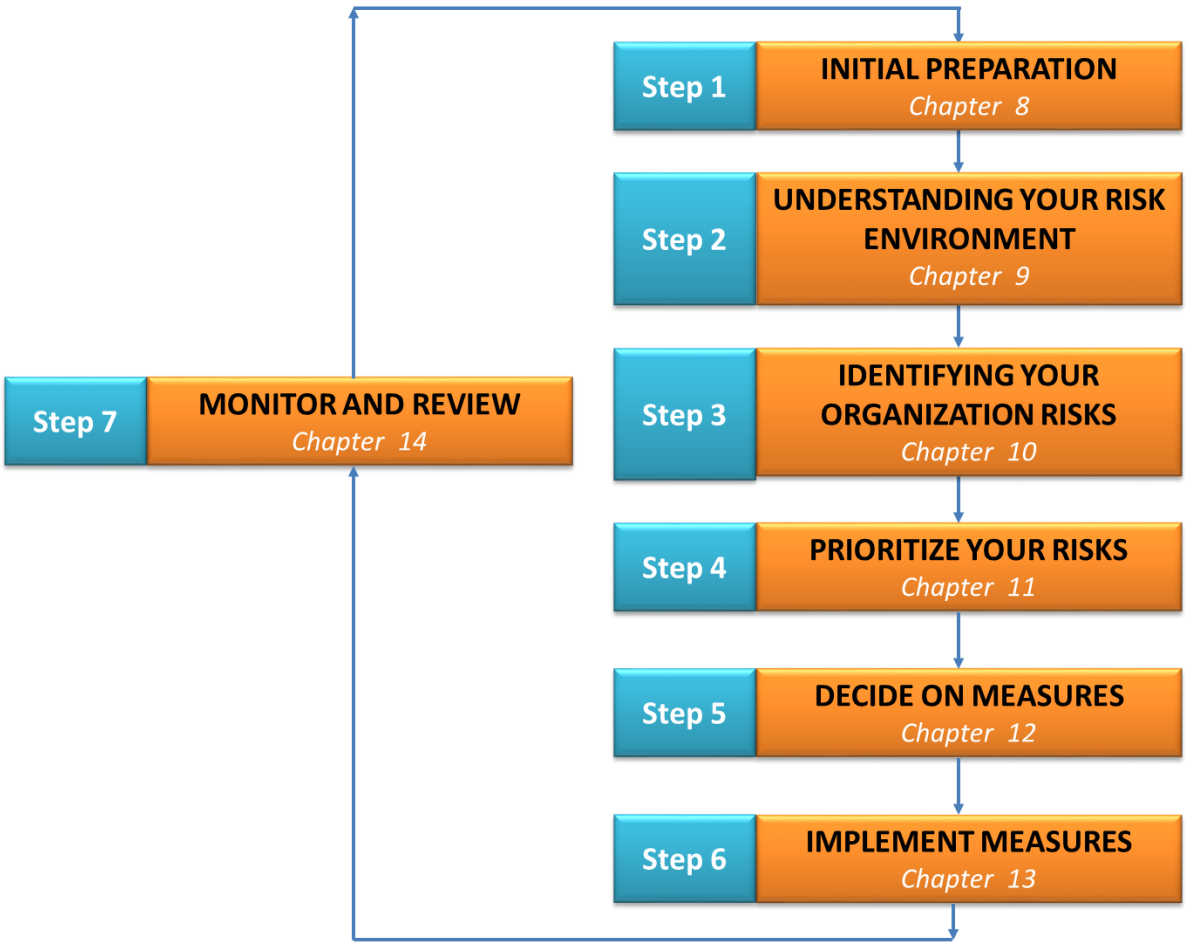
The specific skills given below would also contribute greatly:

- Project management skills
- Good communication skills (both internally with volunteers or employees and externally with third parties and relevant authorities)
- Some fundamental management qualities such as leadership, responsibility and integrity.

There is, however, no restriction against any other organisation employee or member also joining, attending and participating. In actual fact, all employees and personnel should participate and contribute throughout the project, beginning with risk identification through to the successful deployment of mitigation efforts.

7.5. The Resilience Improvement project steps to follow

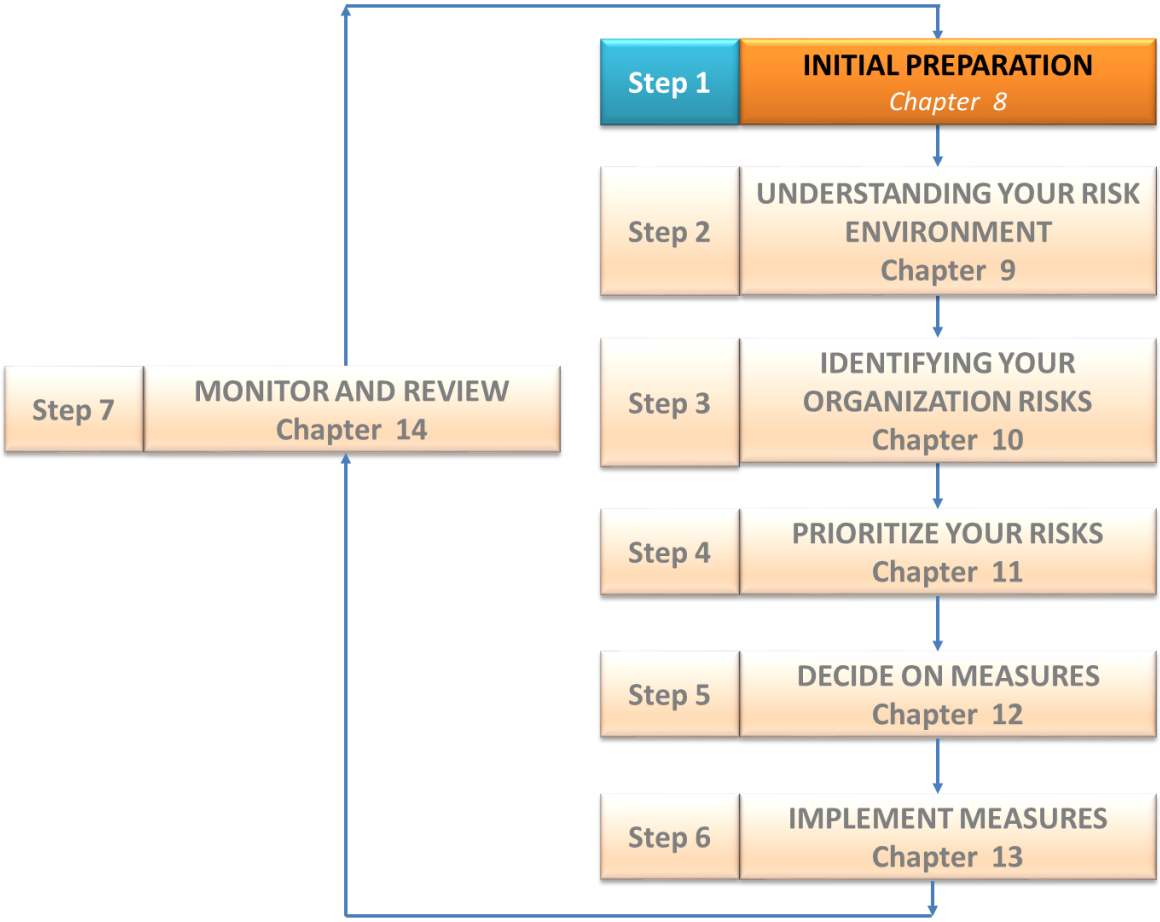
Resilience improvement is a journey made up of seven discrete steps, as presented in the following diagram:



Scheme 1 – Resilience Improvement Project Steps – CASSANDRA methodology

Each of these steps is explained in a separate chapter to follow. These steps are also directly linked to the chapters in the online course.

8. Step 1 – Initial Preparation



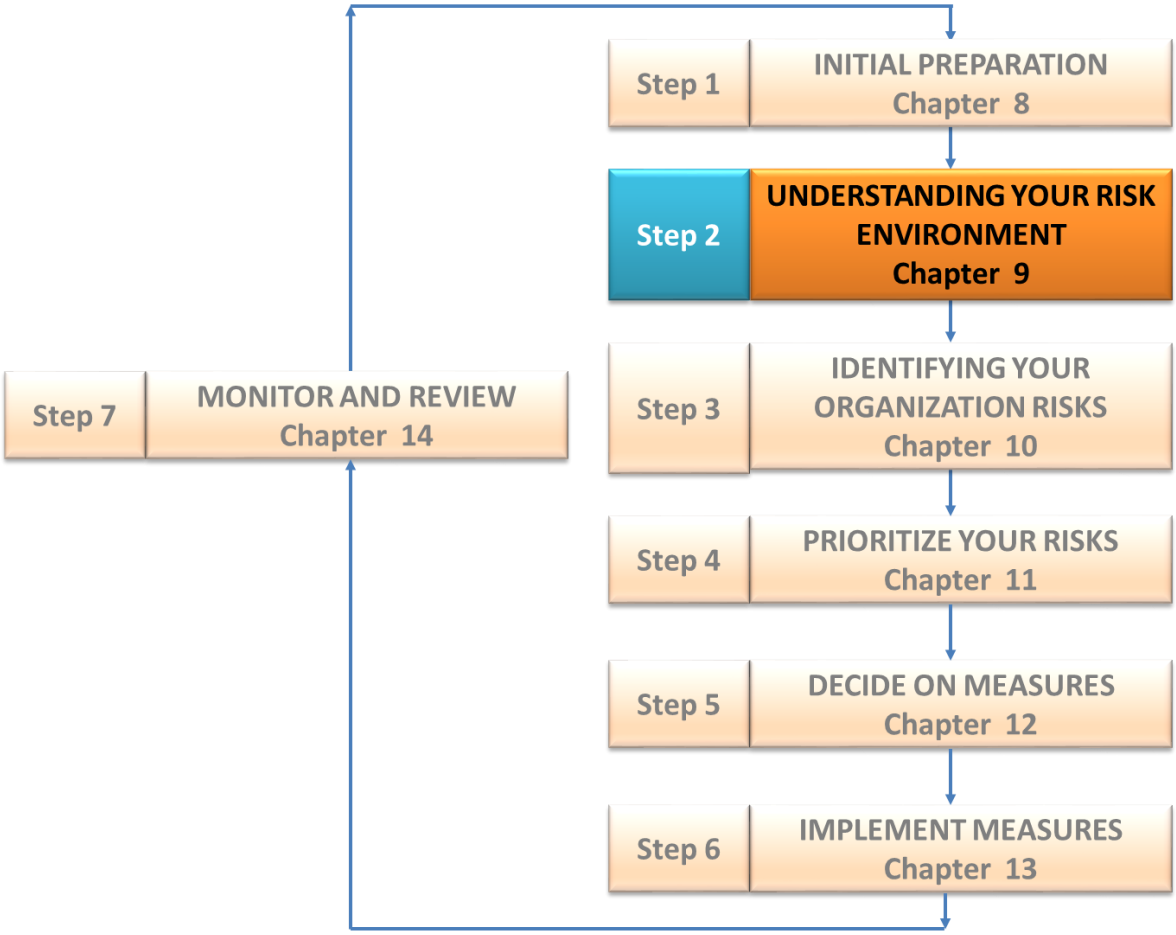
This stage is the fastest to implement once you have made the big decision to begin. All you need to do is:

- Get a copy of this guide (you have already done this!).
- Assign this project to an individual (it could be you, a manager or a high-ranking officer within your NGO).
- Mark the required time in your calendar: 1-3 hours each week for the next 4-5 weeks. Ensure that you will have no interruptions during this time.
- Inform all NGO employees that the organisation will be starting this project and that their assistance will be required and highly appreciated.
- Provide them with the web link to the quick check tool and explain that they need to go through it.

- Suggest that they work through the online course if they would like to.
- Get a pen and some paper. You will need paper for your notes and to prepare for the formal documents. You may also use the templates provided in this guide (documents and templates are provided as attachments at the end of the guide).

Use (if you want to – we advise it) your Excel or Word applications (or something similar) to record the time you spend, any documents and the results of the project.

9. Step 2 – Understanding your risk environment



The risks your organisation faces depend very much on the nature, scope and objectives of your organisation. Organisations that operate within the same sectors and that are of similar size may share basic similarities, but a closer inspection will show that **each organisation is unique**. Organisations also do not operate in a vacuum. Rather, there are many external forces that can influence an organisation or an entity.

Your first step towards organisation resilience should be to **examine and consider the particular characteristics of your organisation and the environment in which you operate**. Document any conclusions from this self-observation to guide your next steps.

When examining the context of your organisation, it is important to consider both **internal** and **external issues** that influence your operations.

External issues are factors beyond the control of your organisation that may impact its effectiveness to operate and its ability to meet strategic goals and objectives. External issues may include:

Social issues	Social issues can refer to problems that affect a significant proportion of society and often have considerable undesirable effects on the quality of life. Social problems are important to consider because they may affect your employees, your partners, your volunteers, your customers and beneficiaries, or the area in which you operate. Relevant social issues may include: • Crime and violence (high crime may require significant security measures) • Unemployment (low unemployment may mean that employees resign and change jobs more easily) • Lack of experts in areas relevant to your organisation, either as volunteers or employees • Poverty • Public safety and terrorism • Outbreaks of disease and other health issues • War • Political instability • Violation of Human rights environment • … Social issues can also refer to other factors, such as the preferences, interests and trends of society, and how changing social interests necessitate the transformation of business models.

Political issues	Political issues include issues relating to the state, government conduct and the administration of public policy. Political issues are also linked to the political climate in the region where your organisation operates (both nationally and throughout the European Union), as well as of regions where your organisation has interests. Political issues can have major implications on the work of an NGO, such as introducing new risk factors or causing considerable loss (e.g. loss of legality). Relevant political issues may include (although they are not limited to): • Official requirements (permits) • Legal matters and the administration of justice (e.g. access to and cost of exercising justice) • Government hostility • Copyright laws • Property and rent laws • Labour and trade laws • Healthcare for you and your employees • Environmental regulations • …

Economic issues	The state of the economy can have a significant impact on any organisation by affecting the revenues of the NGO, including donations, membership fees, grants etc. and supply and demand of an organisation's products or services. Economic conditions, such as a decline in overall economic activity or a drop in consumer confidence, can hurt an NGO. Economic factors worth considering may include: • The national economic environment • The local, regional, national and international competitive environment • The availability of capital • Interest rates • Taxes • Wages • The rate of inflation and deflation • …

Technological issues	Technology is constantly changing and this requires organisations to develop in line with technological progress. Technology can improve the way in which organisations deliver their services and produce their products, how employees and volunteers work and how NGOs market their products or services to potential customers and beneficiaries, as well as to donors and potential members. The need for organisations to continually adapt to a rapidly advancing environment presents many challenges for their stakeholders. Although keeping up with technology requires significant investment, ignoring the forces of technological change could prove disastrous for a business or an organisation. Technological issues to consider may include: • Mobility (mobile computing, mobile phones, universal email etc.) • Transformation of the workplace (e.g. working from home) • Cloud services • Social media (e.g. think of how your organisation is gossiped about on social networks!) • Information security (e.g. viruses, malware, loss of data etc.) • New promotion and distributive channels for providing services and products • New legislation regarding storage and use of data • …

Environmental issues	Environmental issues include factors that affect the location of an NGO, the countries and counties in which it operates, as well as regulations that govern which activities are permitted in relation to the environment. When evaluating environmental issues, it may be advisable to consider factors such as: • Geographical location • Proximity to beneficiaries and customers (linked to transportation of products and the delivery of services) • Climate and an organisation's natural or artificial surroundings • Weather conditions (including extreme cold, rain, snow, heat etc.) • Natural disasters (earthquakes, extreme temperatures etc.) • Energy requirements and expenses (e.g. cost of heating or cooling) • Availability and quality of public utilities • Environmental regulations • Toxic or hazardous materials (e.g. stored in a nearby environment) • …

Internal issues are factors within an organisation that are under its own control. Internal factors determine how an entity approaches its work and are crucial to its success. Internal issues may include:

Governance: organisational structure, roles and responsibilities	Governance refers to the framework of rules, policies, practices, processes and controls by which an organisation is directed, operated, regulated and controlled. Good governance can help your organisation reach its objectives and achieve long term success for the benefit of its stakeholders. Governance issues could be different for each NGO and directly related to the type, area, model and the way in which it approaches its objectives. Whether there are employees or just volunteers, whether there is a typical management structure or decision is made on a team level or at donor level directly influences the way an NGO is governed. Some aspects of good governance are: • Organisational structure and efficiency • Roles and responsibilities (these must be clearly and fully defined) • Decision-making processes (both for key and day-to-day decisions) • Succession (substitution) planning for management and employees • …

Strategy: policies and objectives of the organisation	An organisation's strategy is its vision for its future and the direction it must take to achieve its long-term goals. Choices made on the path to the future are dictated by its core values. Pertinent points include: • Organisation objectives (to be achieved in the future) • Vision • Operations (Business) Plan • Allocation of resources • Availability of resources • Delegation and decentralisation of responsibilities • Management systems (existence of written rules and operational processes and policies) • …
Standards	An organisation's standards refer to its agreed, adopted and established practices. Standards may cover service delivery and process management and are frequently supported by guidelines. This may include: • Standardisation of the production and delivery of products or services (to ensure consistent quality and / or control) • Written guidelines • Models for internal and external communication (e.g. standardised letter format, 24-hour complaint response rate etc.) • …

Resources and capabilities	Organisational capabilities are the competencies, expertise, capacity and materials that an organisation requires to fulfil its core functions. Organisational capabilities affect all areas, including membership, donors, finance, time, people, systems, technologies and supply chain management. Areas that you may consider include: • The knowledge and expertise of employees and management • Hiring and retaining qualified staff (where applicable) • Creativity and ability for innovation • Existing ICT systems and technologies (adequate, old or obsolete etc.) • Adequacy of personnel (or volunteers) • Number of employees approaching retirement • Financial capabilities • …

Information systems	Information is critical to the success of your organisation. Information systems process your data and provide information to support decision-making and operations. To maximise the value that information systems bring to your organisation, you should consider issues such as your current ICT systems, the extent to which your operations are assisted by or dependent on ICT, the flow of information, information security issues and the process of making decisions. Examples of key areas include: • Strategic ICT planning (what do I expect from ICT and how I will get it – am I already getting it?) • ICT Policies and procedures • Support and maintenance issues • Backup and disaster recovery issues • Information security (e.g. access control, malware, viruses, information leakage etc.) • Flow and distribution of information (amongst employees, customers, members or volunteers) • …

Internal or external stakeholders and other third parties	Stakeholders are internal or external groups with a shared interest in the success of your NGO. Internal stakeholders can be: • Founders, members • Donors • Managers and employees External stakeholders may include: • Beneficiaries • Customers • Partners • Suppliers • Contractors • Local government and community • Other NGOs Issues worth considering in relation to stakeholders may include: • The management of relationships with stakeholders • Their perceptions, values and interests • Effectively engaging and communicating with stakeholders • …

All of the above issues will have a bearing on the existence, operations and future successes or failures of your organisation.

It is probable that each of these areas may be hiding particular risks and opportunities that are relevant to you, which is why it is necessary to spend some time considering how they relate to your objectives.

Let's discuss some examples:

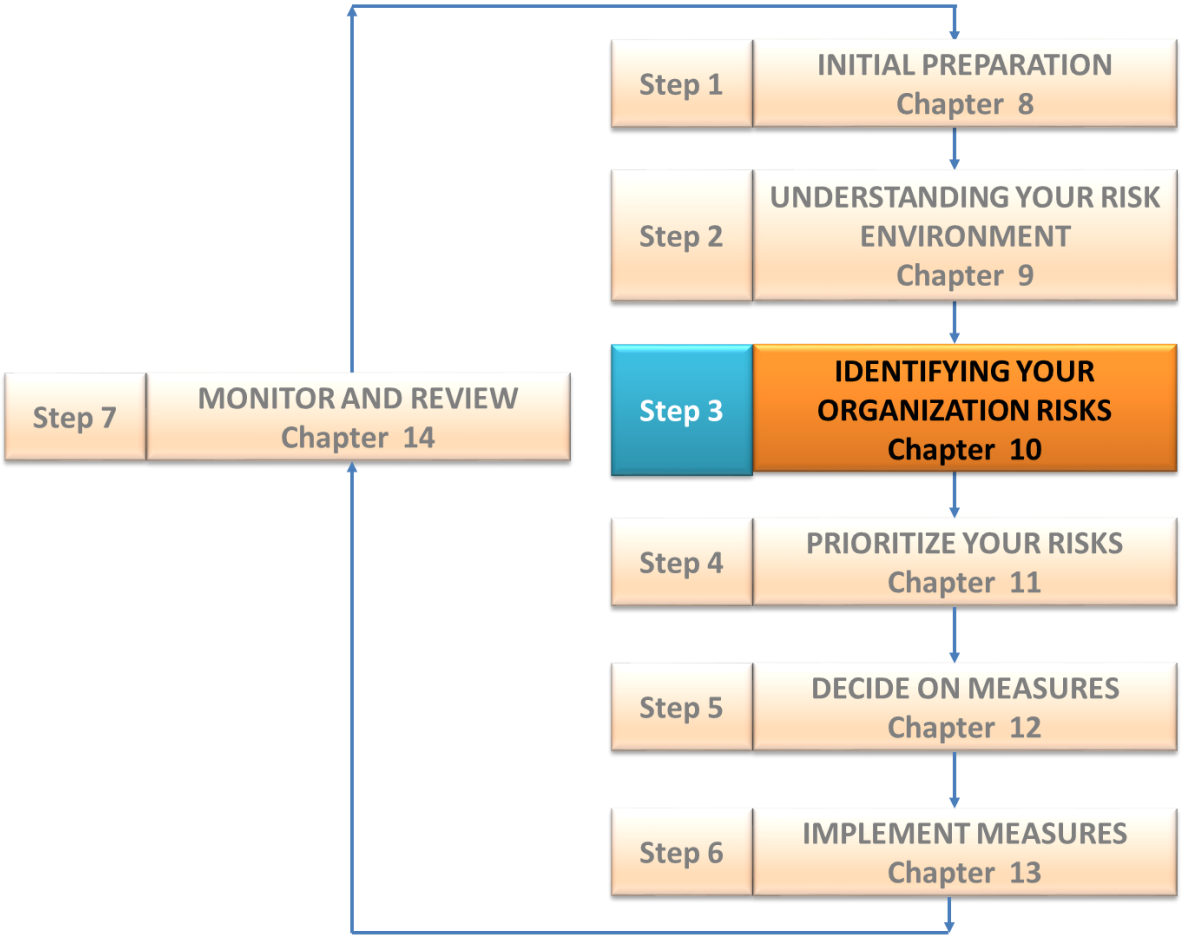
- High unemployment in your area will clearly make it easier to find new employees, but a lack of experts in your specific areas of interest will make it more difficult to replace an employee that has retired or left your team. Unemployment therefore poses both a positive risk (and an opportunity) and a negative risk.
- External factors and issues related to local or global politics may well influence your NGO. A terrorist attack, for example, may result in restrictions in the operations of some NGOs within a specific area or county, causing severe damages to them.
- A further example is working with old (or obsolete) ICT technology. This exposes you to several risks, including:
    - Problems finding ICT experts to help you with technical problems
    - Difficult and expensive maintenance or repair once an IT device fails
    - Reduced productivity (slow IT systems, lack of memory etc.)
    - Exposure to viruses and hacking since these systems are often not supported by their makers against the new, and more aggressive, viruses that are appearing every day.
- Not backing up precious data and information on your ICT systems (including laptops) is a considerable risk. Hard drives in IT systems usually fail without warning, resulting in the permanent loss of the data.
- Failure to have a simple business plan and yearly strategy exposes the NGO to risks connected with poor financial management, poor resource management and personnel cost, unknown ability for making a profit and inability to effectively respond to sudden negative environmental changes or negative incidents.
- Not having written, standardised guidelines and processes for key activities may result in customers and beneficiaries receiving varying levels of service quality (since employees or volunteers may not have a standard way of working). A lack of documentation could be severe (even catastrophic) if a key employee were to leave the organisation without prior notice.

- Flu pandemics or seasonal illnesses can often cause extended employee absences from work, thereby resulting in poor or no customer or beneficiary service during high seasons. This is a high risk at all times, especially if your NGO provides personnel-related services (e.g. an organisation that offers a service).
- The geographic location of your NGO is directly related to weather risks and possible natural disasters (e.g. areas prone to snow storms or heavy winters or heatwaves). Being located near a river with a history of flooding in recent years is also a risk worth considering. Organisations in countries like Greece should assess the risk of an earthquake and consequences it would entail. If you are located near a forest, especially in the Mediterranean area, the risk of fire should be considered. Other issues could arise if you are located near a site where hazardous materials are stored (such as a gas station), or located in a city area where the public often demonstrates or which is poorly monitored by the police.
- The failure or withdraw of a key partner or donor is something you should also consider, especially when a significant part of your revenues or funds highly depend on this partner.
- Poor contract management (i.e. not paying attention to the terms, requirements or commitments of a contract) may cause you severe losses, and in certain cases could result in the closure of your organisation.
- A reputational issue (e.g. a scandal) a donor or funding organisation may cause loss of customers, supporters or volunteers (and of course loss of funds) to an NGO.

We could go on to list hundreds of further examples of exposure to risk. We chose these examples, to show you some of the risks that a typical NGO might face. The most important objective of this chapter is to help you to consider, analyse and understand your organisation's overall environment (both internally and externally), and the relationship this has on your exposure to risk.

Once you have reached a good understanding of your NGO context, you are ready to move on to the next step.

10. Step 3 – Identifying your organisation's risks



10.1. All of the risks?

This is one of the most important steps of your project. It is perhaps the most important, because failure to identify a specific risk means that none of the following steps can be applied to that risk. The problem with this is that the risk remains an unseen and bypassed issue that may materialise at any moment, leaving you unaware as to how to manage it, simply because you failed to identify it initially.

It is, however, important to bear in mind that you will not be able to trace, recognise or identify every single (100%) hazard and risk in place or all of the threats that may exist. This is impossible. We are all humans, and our efforts are limited because of this.

What you really need to know: if you work systematically and follow a specific methodology then you can be confident that you have – in accordance with your

teams, personal abilities and limitations – done your best and have most probably identified all major critical and significant risks linked to your entity.

Another important point: the results of a risk identification effort may be more productive (in terms of the number of risks identified) if this is carried out by an expert (instead of by you). Whilst this may be true, you should bear in mind that, by following the suggested approach and giving the required time and attention to this activity, your work will not at all be inferior: by the end you can be certain that you will have identified the vast majority of risks linked to your operation environment.

Last but not least: you should keep in mind that the work you have done will be a specific picture of your organisation's risks at the specific point in time at which it was completed. By next week there may be different risks than those you have identified today. Even by tomorrow your NGO may face new risks due to a change in the legal or state environment (e.g. a new legislation) or due to an unexpected threat (e.g. a terrorist attack) that was not there yesterday.

This does not mean that you must repeat the risk identification every day from scratch and start the CASSANDRA methodology again from the beginning. A good identification effort will typically provide you with a list of all the significant risks, the vast majority of which will continue to be there tomorrow or for the coming few months (unless you mitigate them or deal with them). All you have to do on the following days is spend a few seconds asking yourself this simple question: "Out of all of today's activities, changes and new developments, has my organisation been exposed to any new (unidentified) risks?" If the answer is yes, then this newly identified risk can be added to the list and treated separately. Assessing and treated just this specific (new) risk – if it is an issue – will require only a few seconds or minutes of your time.

Stepping back to look at the big picture, **this methodology requires you to run the risk identification process fully at least once every year or after every significant change to check if the risks that you documented in the original list still exist or need to be removed. During this annual effort you will also be able to add any newly identified risks.**

Although the list will never be empty, following the CASSANDRA methodology will definitely result in a small or very small one for the periods to come. And the really

good news is that your organisation will be less and less exposed to risks in the future.

10.2. Risk categorisation

You will not be able to systematically identify your risks unless you approach your NGO and its environment through a category filter. This will allow you to separate out various context areas and draw your attention to one area at a time to ensure that in-depth study has been done. Categorisation may vary between NGOs and depends on their area of operations and the risk manager (who is you by the way!). There are also several viable approaches that can be found in relevant literature or online. For the purposes of this guide, however, we propose the following seven risk categories (based on best practices) as the most suitable for **NGOs:**

1. Scope-related and strategic risks
2. Operational and continuity risks
3. Financial risks
4. Technology, ICT and information security risks
5. Regulatory and legal risks
6. Human resources risks
7. Governance and stakeholders risks

In the following paragraphs we will analyse each of these categories and provide specific examples to help your risk identification. You may also discover that risks included under one category could also be included in another similar or different group. This is not a problem because the aim is to finally identify risks, regardless of which category they might fall under.

10.2.1. Scope-related and strategic risks

These are risks related to:

(a) The specific area and market (local or international) in which the organisation is targeted or engaged to

(b) The overall business and societal environment

(c) The strategies and strategic goals of your organisation.

In order to be successful, it is imperative that your NGO has a well-thought-out business plan. Strategic risk is the risk that your organisation's strategy may become less effective, and may therefore struggle to reach its goals. This could be the result of technological changes, powerful new competitors entering your local 'market', some shifts in customer and beneficiaries demand, a change of view and perspective of donors, an increase in your usual costs or any other large-scale changes.

A non-exhaustive list of areas to be considered could include:

- "Market" risks (and operational area risks)
- Political environment
- Competition (by similar NGOs)
- Public safety status
- National economy
- Changes in customers and donors behaviour
- Changes in the demand for services or products
- Labour laws (both any changes and existing problems)
- New disruptive technologies
- Changes in protectionism
- Rising costs for labour or raw materials
- Investment risks
- Brand and Marketing Communication
- Risks to your reputation or your donor's reputation
- Fraud and corruption
- Obsolescence of intellectual property
- Poor quality control and service placement
- Ignoring your donor's wishes

- Unintentional disrespect of your donor
- Lack of transparency on leadership, distribution of funds etc.
- Failing to comply with charitable registration laws

10.2.2. Operational and continuity risks

These are risks associated with the organisation's operations, its services, the activities carried to provide its services, and administration activities. It also includes risks related to ongoing operations (in the context of disasters and negative incidents). Operational risks refer to unexpected failures in your organisation's daily operations, whether these are caused by technical failures, people, or any other process failure.

A non-exhaustive list of areas to be considered could include:

- Poor quality service delivery
- Poor project management
- Risks in logistics and transportation
- Compulsory changes and the ability to deliver
- Contract management risks
- Insurance management and current coverage (including management and personnel liabilities)
- Outsourcing management
- Human error in operations
- Labour disputes and strikes
- Forgery
- Fraud
- Epidemics, pandemic flu
- Succession or substitution. Organising management and employees
- Water leakage, plumbing failures

- External or Internal power supply
- Power surges or spikes
- Failure of heating, ventilation, air conditioning
- Machinery breakdown
- Loss or destruction of property
- Hazardous materials: chemical spillages and contamination (connected to nearby production, transportation and storage)
- Internal fires: severe/major/minor
- External fires: severe/major/minor
- Dust storms
- Earthquakes: severe/major/minor
- Flooding and drought
- Landslides
- Heatwaves
- Hurricanes, typhoons, windstorms
- Snow and ice storms
- Volcanoes
- Strong winds, hurricanes, tornadoes
- Tides and tidal waves
- Physical security and site access
- Health and safety equipment and measures
- Theft or burglary
- Bomb threats
- Kidnappings
- Terrorist attacks

- Traffic or vehicle accidents
- Rail, aviation and maritime accidents
- Armed attack on facilities
- Collateral damage from airstrike or fighting near the NGO's facilities

Operational continuity risks are related to the stoppage or disruption of an organisation's operations because of a disastrous event, whether a fire, earthquake, flood or kidnap or negative publicity etc.

They also include the unavailability of staff, key suppliers, grant providing organisations and donors as well as the services of key partners. Because they are specific risks, their treatment (discussed in the relevant chapter later on) requires a specific approach and preparation.

10.2.3. Financial risks

These cover all financial areas of the organisation's lifecycle, whether capital, financial planning, funding, costing and pricing, collection of revenues etc.

A non-exhaustive list of areas to be considered could include:

- NGO capital
- Supplier payments
- Collection of funds
- Collection of members' debts
- Management risks with operating expenses
- Capital expenditures
- Budget management
- Accounting and financial management
- Social insurance payments
- Cash flow and liquidity
- Access to credit and credibility

- Interest rates risks
- Currency risks
- Cost estimation
- Sales pricing structure (and loss / profit / expenses coverage margins)

10.2.4. Information and communication technology (ICT) and information security risks

Technology risks are those related to all kind of technologies that the organisation uses (e.g. computer systems for accounting or members management or members communication etc.).

ICT systems are usually used by organisations as a part of their core operations and address administrative, communicative and marketing issues. Almost all organisations use ICT systems today as part of their administration and management activities (whether a single PC or a laptop, or a small office network of computers).

10.2.4.1. Identifying your information assets

In order to help you identify the relevant risks, it is important that you have a clear picture of what is included in what we call “ICT systems”, or, in other words, your “Information Assets”.

Because information is not always stored electronically, the term “Information Assets” also refers to any other form of information, for example information “stored” on papers or printouts.

The following table is designed to help you identify these assets:

GROUP	DESCRIPTION	ASSET EXAMPLES
IT Systems	We use the term “system” to refer to a “unit”, including hardware, software and data that are used to process information. For example, by referring to our “ERP System”, we mean the server that hosts the ERP application. This application and the ERP data are stored on the server drives. A printer is also an IT System.	• Servers • PCs • Laptops • Workstations • Backup system • Storage system • Printers • USBs • CDs • External disks • Smartphones • …

GROUP	DESCRIPTION	ASSET EXAMPLES
Network	Devices required to set and manage the organisation's IT system network. A network includes all cabling, routers and modems used to connect to communication lines.	• Cabling • Switches • Routers • Wi-Fi
Communication	Connections to other voice and data networks, provided by telecom companies.	• Data and internet lines • Voice lines
Applications	This refers to software applications and the tools used to process information. These are installed within IT Systems.	• ERP • Email • Internet browsers • WEB site • MS Office (word, excel etc.)
3rd Party systems	These are services provided by 3rd parties that are related to IT systems, such as applications that are owned by 3rd parties but which provide access for others to use and benefit from.	• Cloud storage services (we use the storage and disks of 3rd parties to store our data) • Cloud applications (using applications that are stored in the cloud and are not on our IT systems)

GROUP	DESCRIPTION	ASSET EXAMPLES
Other forms of stored information	Examples of this include paper documents, people's knowledge, printouts, etc.	• Supplier Contracts • Employment Contracts • Application forms (paper) • Patents • Registration forms (paper)

We suggest you use the "Information Technology and Communication Systems" tables provided in **Chapter J, paragraph J4b** of the Annex **18.3 Business Continuity Plan Template**, to document your organisation's information assets (see also chapter **13.12.6 Action 5: Prepare a resources and operations recovery plan**). Use the first column of the template to document all your information assets.

ICT systems are exposed to specific risks:

(a) Related to their operations (e.g. poor or bad performance, equipment failure or breakdown, power loss etc.)

(b) Related to a specific category of threats, information security threats, that require a particular degree of knowledge and expertise to be identified, understood and treated.

10.2.4.2. IT infrastructure and risks related to operation

These are risks related to your ICT systems and, more specifically, to the way in which these (a) were required, designed, purchased, and implemented and (b) are now operating and managed.

We usually identify threats and risks by using the list of the information assets and filtering them through a four-layered approach:

a. Organisation and administrative layer (identifying risks or threats that are related to the way in which you manage your ICT systems and their operations).

   Here are some examples:

   - Nobody has checked the quality (and quantity) of the equipment ordered and delivered, whether in the past or present.
   - Existing applications (membership management applications, office applications etc.) do not fit properly and are inadequate for the organisation's needs due to poor specification management when they were purchased.
   - There are no written instructions for how to use the applications delivered by the sellers (they were either not requested or simply do not exist).
   - Training for users on how to use the ICT systems is poor, resulting in a significant number of mistakes each day. New employees are not adequately trained.
   - ICT equipment is not maintained properly or in accordance with the seller's specifications.
   - Because there is no problem-solving process within the organisation, employees do not know how to resolve technical issues or improve the performance of their ICT systems.
   - …

b. Technical layer (identifying risks or threats that are related to the organisation's ICT system technology and its implementation).

   Here are some examples:

   - ICT Equipment purchased is of poor technical quality.
   - Data communication lines are poor quality or run at a low speed and do not support the organisation's needs.
   - There are not adequate controls in the software for applications and the programme does not check the quality of the data entered.

- Buying poor quality ink cartridges causes the printers to malfunction.
- …

c. Physical layer (identifying risks or threats that are related to the 'box structure' of the ICT systems as well as how these are physically installed or operated within organisation premises).

   Here are some examples:

   - Servers and main IT systems are stored randomly throughout your premises.
   - The side covers of server boxes are left open after maintenance (exposing them to dust, water, falling office items etc.).
   - Network cables are left unprotected and strewn around.
   - …

d. Human layer (identifying risks related to human and personal involvement).

   Here are some examples:

   - Errors in daily operations as a result of poor training or personnel behaviour e.g. poorly trained users making errors and mistakes in producing results when using IT systems.
   - Human errors e.g. processing and entering data incorrectly, deleting data or destroying paper files carelessly, opening infected email attachments etc.
   - …

10.2.4.3. Risks related to information security

Information security refers to the protection of an organisation's information and information assets. Information and information assets might be data stored electronically such as in disks or CDs, or IT systems that store and process data and information, or communication systems that transfer data between your systems, or IT applications such as ERP and email, or paper files and archives kept in drawers. This information can include intellectual property rights, business secrets and patents.

Protecting information assets, and thereby maintaining information security, requires the protection of the three elements (CIA triad) that are considered to be the most crucial components of information:

- **Confidentiality**: information is not made available to or disclosed to unauthorised individuals, entities, or processes.
- **Integrity**: maintaining and assuring the accuracy and completeness of data; protecting data from unauthorised or undetected changes, including deletion.
- **Availability**: protecting information and ensuring that it is available when needed.

Maintaining information security for your ERP data, for example, means protecting data confidentiality (not disclosing information to unauthorised parties), data integrity (not changing or deleting data without the proper authorization, whether deliberately or accidentally), and data availability (data and IT systems should be available at all times, regardless of system failures or onsite disasters).

The pertinent threats and risks are, therefore, those that are connected with or threaten the confidentiality, integrity and availability of your NGO's information assets.

On their own, information systems are only part of the bigger picture. The reality is far more complex.

As you work on identifying the risks and vulnerabilities of your ICT systems, you will need to think once again about the following four distinct layers:

a. Organisation and administrative layer (identifying risks or threats that are related to the way in which you manage your ICT systems and their operations).

   Here are some examples:

   - No one is in charge of security issues within your organisation.
   - There is no policy or managerial decision about who may access ERP or email applications.

- No one bothers (or even thinks) to delete a user and remove their privileges from the system after they have left the organisation.
- A risk assessment is never carried out.
- Employees are never trained or made aware of what phishing is and how to deal with it.
- IT data is never backed up.
- Employees share their passwords with each other in order (they believe) to be more productive.
- There is no business continuity plan in place.
- …

b. Technical layer (identifying risks or threats that are related to the organisation's ICT system technology and its implementation).

Here are some examples:

- Several applications are still in use although they are very old and obsolete, thereby creating an opening to known security issues.
- Site Wi-Fi is open to all employees, neighbours, visitors and passers-by.
- Patches and updates are never applied to any application.
- Data on backup tapes that are send out of office is not encrypted.
- There is no spam filter on incoming emails.
- Users have access to any web site, including online games, gambling and porn.
- Anyone can access any of the organisation's systems from home.
- There is no backup in place to recover accidentally deleted data.
- …

c. Physical layer (identifying risks or threats that are related to the 'box structure' of the ICT systems as well as how these are physically installed or operated within organisation premises).

Here are some examples:

- PC's and laptops are always left open and are next to the reception desks so visitors can read the information on their screens.
- No one knows what the organisation's ICT equipment comprises of. There is no list of assets.
- USB sticks are left unprotected at the reception area.
- Important or critical papers are left out on desks because there are no areas of controlled access where they can be stored (e.g. locked drawers).
- There is no out-of-hours intruder alarm.
- Everybody, including ex-employees, has site keys.
- Unprotected cables are all over the floors, around desks and in the corridors.
- …

d. Human layer (identifying risks related to human and personal involvement).

Here are some examples:

- Dishonest staff – fraud. Theft of data or sensitive information by employees for personal benefit (e.g. data that is of interest to competitors).
- Intentional alteration of data (including the deletion, modification and insertion of data stored on systems).
- Illegal data manipulation for various reasons, such as covering process errors and avoiding penalties. One example is employees changing financial statements to avoid being blamed or fined by the authorities for missing report deadlines.
- Installation of malicious or illegal software on organisation systems.
- Unconscious or accidental disclosure of confidential NGO data and information by employees on social media, for example an employee sharing details with his friends on Facebook about an important project that he delivered and is very proud of.
- …

Some risks can also be categorised under more than one filter. Just putting them under one filter does not, however, change the action that is required.

10.2.4.4. Specific information security risks: cyber risks

"Cyber risk" refers to any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

Internet, the availability of public access networks, increasingly interconnected ICT systems, the storage of large amounts of personal and valuable information on IT systems, the increasing dependency of organisations on ICT systems, employee use of personal devices (smartphones, tablets or laptops) within organisation networks, globalisation, social networks and, not to be forgotten, games like Pokémon Go, all create a world that is becoming more and more complicated each day and makes information protection an extremely complex challenge for organisations of all sizes. Organisations rely more and more on cloud services, use websites for e-commerce and e-business operations, use online services from other companies (both locally and globally), make electronic payments and process credit cards.

All of these make ICT systems more and more attractive for criminal activities such as data theft, illegal access, fraud, blackmail, sabotage, as well as many other crimes related to intrusion, information access and the disruption of ICT systems. This is done by "hackers".

"Hackers" are people or ICT systems that look for weaknesses in computer systems or networks to exploit.

Their efforts are motivated by:

- Profit (data theft, especially in the case of personal information, money, intellectual property, extortion of businesses and their customers, corporate espionage by rival organisations etc.).
- Protest ("hacktivists" who focus mainly on conveying a political message).
- Challenge (e.g. breaking into the CIA's system just for the fame).
- National interest (espionage by foreign governments).
- Enjoyment.

- Many other motivations (including legal reasons, such as being hired by an organisation to evaluate weaknesses and help remove them).

Hackers employ many different tools and methods, including:

- Malware or malicious software: covers software codes such as viruses, spyware, Trojans, worms and more recent ransomware. Malware is designed to steal or destroy data, spy on the actions of users, criminally abuse user systems, or extort money from the users.
- Phishing: hackers send email scams with the aim of obtaining personal and financial information from the recipient.
- Spear Phishing: usually done by someone known to the target, who communicates on a personal basis and tries to deceptively obtain personal or financial information.
- Denial of service (DoS) attacks: hackers attack the targeted system (usually a website), “blocking” the system and stopping the system from performing.
- Software security flaws: weaknesses in the security of an application as a result of programming errors. Security flaws can be exploited by cyber attackers to gain access to user systems, steal data and perform other malicious acts.
- Change of internet content: hackers attack websites and change the site content to expose the organisation’s image negatively to its online customers.
- Inappropriate or malicious internet content: hackers attack websites, controlling them and using them as a basis for further attacks. Compromised web sites can be used for impersonation attacks (phishing), to spread malware, or to distribute inappropriate content.

It is important to remember that a risk may not only come directly from an unknown source. Risks to your ICT can come from trusted connections and the networks or ICT systems of fully trusted business partners, simply as a result of them being hacked.

Every NGO, even one just using a single PC, should keep these risks in mind.

10.2.4.5. Wrap-up

This chapter has taken a more analytical approach because, for an average NGO, and due to the nature of information technology and information security, these are key areas of concern where there continues to be a lack of understanding, in-depth knowledge and familiarity amongst employees. Addressing these areas usually requires common sense and the help of an expert (your ICT Consultant or the provider of your ICT systems and solutions). In the latter case it is also necessary that you understand the underlying risks of this dependent relationship.

A non-exhaustive list of areas to consider during your identification of risks could include:

- Accidental deletion of data.
- Incorrect entry of data.
- Workstations or computers that can be accessed without a password.
- Insufficient or non-existent software licences.
- Insufficient training of new or temporary employees or users.
- Need to access critical files when an employee is absent (they are locked on his computer).
- Files lost or misplaced by users.
- Lost mobile devices.
- PC's sent to third parties for repair with their disks full of organisation data.
- Lack of documentation for users and administrators.
- Failure of application software (due to problems with software or hardware, employee errors etc.).
- Failure of central computer equipment.
- Communications failure (vocal): problems with a telephone centre or provider.
- Hardware malfunction.
- The impact of power failures on information and data.

- Failure of equipment.
- New or upgraded software corrupting documents and files.
- Software malfunction.
- Software upgrades affecting availability of data or other programmes.
- Availability of files stored in PC directories and failure of PC disks.
- Backups that are poor (no one is sure what is backed-up) or non-existent.
- Backups that are not verified.
- Backup media that is never verified.
- Backups that are stored in the office.
- Faulty hardware.
- Faulty programming.
- Loss of system or equipment availability.
- Approval of unauthorised or fictitious transactions.
- Information accessible to cleaning staff in the evening.
- Premises or information accessible to former employees or ex-members.
- Confidential or restricted areas physical accessible to unauthorised parties.
- Physical disclosure of sensitive or privileged information.
- Physical intrusion by unauthorised parties.
- Poor security in the working area.
- Incorrect or inappropriate file access for employees or members.
- Forgery of documents sent out for authorisation.
- Fraudulent programming that impacts the integrity of data.
- Accessibility of malicious internet sites.
- Hacking.
- Phishing.

- Computer viruses.
- Reports disclosed to unauthorised or unintended parties.
- Denial-of-service attacks (on an organisation's website).
- Email security.
- Sharing of employees' passwords.
- Sensitive information disclosed during social discussions.
- Internal theft of information.
- Network sniffing.
- Cyber-attacks.
- Exploitation of system usernames and default passwords.
- Confidential information exchanged between interoffice messengers and employees.
- Confidential information handled by interoffice messengers.
- Offsite data storage not encrypted and compromised.
- Inadequate firewall configuration.
- Identity theft (in its various forms: customer, supplier, employee, etc.).
- Information corrupted by former employees.
- Launch of unauthorised programs by users causing major problems to the main systems.
- Attempts to vandalise or sabotage the network.
- Sensitive information taken outside the organisation.
- Supplier support not available because of his failure.
- Dependence on a single individual's knowledge of ICT systems.
- The third party (dealer) that supports the systems can access confidential information.

10.2.5. Regulatory and legal risks

These risks are associated with an organisation's legal and regulatory environment, as well as the requirements that an NGO abides by applicable legislation. Risk usually arises from regulatory agencies changing the current rules (or imposing new rules) that negatively affect the NGO's current position.

A non-exhaustive list of areas to be considered could include:

- Compliance with legal requirements (related to the specific sector or service).
- Compliance with regulatory requirements (related to the specific sector or service).
- Health and safety compliance in the working area (firehoses, fire extinguishers, labels, etc.).
- Contractual risks (contracts with customers and suppliers).
- Negative court decisions in ongoing trials.
- Meeting state and tax requirements on time.
- Changes to regulations and laws.
- Violations of labour codes or other laws in the host country
- Violations of international sanctions or counter-terrorism restrictions
- Failing to comply with charitable registration laws

10.2.6. Human Resources Risks

This category covers risks related to an organisation's human resources, employment, health and safety issues, competencies etc. This includes members and volunteers.

A non-exhaustive list of areas to be considered could include:

- The availability of competent staff within the organisation and on the market.
- Current number of staff.
- Current competencies of staff.

- Health and safety issues.
- Workplace accidents.
- Travel safety.
- Maternity leave.
- Loss of key staff (illness, resignation etc.).
- Inadequate or unclear employment practices.
- Employee dishonesty.
- Planning for succession or substitution (who will replace any unavailable employees).
- Workplace accidents.
- Workplace violence.
- Lack of training for organisation ICT systems.
- Lack of safety training.
- Lack of training for organisation procedures and processes.
- Pandemic flu.
- Lack of adherence to safety practices.
- Resignation, termination, or retirement.
- Strikes or labour unrest.
- Poor morale or performance.

10.2.7. Governance and stakeholders risks

These are risks related to:

(a) The way in which an organisation is governed and managed.

(b) How relationships are managed with organisation's stakeholders (those with a direct or indirect interest in the NGO. Examples include donors, beneficiaries, grant providing organisations, trustees, members, employees, customers, suppliers,

governments, local communities, media, banks, and other investors or credit providers etc.).

A non-exhaustive list of areas to be considered could include:

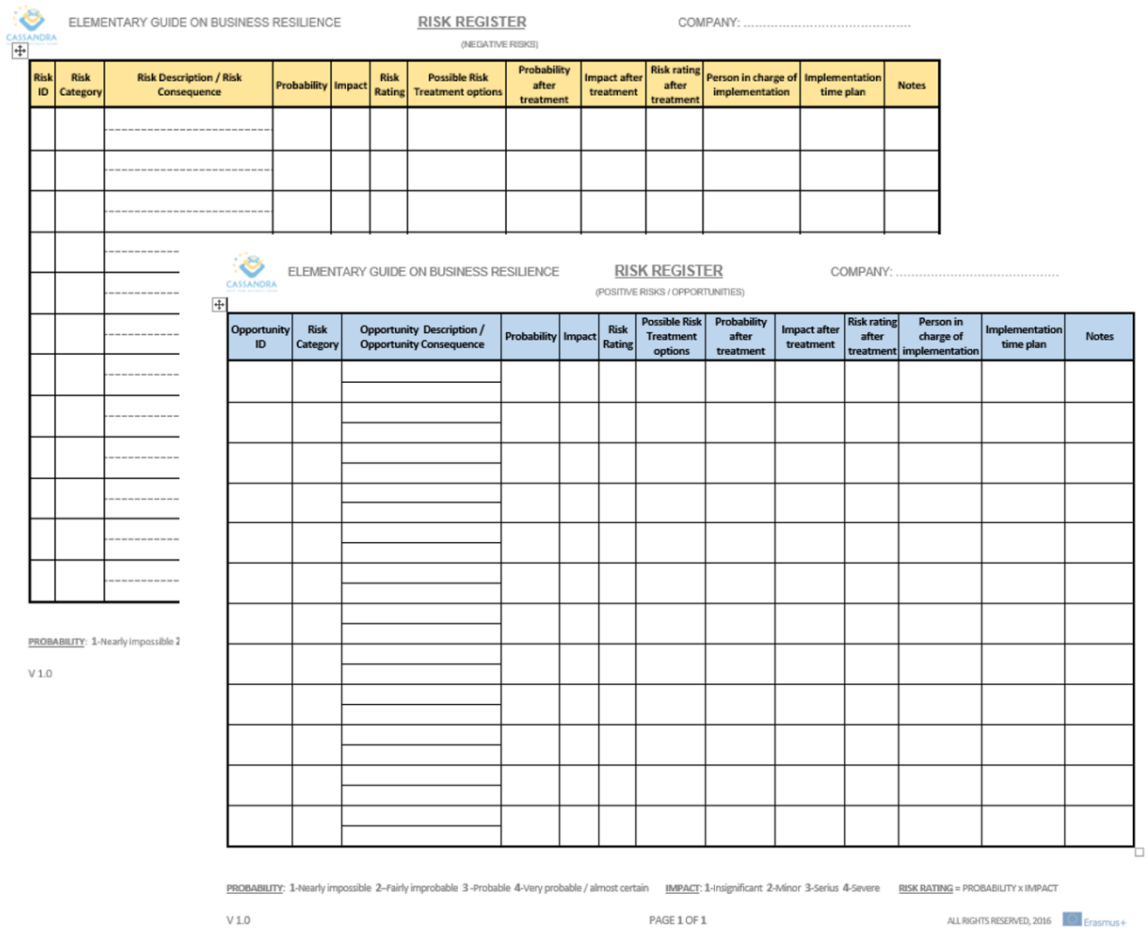
- Organisation structures and charts.
- Universally clear roles and responsibilities.
- Management skills.
- Management competencies.
- Authorisation processes (including access to ICT systems).
- Poor management or micromanagement.
- Office politics.
- Missing organisation values and principles.
- Evaluation and management of suppliers and dealers.
- Interests of employees.
- Management of communication with employees.
- Management of and communication with donors (communication with and dependence on key donors).
- Relationships with the local community (and neighbourhood).

10.3. Work systematically and methodologically

Successfully identifying risks requires you to work in a systematic way and follow the steps of the CASSANDRA methodology. These are explained in the paragraphs and chapters that follow.

10.3.1. A form to use: the risk register

Before anything else, you will need a form with which to document the risks that you identify. You may use the forms that are provided in the annexes section of this guide in spreadsheet format.



ELEMENTARY GUIDE ON BUSINESS RESILIENCE

RISK REGISTER

(NEGATIVE RISKS)

COMPANY: .....

Risk ID	Risk Category	Risk Description / Risk Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes

PROBABILITY: 1-Nearly impossible 2

V 1.0

ELEMENTARY GUIDE ON BUSINESS RESILIENCE

RISK REGISTER

(POSITIVE RISKS / OPPORTUNITIES)

COMPANY: .....

Opportunity ID	Risk Category	Opportunity Description / Opportunity Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3-Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-Minor 3-Serius 4-Severe RISK RATING = PROBABILITY x IMPACT

V 1.0 PAGE 1 OF 1 ALL RIGHTS RESERVED, 2016 Erasmus+

This is called a risk register and is used to document and follow-up potential risks to your organisation that you have identified. It includes the probability, impact, and rating (severity) of each risk, as well as the proposed and chosen actions to treat (minimise/mitigate) these risks.

For this part you will only need the first three columns of the template.

Column 1 (Risk No.) will just be a serial number.

Column 2 The category of risk (see previous paragraph).

Column 3 (Risk Description / Risk Consequence) is the most important column. This is where you will describe the risks that you have identified (in your own words), as well as noting down any other information related to the specific risk that you may consider necessary for it to be properly documented. You may also use the form to document the consequences, what will happen to the NGO and its members if this risk materialises.

You can use an electronic or paper form (print several copies of the template). Use as many pages as you need.

For your own convenience, we suggest that you use the electronic document, preferably in the excel format, since this will significantly assist you in the following steps.

Because there may be negative AND positive risks, there are **two** risk register forms, one for negative risks (coloured orange) and one for positive risks and opportunities (coloured light blue).

10.3.2. Ensure that you separate issues and problems from risks

Whilst identifying risks, it is sometimes easy to misinterpret issues and problems (in your business or day-to-day operations) and mistakenly consider them to be risks.

> An **ISSUE is a problem that has happened and is already a reality. This will already be having an impact** on your organisation's objectives and operations. What was meant to go wrong has already happened and now requires a solution to minimise the extent of any negative impact that has already affected the organisation.
>
> A **RISK** is **something that may happen in the future and may have an impact on** the organisation's objectives and operations. It may or may not happen. Unlike an existing issue or problem, you can plan for each risk and implement measures and solutions so that it will not happen!

In other words, issues are already here and must be dealt with. Risks can be avoided and might never happen. A risk can become an issue, but an issue is not a risk, because it has already happened.

To help you with your work, you may use the following phrases:

- **"There is a risk of …….. and if it occurs, the consequence will be ……."**
- **"Failure or loss of …….. will have/result in ……. as a consequence."**

e.g.

- There is a risk of a fire in the office if smoking is permitted. If it occurs, the consequence will be that everything in the office will be burned and lost.
- Failure of your IT server system will result in your operations coming to a complete stop as a consequence.

You do not have to write down the entire phrase. Just write the risk (and its consequence):

RISK	CONSEQUENCE
Fire in the office due to smoking	Loss of building and office, business being stopped
Failure of IT server (either due to disk or power failure)	Complete end of our operations

10.3.3. Work alone or with your staff

Although you may think that you can do it alone, we highly recommend that you involve your employees in this project. It is certain that each one of them is knowledgeable about a specific area of operations that could contribute significantly to your risk identification. Even more than this, the common sense of a team will help to minimise any exaggeration of identified risks.

You can decide if you want to work alone.

Involving your team requires the following steps:

STEP	DESCRIPTION	TICK BOX
1	Run a kick-off meeting with all your employees (if possible).	
2	Ensure that they have all used the quick check tool (see Step 1).	
3	Explain what risk management and resilience are in your own words. Tell them about the scope and objectives of this project and the expected outcome ("a more resilient NGO that will benefit everyone").	
4	Explain to them the difference between risks and issues or problems (see the relevant paragraph above) so that you minimise the loss of time and the contribution of inaccurate information.	
5	Briefly explain the various risk categories (see the relevant paragraph above). Explain to them that you will focus on working within each category separately.	
6	Explain to them about positive and negative risks.	
7	Show them (or hand out) the two risk register forms.	

10.3.4. Start identifying

Brainstorming, which can either be done alone or with a team, is perhaps the best way to systematically identify the risks your organisation faces.

Focus on each category of risk and examine the status of your operations. You could use questions like the ones below to help you identify areas at risk:

- What could go wrong?
- What can go better?
- How might we fail?
- Where are we vulnerable?
- Which assets do we need to protect?
- How might someone steal from the organisation?
- How might someone disrupt our operations?
- What might disrupt our operations?
- What happens if I cannot come to work tomorrow?
- What happens if employee X leaves the organisation?
- What happens if a service sells extremely well (far better than we considered when planning)?
- Which information and information systems do we rely on most?
- Which activities are most important? What could cause them to fail?

You could also focus on each of the organisation's activities and assess what could go wrong (or be improved).

You will also be able to identify risks through a physical inspection. Walk around your office area and neighbourhood checking for risks linked to your facilities (office area, environment, buildings around etc.).

For those that have done a SWOT[8] analysis for any of your services, activities, operations and objectives, then the "Threats" column is a great source for your list of risks.

[8] SWOT analysis is an acronym for Strengths, Weaknesses, Opportunities and Threats. It is a structured method that evaluates those four elements for a project or product or business venture. It involves (a) specifying an objective for the organisation or product or project and (b) identifying the internal and external factors that are favorable and unfavorable to achieve that objective. It is required to identify:

- Strengths: characteristics of the organisation or project or product that give it an advantage over others

Reviewing organisation documents may provide you with further information about exposures to risks. You could check documents such as:

- Contracts for facilities, outsourced services.
- Insurance coverage contracts.
- Contracts with customers for service delivery.
- Contracts with grant providing organisations
- Agreements with donors
- Contracts with key partners or suppliers.
- Policies and procedures documents (if applicable).

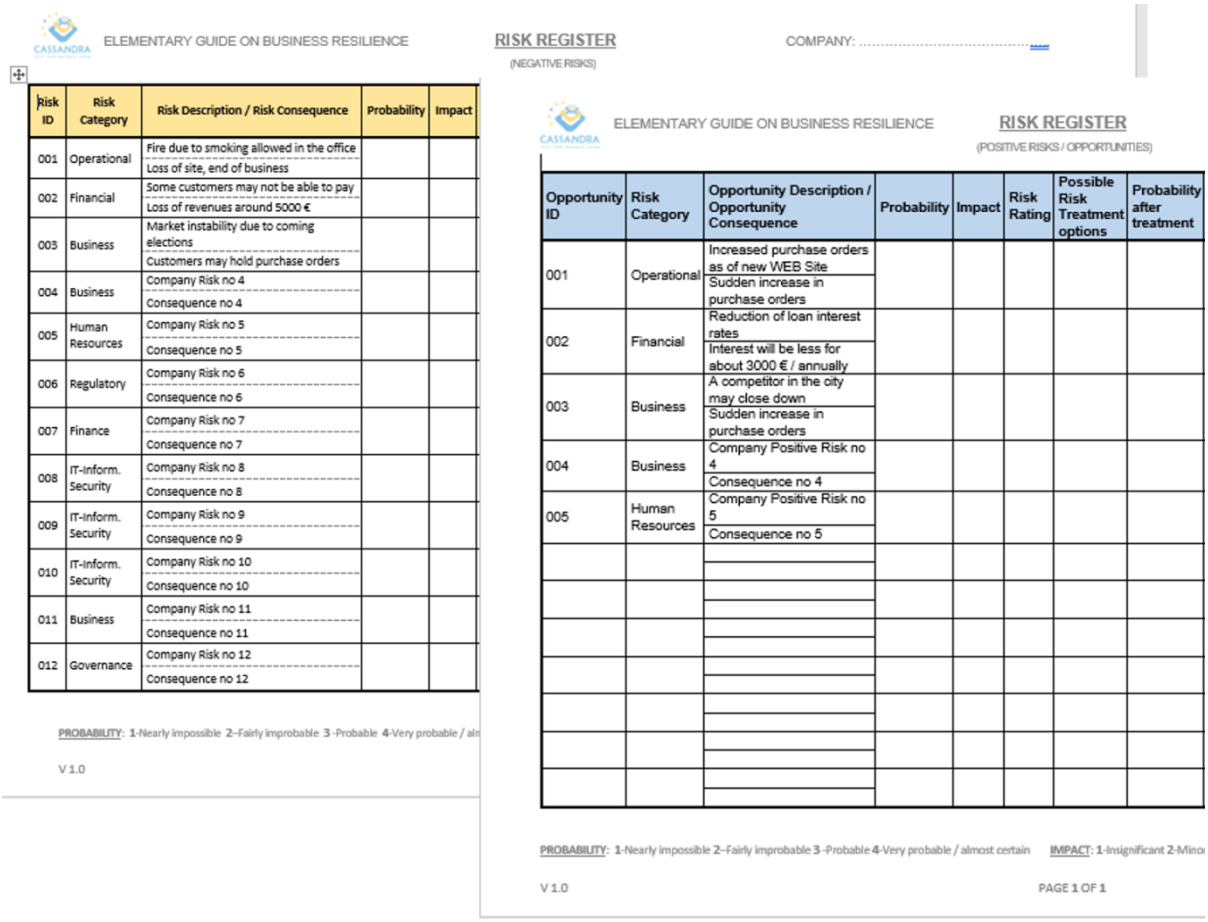
Use the RISK REGISTER forms provided to document the risks that you have identified (you only require the first three columns at this stage).

You may use the first three columns of the forms for your documentation needs. The sequence in which you record the risks in the REGISTER does not play any role.

Once you feel that you have finished, have a look at the list and make sure that you have documented risks and not issues or problems (as clarified above). By the end, your risk registers (for both positive and the negative risks) should look similar to the examples below.

- Weaknesses: characteristics of the organisation or project or product that place it at a disadvantage relative to others
- Opportunities: elements in the environment that the organisation or project or product could exploit to its advantage
- Threats: elements in the environment that could cause trouble for the organisation or project or product

For more information about SWOT Analysis you can visit https://en.wikipedia.org/wiki/SWOT_analysis or other sources online.



ELEMENTARY GUIDE ON BUSINESS RESILIENCE

RISK REGISTER

(NEGATIVE RISKS)

COMPANY: .....

Risk ID	Risk Category	Risk Description / Risk Consequence	Probability	Impact
001	Operational	Fire due to smoking allowed in the office Loss of site, end of business		
002	Financial	Some customers may not be able to pay Loss of revenues around 5000 €		
003	Business	Market instability due to coming elections Customers may hold purchase orders		
004	Business	Company Risk no 4 Consequence no 4		
005	Human Resources	Company Risk no 5 Consequence no 5		
006	Regulatory	Company Risk no 6 Consequence no 6		
007	Finance	Company Risk no 7 Consequence no 7		
008	IT-Inform. Security	Company Risk no 8 Consequence no 8		
009	IT-Inform. Security	Company Risk no 9 Consequence no 9		
010	IT-Inform. Security	Company Risk no 10 Consequence no 10		
011	Business	Company Risk no 11 Consequence no 11		
012	Governance	Company Risk no 12 Consequence no 12		

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3-Probable 4-Very probable / alr

V 1.0

ELEMENTARY GUIDE ON BUSINESS RESILIENCE

RISK REGISTER

(POSITIVE RISKS / OPPORTUNITIES)

Opportunity ID	Risk Category	Opportunity Description / Opportunity Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment
001	Operational	Increased purchase orders as of new WEB Site Sudden increase in purchase orders					
002	Financial	Reduction of loan interest rates Interest will be less for about 3000 € / annually					
003	Business	A competitor in the city may close down Sudden increase in purchase orders					
004	Business	Company Positive Risk no 4 Consequence no 4					
005	Human Resources	Company Positive Risk no 5 Consequence no 5					

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3-Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-Mino

V 1.0

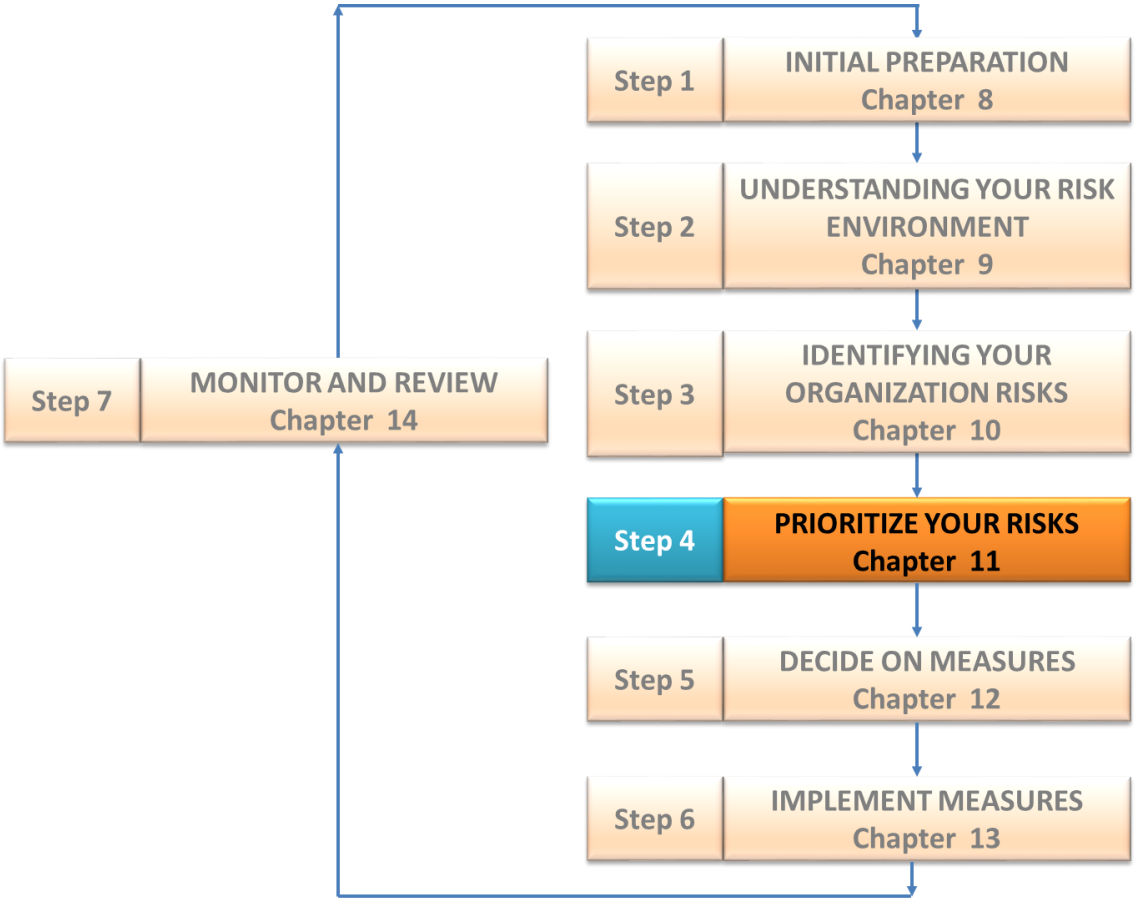
PAGE 1 OF 1

10.3.4.1. Tip for identifying ICT and information security risks

When using the generic approach discussed above for risk identification, do not forget to additionally consider or make use of the following steps to help you identify risks connected with ICT and information security.

- Use your list of ICT infrastructure that you prepared as discussed in chapter **10.2.4 Information & Communication Technology (ICT) and Information Security Risks**.
- Identify risks by applying the filters outlined in the “IT infrastructure and operations related risks” and “Risks related to information security” paragraphs of chapter 10 for each asset.
- Use the provided list of possible risks, threats and vulnerabilities to help you.
- Analyse which risks could lead to compromising confidentiality, integrity, or availability of your information assets.

11. Step 4 – Prioritise your risks



Once you have completed the previous step, you should have a risk register document in place that contains a good number of risks. These risks usually fill several pages of the document. If you now look at them through the eyes of a manager, you will get a (good) overview of this basic list of risks which are simply documented without being distinguished in accordance with the organisation's concerns and requirements.

Nothing in the list shows the NGO's management:

- What is important and what is not.
- What requires your attention and what could perhaps be bypassed.
- What is urgent and what can wait.

Unless these questions are answered, you will not be able to really decide how to respond to these risks. Should you just work on the first 10 or on those that you think

are most important? What if the organisation does not have enough money to deal with all of the risks on the list?

When you apply some common sense, it seems important to find out a way to prioritise your risks so that you can start treating those that are most significant without losing time, money and resources to those of only minor importance.

This prioritisation requires you to calculate and evaluate two factors for each risk: its **probability** (likelihood) and **impact** (consequences).

11.1. Probability (likelihood)

The probability of a risk is directly related to the likelihood of that risk occurring.

If we follow the typical mathematical approach when talking about the probability of a negative or positive event occurring, we can typically express this as a statistical figure in relation to time (the probability of a specific risk occurring within 1 year, within 5 years, within 20 years and within 100 years).

Here are some real-life examples:

- The probability of an earthquake of 5.5 R or greater is 1 every 20 years in Athens, Greece.
- On the Danube River in Passau, Germany, the expected value for the number of floods occurring in any 100-year period is 1 (in light of historical data from 1501 to 2013).
- Based on a large field sample of drives, Google's 2007 study found that the actual annualised failure rates (estimated probability that a device or component will fail during a full year of use) for individual drives ranged from 1.7% for first year drives to over 8.6% for three-year-old drives.

As illustrated above, it seems as if there are two problems with this approach:

(a) In order to be able to calculate probability, access to statistical and historical information and mathematics is required. This is something that a very large company (such as big insurance firms) may be able to do, but it is doubtful that an average person (such as an NGO member, manager, or employee) will be able to do this, given the time, skills and possibilities available to them.

(b) Although the probability of a Passau flood is 1 every 100 years:

1. This does not exclude two, three or more floods occurring within the next 100 years.
2. This does not mean that the next flood will occur in the year 2115, should a flood have occurred last year.

Your objective is to prioritise your risks, rather than to create a scientific report. You will not have access to statistical data that ensures 100% accuracy for your calculations, and you will not be able to make the complex calculations required for a probability. For the purposes of your work it is sufficient in virtually all cases to use your common sense and understanding of the organisation's environment in conjunction with the simple approach presented below.

For a typical risk prioritisation it is sufficient to **define and use a scale of probability** with a scale of 3, 4, 5, or more steps. You could use either numbers or descriptions to label the various steps of the scales. This is presented in the following table:

4-STEP SCALE EXAMPLE

SCALE		PROBABILITY OF OCCURRENCE
1	Unlikely	Less than 7% Has never happened or may happen once every 15-20 years
2	Moderate	Between 8% and 40% Expected to happen once every 6-15 years
3	Likely	Between 41% and 80% Expected to happen once every 1-5 years
4	Almost Certain	Greater than 80% Expected to happen more than once every year

Alternatively

- On a 3-Steps scale you could use
  - 1 - Low
  - 2 - Medium
  - 3 - High
- On a 5-Steps scale you could use
  - 1 - Nearly Impossible
  - 2 - Fairly Improbable
  - 3 - Probable
  - 4 - Very Probable
  - 5 - Practically Certain

For the purposes of this guide we will use the 1-4 scale (4-steps scale).

11.2. Impact (consequences)

Impact refers to the estimated consequences that a risk may have on an organisation, if and when it occurs.

The consequences on an organisation may vary not only in relation to their extent (e.g. high or low), but also in relation to the operational area (or areas) affected:

- **Financial** (resulting in financial loss or unbudgeted expenses and property value):
    - Loss of revenue
    - Loss of funding
    - Loss of grants
    - Loss of profit.
    - Penalties and fines.
    - Unbudgeted expenses.
    - Loss of bank credit.
    - …
- **Operational** (resulting in part or all of the organisation's operations coming to a stop):
    - Inability to operate and deliver some or any services.
    - Poor performance.
    - Services delivered of a poor quality.
    - Ignoring the wishes of donors
    - Unrealistic expectations
    - …
- **Health and safety related** (impacting the health and safety of employees, neighbours, customers, visitors etc.):
    - Injury of employees or volunteers.

- Poor safety conditions in the working area.
- Poor welfare for employees and volunteers.
- …

- **Reputational** (affecting brand image and the organisation's reputation):
  - Negative media publicity.
  - Large numbers of customer complaints.
  - Loss of a beneficiary's trust in the NGO's services.
  - Negative public statements or litigation by staff, ex-staff or stakeholders
  - …
- **Legal / Regulatory** (resulting in an inability to conform with regulatory requirements or legal actions):
  - Legal actions against the NGO or management.
  - Loss of regulator permits or licenses.
  - Severe penalties.
  - Failing to comply with charitable registration laws
  - …
- **Human Resources** (resulting in employee-related consequences):
  - Staff resignations.
  - Low employee morale.
  - Staff missing or unavailable.
  - Poor or no volunteer effort
  - …

The impact of a risk occurring could be confined to only one area (e.g. only financial impact), or it could be a combination of several or even all areas simultaneously.

Just as with prioritisation, it is also necessary here to **define and use a scale of impact** with a scale of 3, 4, 5, or more steps. You could use either numbers or

descriptions to label the various steps of the scales. This is presented in the **sample scale** below:

NEGATIVE RISKS IMPACT SCALE		
SCALE		**IMPACT (CONSEQUENCES)**
1	Insignificant	Health and safety: none. Financial: loss of < €500. Operational: operations interrupted for less than 1 day. Reputational: no impact. Regulatory / Legal: no impact.
2	Minor	Health and safety: first aid treatment. Financial: loss of between €500 and €2,500. Operational: operations interrupted for 1-2 days. Reputational: a few unsatisfied customers / donors. Regulatory / Legal: minor non-compliance with regulatory requirements.
3	Major	Health and safety: medical treatment required. Financial: loss of between €2,500 and €10,000. Operational: operations interrupted for 3-5 days. Reputational: several unsatisfied customers / donors. Limited news coverage. Regulatory / Legal: significant noncompliance with key regulatory requirements. Legal action taken against the organisation.
4	Severe	Health and safety: Death or extensive injuries. Financial: loss of more than €10,000. Operational: operations interrupted for more than 5 days. Reputational: many unsatisfied customers / donors. Publicised in local media. Regulatory / Legal: Long-term or permanent non-compliance with key regulatory requirements. Loss of permit and multiple legal actions against the organisation.

The following table could be used for the positive risks impact scale:

POSITIVE RISKS (OPPORTUNITIES) IMPACT SCALE		
SCALE		**IMPACT (CONSEQUENCES)**
1	Insignificant	Health and safety: no impact. Financial: unexpected donations (or savings) of < €1,000. Operational: no impact. Reputational: no impact. Regulatory / Legal: no impact.
2	Minor	Health and safety: no impact. Financial: unexpected donations (or savings) of between €1,000 and €10,000. Operational: required operations improved by 5% (to support extra sales). Reputational: positive statements from a couple of customers / donors. Regulatory / Legal: no impact.
3	Major	Health and safety: no impact. Financial: unexpected donations (or savings) of between €10,000 and €30,000. Operational: required operations improved by 20% (to support extra sales). Reputational: positive statements from some customers / donors. Limited news coverage in a few blogs, resulting in new donors and some phone calls. Regulatory / Legal: new engagement contracts require legal assistance.

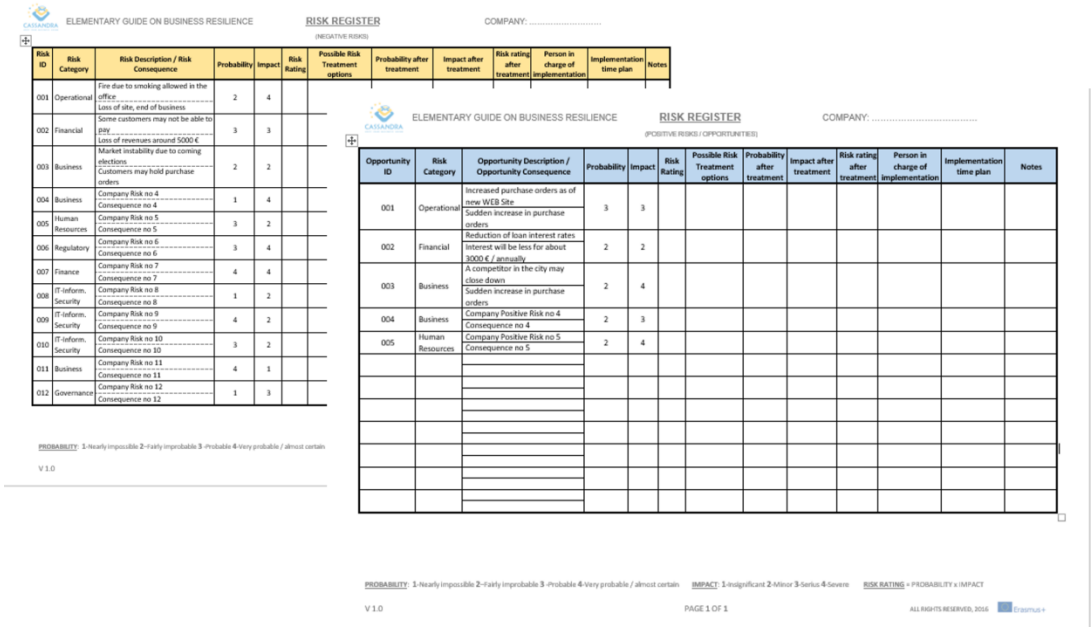
POSITIVE RISKS (OPPORTUNITIES) IMPACT SCALE		
SCALE		**IMPACT (CONSEQUENCES)**
4	Severe	Health and safety: no impact. Financial: unexpected donations (or savings) of more than €30,000. Operational: required operations improved by 70% (to support extra sales). Reputational: Positive statements from several customers / donors. Extensive spread of news in media, resulting in new donors and a large number of phone calls. Regulatory / Legal: new engagement contracts require extensive legal support.

For the purposes of this guide we will use the 4 steps impact scale and the table given above.

11.3. Risk rating

In the light of the previous section, go back to your risk register and document the probability and impact of each of the risks you have identified.

Your register of positive and negative risks should now look something like this:



ELEMENTARY GUIDE ON BUSINESS RESILIENCE RISK REGISTER COMPANY: .....

(NEGATIVE RISKS)

Risk ID	Risk Category	Risk Description / Risk Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes
001	Operational	Fire due to smoking allowed in the office Loss of site, end of business	2	4								
002	Financial	Some customers may not be able to pay Loss of revenues around 5000 €	3	3								
003	Business	Market instability due to coming elections Customers may hold purchase orders	2	2								
004	Business	Company Risk no 4 Consequence no 4	1	4								
005	Human Resources	Company Risk no 5 Consequence no 5	3	2								
006	Regulatory	Company Risk no 6 Consequence no 6	3	4								
007	Finance	Company Risk no 7 Consequence no 7	4	4								
008	IT-inform. Security	Company Risk no 8 Consequence no 8	1	2								
009	IT-inform. Security	Company Risk no 9 Consequence no 9	4	2								
010	IT-inform. Security	Company Risk no 10 Consequence no 10	3	2								
011	Business	Company Risk no 11 Consequence no 11	4	1								
012	Governance	Company Risk no 12 Consequence no 12	1	3								

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3-Probable 4-Very probable / almost certain

V 1.0

ELEMENTARY GUIDE ON BUSINESS RESILIENCE RISK REGISTER COMPANY: .....

(POSITIVE RISKS / OPPORTUNITIES)

Opportunity ID	Risk Category	Opportunity Description / Opportunity Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes
001	Operational	Increased purchase orders as of new WEB Site Sudden increase in purchase orders	3	3								
002	Financial	Reduction of loan interest rates Interest will be less for about 3000 € / annually	2	2								
003	Business	A competitor in the city may close down Sudden increase in purchase orders	2	4								
004	Business	Company Positive Risk no 4 Consequence no 4	2	3								
005	Human Resources	Company Positive Risk no 5 Consequence no 5	2	4								

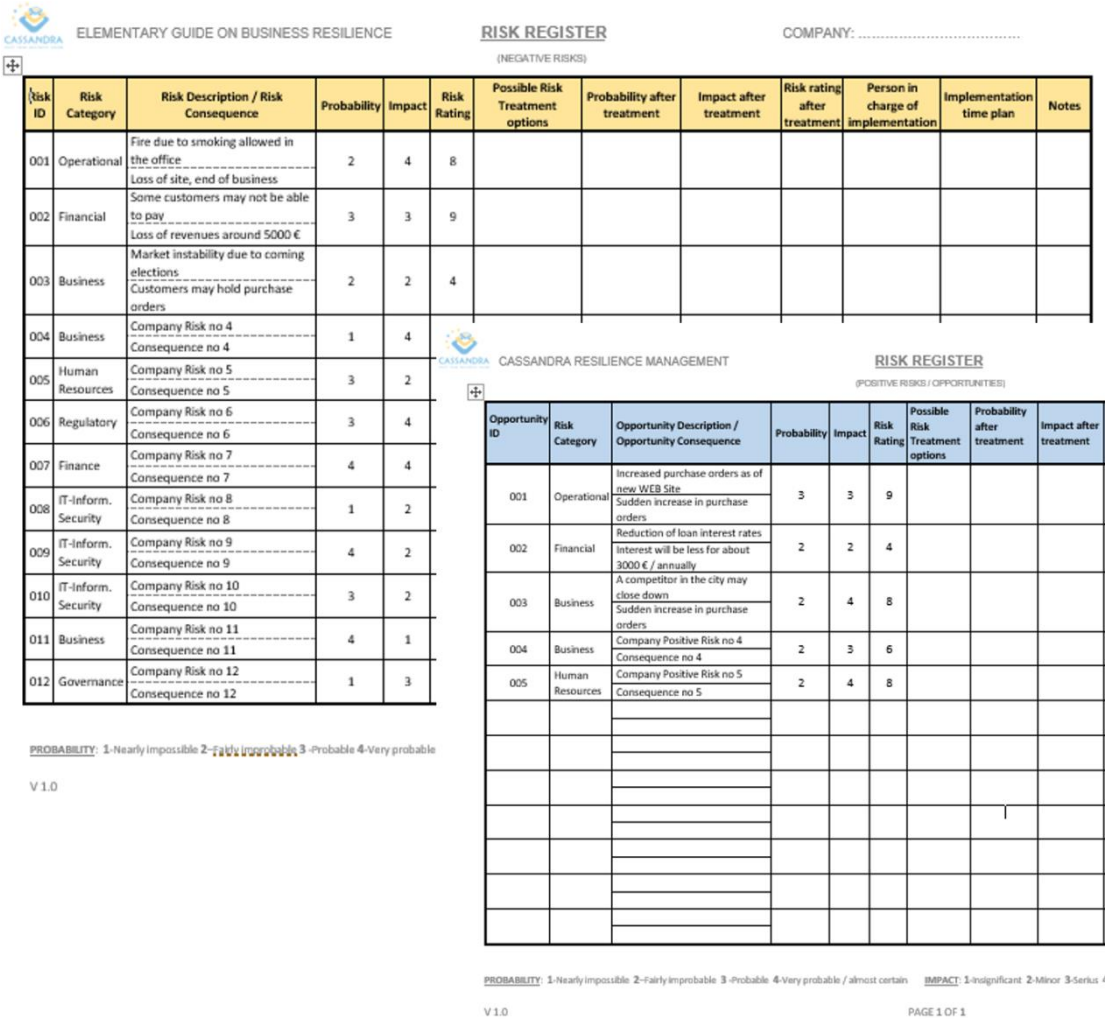
PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3-Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-Minor 3-Serius 4-Severe RISK RATING = PROBABILITY x IMPACT

V 1.0 PAGE 1 OF 1 ALL RIGHTS RESERVED, 2016

You can quantify a risk by producing a figure that encapsulates the "size" of the risk in relation to the size of its probability AND impact values. This is done by multiplying together the probability and impact scores:

Risk Rating = **Probability** (likelihood) x **Impact** (consequences).

For the next step, go back and document the results of this multiplication in your risk register. The final result should look similar to the table below:



ELEMENTARY GUIDE ON BUSINESS RESILIENCE

RISK REGISTER

(NEGATIVE RISKS)

COMPANY: .....

Risk ID	Risk Category	Risk Description / Risk Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes
001	Operational	Fire due to smoking allowed in the office Loss of site, end of business	2	4	8							
002	Financial	Some customers may not be able to pay Loss of revenues around 5000 €	3	3	9							
003	Business	Market instability due to coming elections Customers may hold purchase orders	2	2	4							
004	Business	Company Risk no 4 Consequence no 4	1	4								
005	Human Resources	Company Risk no 5 Consequence no 5	3	2								
006	Regulatory	Company Risk no 6 Consequence no 6	3	4								
007	Finance	Company Risk no 7 Consequence no 7	4	4								
008	IT-Inform. Security	Company Risk no 8 Consequence no 8	1	2								
009	IT-Inform. Security	Company Risk no 9 Consequence no 9	4	2								
010	IT-Inform. Security	Company Risk no 10 Consequence no 10	3	2								
011	Business	Company Risk no 11 Consequence no 11	4	1								
012	Governance	Company Risk no 12 Consequence no 12	1	3								

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3 -Probable 4-Very probable

V 1.0

CASSANDRA RESILIENCE MANAGEMENT

RISK REGISTER

(POSITIVE RISKS / OPPORTUNITIES)

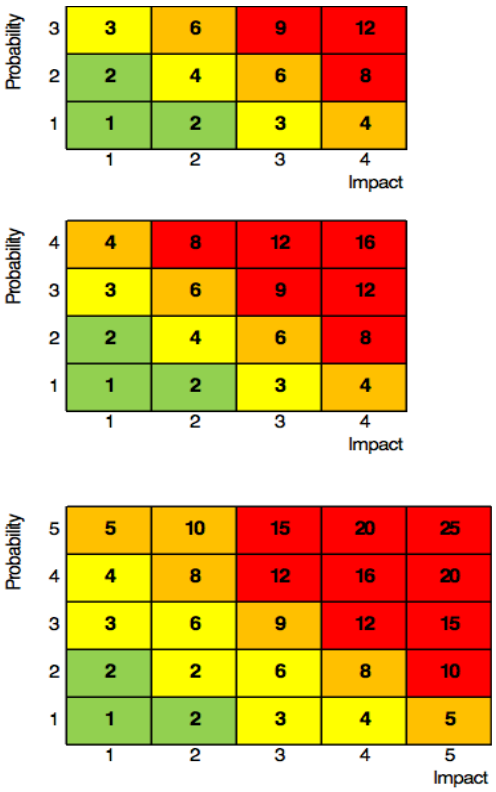
Opportunity ID	Risk Category	Opportunity Description / Opportunity Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment
001	Operational	Increased purchase orders as of new WEB Site Sudden increase in purchase orders	3	3	9			
002	Financial	Reduction of loan interest rates Interest will be less for about 3000 € / annually	2	2	4			
003	Business	A competitor in the city may close down Sudden increase in purchase orders	2	4	8			
004	Business	Company Positive Risk no 4 Consequence no 4	2	3	6			
005	Human Resources	Company Positive Risk no 5 Consequence no 5	2	4	8			

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3 -Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-Minor 3-Serius

V 1.0

PAGE 1 OF 1

11.4. Risk matrix



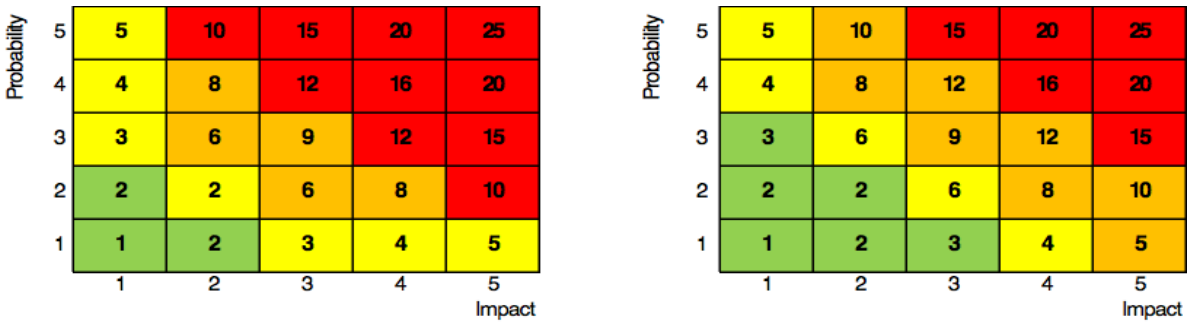
A risk matrix is a grid-style "**traffic light system**" that you can use to help visualise the ratings of your risks. Traffic light colours are used to distinguish between the severities of the risks and help you utilise your risks prioritisation better. The scale starts with **green** (for the least severe risks) and finishes with **red** (for the most severe risks).

- **Red** = Significant risks that must be dealt with (High)
- **Orange =** Less significant risks that you should deal with (Tolerable)
- **Yellow** = Medium risks that you might deal with (Low)
- **Green** = Minor risks that you will not spend resources on treating, as long as they retain the same rating (Very low).

The grid is a combination of the probability and impact scales. Its size depends on the scales you have used for probability and impact. In the examples shown we have (a) a risk matrix based on probability 3 – impact 4 scale (b) a risk matrix based on probability 4 – impact 4 scale and (c) a risk matrix based on probability 5 – impact 5 scale.

Looking at the matrix, we understand that the most important risks are those that have **both a high probability AND a high impact. These are in the top right corner of the matrix.**

However, risks with just a high probability rating (top row) or high impact rating (right column) are also important and require your attention.



Depending on your own appetite or tolerance (your "risk appetite") you might:

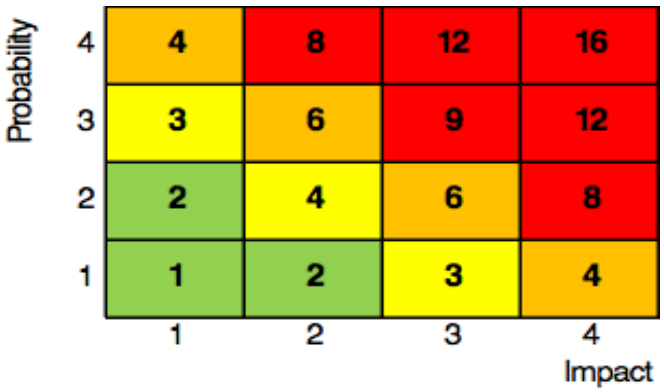
a) Be more aggressive and choose to consider a wider range than just the red area, or

b) Be more conservative and decide that it is enough to deal with only the risks rated between 15 and 25, as well as minor risks with a rating of 3 or less.

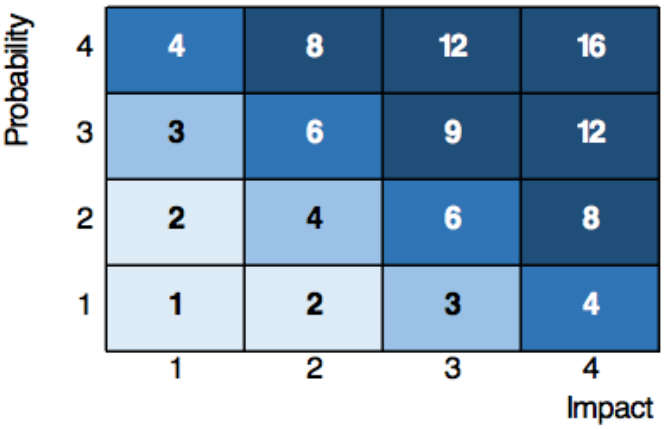
We can see these two examples in the picture above.

11.5. Risk prioritisation

For the purposes of this guide we will use the 4 x 4 risk matrix, since this matches the probability and impact scales in the previous chapters:

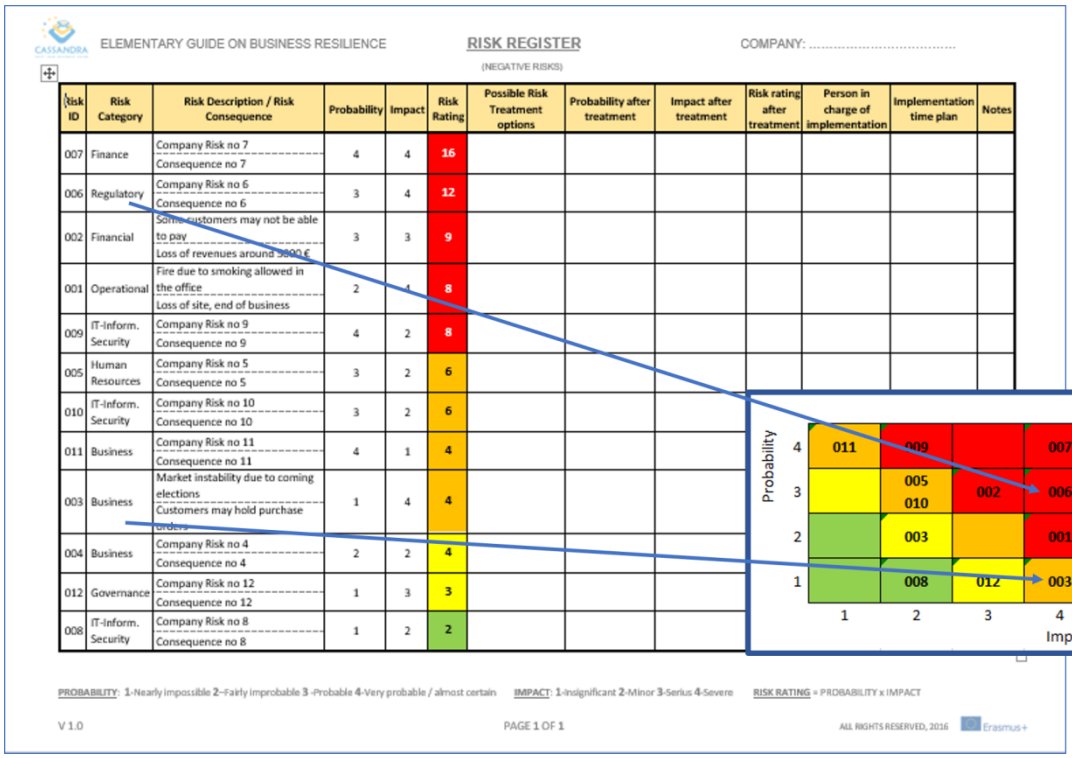


We will also use a rather aggressive approach to characterising the areas of significant risk, namely those risks rated 8 and above. The green ones are those rated 1 or 2.



The same approach is applied to the positive risk matrix table.

Going back to your risk register, apply this traffic light system to the risk rating column. This will help you with your overall picture of risk prioritisation. If you sort the register list by the risk rating column[9], then your picture will be like the one below, making it easy to respond to questions like "Which (negative or positive) risks should I deal with first?"



ELEMENTARY GUIDE ON BUSINESS RESILIENCE

RISK REGISTER

(NEGATIVE RISKS)

COMPANY: .....

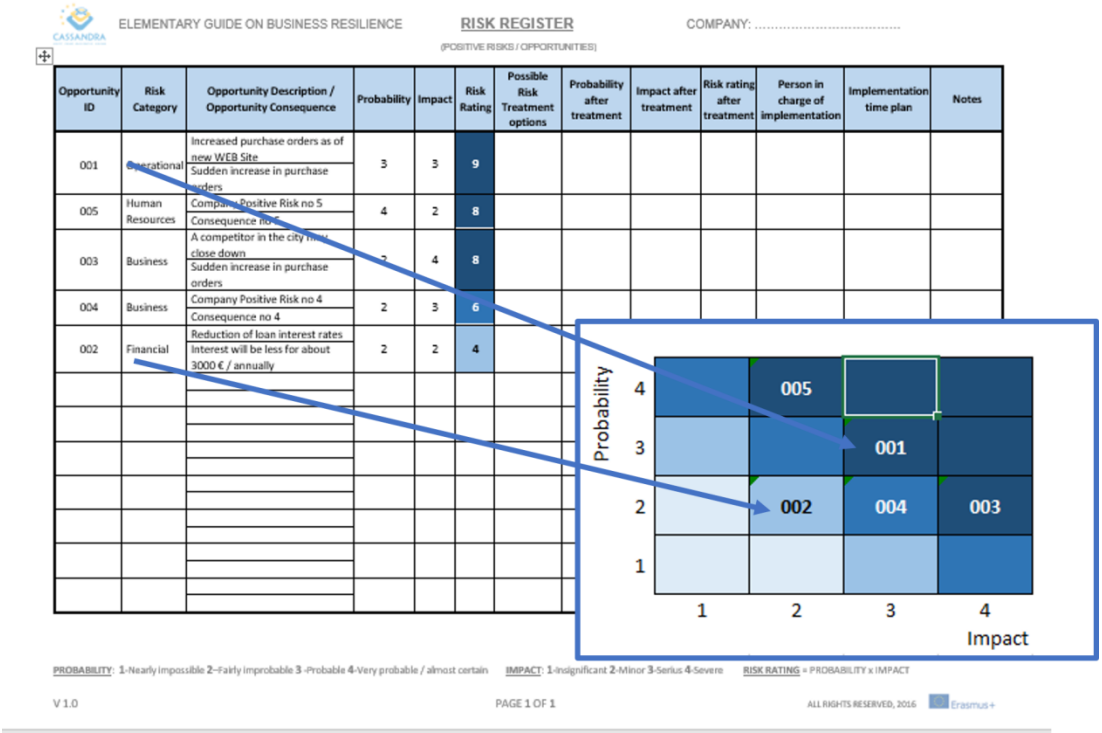
Risk ID	Risk Category	Risk Description / Risk Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes
007	Finance	Company Risk no 7 Consequence no 7	4	4	16							
006	Regulatory	Company Risk no 6 Consequence no 6	3	4	12							
002	Financial	Some customers may not be able to pay Loss of revenues around 5800 €	3	3	9							
001	Operational	Fire due to smoking allowed in the office Loss of site, end of business	2	4	8							
009	IT-Inform. Security	Company Risk no 9 Consequence no 9	4	2	8							
005	Human Resources	Company Risk no 5 Consequence no 5	3	2	6							
010	IT-Inform. Security	Company Risk no 10 Consequence no 10	3	2	6							
011	Business	Company Risk no 11 Consequence no 11	4	1	4							
003	Business	Market instability due to coming elections Customers may hold purchase orders	1	4	4							
004	Business	Company Risk no 4 Consequence no 4	2	2	4							
012	Governance	Company Risk no 12 Consequence no 12	1	3	3							
008	IT-Inform. Security	Company Risk no 8 Consequence no 8	1	2	2							

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3-Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-Minor 3-Serius 4-Severe RISK RATING = PROBABILITY x IMPACT

V 1.0 PAGE 1 OF 1 ALL RIGHTS RESERVED, 2016 Erasmus+

For the positive risks, the risk matrix and risk register will be similar to the ones below.

[9] This is where using the Excel template greatly helps. The sorting only takes a few seconds.



ELEMENTARY GUIDE ON BUSINESS RESILIENCE **RISK REGISTER** COMPANY: .....

(POSITIVE RISKS / OPPORTUNITIES)

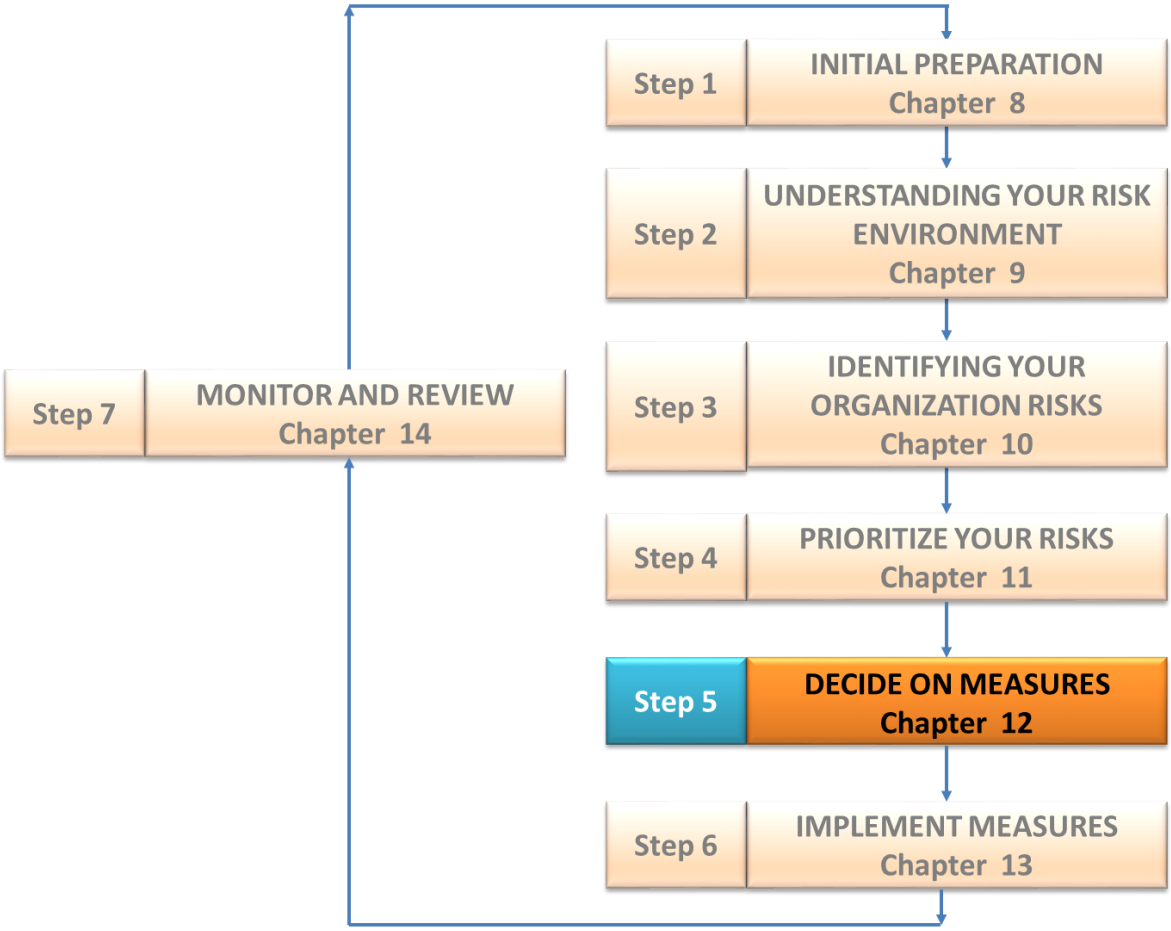
Opportunity ID	Risk Category	Opportunity Description / Opportunity Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes
001	Operational	Increased purchase orders as of new WEB Site Sudden increase in purchase orders	3	3	9							
005	Human Resources	Company Positive Risk no 5 Consequence no 5	4	2	8							
003	Business	A competitor in the city near close down Sudden increase in purchase orders	2	4	8							
004	Business	Company Positive Risk no 4 Consequence no 4	2	3	6							
002	Financial	Reduction of loan interest rates Interest will be less for about 3000 € / annually	2	2	4							

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3 -Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-Minor 3-Serius 4-Severe RISK RATING = PROBABILITY x IMPACT

V 1.0 PAGE 1 OF 1 ALL RIGHTS RESERVED, 2016 Erasmus+

As can be seen, the risk matrix view provides you with a better picture of the risks that have been identified and their prioritisation.

12. Step 5 – Decide on measures



It is important to keep in mind throughout this project that your ultimate goal is to minimise your organisation's risks and its exposure to threats, so that you can continue to protect its ability to operate and accomplish its objectives, thereby maintaining growth and profitability.

Up to now, you have completed two very important steps to this end:

(a) Identifying the risk your NGO faces.

(b) Prioritising these risks, by sorting them on the basis of how critical they are and how much of a priority they are to deal with.

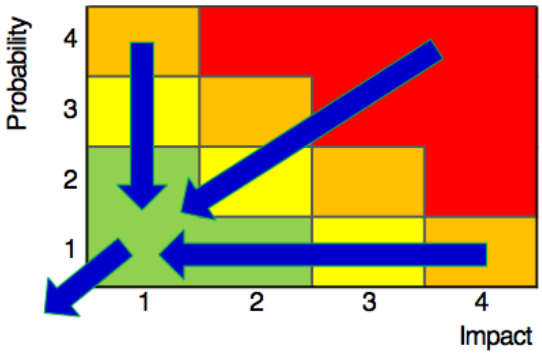
This step is all about identifying and deciding to employ specific measures and treatments to minimise your organisation's overall exposure to the risks you have identified.

12.1. The treatment theory

Our **basic risk treatment approach** is simple:

> **"Improve the position of each specific risk in the matrix either towards the green area to an acceptable point, or remove it completely out of the matrix (and out of the organisation's life)".**

This means that you will work on each specific risk and, as a result of your efforts, you will lower its risk rating, thus moving it



- from the red area to orange/yellow/green areas or
- from the orange to yellow/green areas or
- from the yellow to green area or
- completely out of the risk register of the organisation

12.1.1. What is the acceptable point for a risk (or when is a risk acceptable)?

Acceptance of a risk **is a decision that you usually make** under one of the following conditions:

(a) The overall rating of the risk is already low enough because of the low probability (likelihood) of it occurring and the minor impact (consequences) that the risk would have on the NGO if it occurred.

(b) The overall effort and cost of reducing or minimising the risk is greater than the impact it would have if it occurred.

(c) For a variety of reasons it is not possible to implement any measure or to do anything to improve the risk's current rating.

Risks of that type are usually, although not always, in the green area of the risk matrix. That is actually the best case scenario. You may usually accept a risk if it

cannot be avoided, reduced or transferred, regardless of which risk matrix area it is in.

In such a case, **you should decide to declare the risk as <u>ACCEPTABLE</u>**. Be sure to keep it in the risk register and continue to monitor it.

12.1.2. What should you do with the acceptable risks?

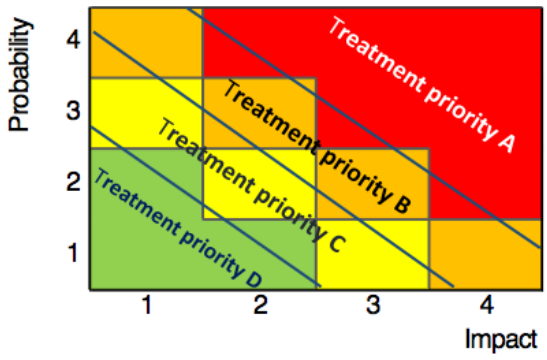
For a risk that has been deemed acceptable you will either do nothing about the risk or just prepare a simple plan in advance about what to do when or if the risk occurs. Once the risk has occurred, you can fix the problem (with or without the plan) and move on.

12.1.3. What should you do with the rest of the risks (unacceptable risks)?

Any risks that have not been deemed acceptable (the vast majority of risks) are usually those with a high probability or a high impact, in other words those with a medium to high risk rating. These are usually the risks that are in the red, orange and yellow areas of the matrix and the ones that you are not able or willing to tolerate, because they would expose your organisation to significant (negative) consequences.

Deal with these risks by implementing one or more of the risk treatment strategies outlined in the following chapter.

It is important to remember to work on each specific risk individually, **"one by one". Each risk is unique** because of its nature, source, probability and impact(s). This means that the measures and treatment that can be used to minimise it are similarly unique.



Each risk must therefore be treated separately. There is no magic recipe for automatically recognising the specific measures, treatments or controls required. You will have to work with one risk at a time.

Using the results of the previous steps, begin methodically with the priority A risks, then move on to B, C and, finally, D.

12.2. The different risk treatment strategies

In order to implement the **basic risk treatment approach** outlined above, you could choose the specific treatments and actions for each risk separately by using one, several, or all of **the following strategies**:

(a) AVOID THE RISK

- **Avoid the risk** (remove it completely from your organisation) by deciding not to start or continue the activity that has given rise to this specific risk:

  E.g. You could eliminate the risk of "expanding your services to a new country but poor funding may result in significant financial consequences" by not providing this service at all.

Risk avoidance is sometimes adopted when an activity or situation involves a high level of risk which could not be adequately treated by another approach. The risk might be too high in comparison with the potential benefits for the organisation that the activity or situation might bring. It may also be that the costs of a risk mitigation solution are not affordable or do not match the expected benefits.

A decision is made to either not become involved in a risky activity or situation, or to withdraw from it completely.

(b) MITIGATE / REDUCE THE RISK

- **Removing the source of the risk**:

  E.g. Replacing a faulty cable that causes random interruptions to the internet connection with a new cable. The source of the risk has been removed, meaning that there is now no such risk ("internet connection interrupted by a defective cable").

  In such a case, the organisation invests effort and money completely removing the source of the risk. Removal is different to reduction. In the case of risk reduction, the risk remains in the risk register, but its rating is lower

than it was before. In the case of risk removal, the risk is no longer an issue for the NGO (at least from that particular source).

- **Changing (reducing) the probability of a risk**:

  E.g. (1) By not permitting smoking on premises, you minimise the probability of a fire caused by smoking.

  (2) Relocating from a mountain or forest area to a city also reduces this risk.

  You can usually minimise the probability of a risk occurring by deploying measures to the monitor AND control of the source of the risk. For example, you could minimise the risk of a poor quality report being sent to donors by implementing a quality control system to check all deliverables before they are sent out to donors. This element of control will minimise the possibility of a low-quality report being sent out.

- **Changing (reducing) the impact of a risk:**

  E.g. (1) By preparing a contingency (continuity) plan for the risk that an earthquake completely damages your premises, you will minimise the impact that an earthquake would have on your operations. This is because you can use your plan to keep your operations up and running, although your primary office site may be destroyed. You can also reduce the impact by buying an insurance contract to cover any expenses incurred by such an event (see below for more on transferring risks).

  (2) By installing an automatic system for extinguishing fires, you minimise the impact of a fire breaking out.

  Mitigating or reducing the impact of a risk may not only require the implementation of specific measures and controls but can, in several cases, also require you to (a) **transfer the risk** (see below) and (b) the prepare **contingency and business continuity plans**. These are alternative solutions for ensuring the continuity of organisation operations and activities and systems. Although they do not change the risk, these plans will be able to mitigate its impacts **once it has occurred**. See also the information on contingencies and continuity plans below.

- **Changing (reducing) both the probability and the impact:**

  E.g. You select and implement two measures at the same time: (a) you ban smoking in the office and (b) you install an automatic system for extinguishing fires. This reduces both factors.

  This is a combination of the two strategies described above.

(c) <u>TRANSFER THE RISK</u>

- **Sharing (transferring) the risk to another party or parties:**

  E.g. You can minimise the risk of completely and irreplaceably losing your assets and premises to a fire by sharing the risk with an insurance firm.

Transferring the risk is, to an extent, an example of a risk mitigation strategy (see (b) above). Transferring risks usually takes the form of:

(a) Insurance coverage for high impact risks. This means that you get back the monetary amount equal to the value of the destroyed or lost premises, goods, equipment, profits, health etc. This includes legal liability risks.

(b) Subcontracting or outsourcing a project, activity, or service (usually one which is secondary to organisation objectives or to the capabilities of members and volunteers) to a third party that you believe can deliver better than you or that have better business capacities in areas where you lack the expertise, ability, or finances to operate (e.g. outsourcing your accounting services instead of employing an accountant or doing it on your own).

The following **<u>two things are very important</u>** to bear in mind with all risk transfer cases:

(a) Outsourcing an activity or service, although it may minimise a risk, can also create other risks that you will have to keep fully under control throughout the relevant outsourcing contract agreements with these third parties (e.g. the risk that an insurance company fails to pay or that the contracted company suddenly becomes bankrupt).

(b) Although you may have transferred the risk, your organisation is still responsible to your stakeholders (customers, donors, members, public authorities etc.).

(d) ACCEPT THE RISK

- **Retaining (accepting) the risk** as the result of an informed decision (i.e. a conscious decision, not simply because a risk has been forgotten or ignored or was never identified).

  Accepting the risk (see also above). We have consciously repeated this strategy in this list, because particularly for small NGOs in the short-term or long-term there may be no other viable approach to take for certain risks. Amongst other reasons, this might be due to a lack of necessary temporal and financial resources. An informed and conscious decision about the (hopefully) only temporary acceptance of risks is, however, still better than completely forgetting about risks, ignoring them, or not even identifying them.

(e) UTILISING OR INCREASING THE RISK (ONLY FOR POSITIVE RISKS AND OPPORTUNITIES)

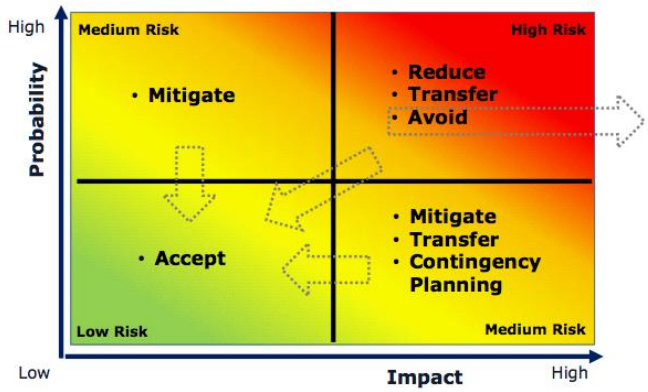
- **Utilising or increasing the risk** in order to pursue an opportunity:

  E.g. It is likely that a service to be delivered to a beneficiary will probably require less time than initially planned. If this does happen, you will save costs and increase your effectiveness. In such a case, you will focus on increasing the likelihood of an early delivery, thereby increasing your positive risk.

This strategy **is only for positive risks**: increasing a risk can be done by increasing its probability or its impact. This means implementing the relevant measures to ensure that the risk WILL occur and that the organisation will benefit from the specific opportunity it creates.

12.2.1. Approaches to treatment based on risk ratings

Because the treatment of each risk is decided separately, it is important for those working on it to be aware of the specific aspects to be considered during their decision-making process.



It is interesting to note that although some risks can have the same ratings (e.g. a high impact risk A with probability 2 and impact 4, and an almost certain to occur risk B with probability 4 and impact 2, result in the same risk rating), they should be treated with very different strategies.

Depending on the values of a risk's probability and impact, it can be categorised into one of four major categories, as shown in the diagram above. As will be discussed, each category is linked to specific strategies for treatment that are usually applicable. This does not mean, however, that any strategies that are not mentioned cannot be used. Below are some of the most common strategies:

(a) Risks with **high probability** and **high impact** (top right corner in the diagram above).

These risks are at a completely unacceptable level. Their high probability means that they are very likely or almost certain to occur. When they occur, the impact they have on the organisation will be high. Because these pose the greatest risk exposure to your NGO, the only option is to reduce the risk to an acceptable level. The following strategies can be used for these risks:

(1) Reduce the risk by implementing appropriate measures to shrink its probability or impact.

(2) Transfer the risk by:

- Subcontracting or outsourcing the specific activities that cause the risk to external agents or companies. This transfer will bring the overall risk rating to a more acceptable level.
- Using insurance to mitigate losses.

(3) Avoid the risk by discontinuing specific activities or operations, thereby eliminating the risk exposure of your organisation.

(b) Risks with **high probability** and **low impact** (top left corner in the diagram above).

These are risks that seem to be occur with high frequency (we can say that this is generally the case) and are having an impact on your organisation. Because their impact is low or insignificant, the problem for the organisation seems to be minor. This is inaccurate, however, because the frequency with which they occur means that the cumulative impact on the organisation could be quite high.

These risks are usually connected to secondary problems in processes, procedures, equipment or activities. Based on their high frequency, we can safely conclude that specific improvements and efforts at mitigation could fully resolve the issues and eliminate or minimise the risks to an acceptable level. Typical examples include problems related to devices that often malfunction (this could be fixed with a good service or by replacing the device). It could also be a problem arising out of an organisation's poor quality assurance for its procedures.

The typical strategy for these risks is:

(1) To mitigate the risks by deploying appropriate measures that mainly focus on reducing their probability.

(c) Risks with **low probability** and **high impact** (bottom right corner in the diagram above).

These risks rarely occur, but their impact on your organisation is very significant when they occur. Typical examples include natural disasters (flooding, earthquakes etc.), fires, or the loss of all ICT systems and infrastructure.

Their high impact (e.g. stopping NGO operations, causing significant financial loss, destroying facilities, rendering staff unavailable etc.) mean that these risks are unacceptable and should therefore be treated.

Typical strategies include:

(1) Mitigating the risks by deploying appropriate measures that mainly focus on reducing the impact if these risks were to occur.

(2) Transferring the risk by utilising:

a. Insurance coverage to mitigate losses.

b. Subcontracting or outsourcing the specific activities that cause the risk to external agents or companies. This transfer will bring the overall risk rating to a more acceptable level.

c. Contingency planning to ensure that alternatives are in place and that the impact on the organisation can be managed once the risk occurs (more information in the paragraph below).

(d) Risks with **low probability** and **low impact** (bottom left corner in the diagram above).

These are risks that can be accepted, and in most cases, require no effort or resources to be further minimised. It is unlikely that they were to occur and, even if they do, their impact will be low.

The typical strategy for these risks is:

(1) To accept the risk (it is still necessary to monitor its status).

12.2.2. ICT and information security measures

In order to identify measures and treatments that will help minimise information technology and information security risks you need to:

- Work on two layers:

  (1) Strategic or managerial layer.

  (2) Technological layer.

- For each layer, work through the following two filters:

  (1) Select the most appropriate measures that are available to minimise exposure to the risk. Make sure that you understand risk exposure ("Which data and

information will have its confidentiality or integrity violated? How will this violation take place?").

(2) Think about your alternatives (even though you have implemented risk treatment measures) if the risk were to occur (examples include backups, disaster recovery, and similar plans).

12.2.2.1. Strategic and managerial layer

Working in this layer is about measures and treatments related to:

1. Identifying the best ICT strategies for your organisation's technology and communication systems (regardless of which kind).

   ICT strategies are related to the strategic choices that you make for your technology systems. The following questions should help to give you some ideas:

   - Should we buy an ERP solution or outsource it?
   - Should we store our data in the cloud or buy our own servers?
   - Do we need a new employee skilled with ICT or employ an external dealer?
   - Which dealer will we select to provide and support our systems? Is it ok to use an individual, should we choose a company?
   - Should we use a Microsoft, UNIX or Apple operating system?

   You must be very careful when identifying and evaluating the various options and selecting your IT solutions.

   For example:

   - **Buying a local server or hosting your applications in the cloud.** The cloud will minimise the risk of equipment failure (e.g. your server failing), but the cloud also requires constant internet access (if you want to constantly access your data). This exposes you to communication risks (e.g. your connection being hacked).
   - **Storing all data files (e.g. Word, Excel and related files) on a central file server or allowing users to store them on their own PC's**. Both options have advantages and risks: if your server is hacked then all data will be

exposed at once, but, on the other hand, backing up ALL your data is simpler and safer with a central server than with several separate PC's.

- **Hosting an application for your organisation's accounting on your own systems or completely outsourcing the work to an accounting company to store your data on their IT systems.** If you host it on your own server, you should be aware of potential technical problems with the server, application software, or system and data backup. Your data will, however, be under your supervision and in the security of your office. If you use the services of an external company, your data will be stored in a system elsewhere that you have no control over and, in most cases, you will know nothing about the external company's security standards and how well prepared that are (what happens if they are hacked?).

Given that these are, in most cases, complex issues that require not only the intelligence of a manager, but also a good knowledge and understanding of technology, we advise using an external ICT consultant to help explain to you the various approaches and solutions. Do not forget, however, that the decision will ultimately be your own and not the consultant's. It is therefore very important that you completely understand in advance the pros and cons of each strategic option. After all, strategic selections cannot be changed easily (or at least at low cost), meaning that you will usually have to live with them for a long time.

2. Choosing and managing relationships with ICT dealers (your "ICT business partners")

When choosing your ICT dealers, there are several things that you must understand and bear in mind (other than the very important criterion of how competent they are with ICT systems and applications) in order to minimise your exposure to risk. Here are some important issues:

ID	RISK CONTROL CRITERIA	TICK BOX
1	Ensure that they can be trusted (so that you can trust them when accessing your ICT infrastructure and data).	
2	Ensure that you have signed a contract with them that describes in detail the services they will provide to your organisation and the level of service they offer (e.g. their response time if a device fails), as well as their commitments in relation to confidentiality and data protection regarding your organisation's information that they will access during their work.	
3	Ensure that you are fully aware and in control of the 'privileges' that you have given your IT dealer (and their employees) as regards your organisation and its ICT systems (e.g. office keys, access passwords for some or all systems, remote access etc.). Do not forget to 'withdraw' these 'privileges' at the end of your collaboration.	
4	Ensure (and keep checking) that they respect the contractual laws you have agreed to. Use contractual penalties.	

3. Identifying and setting up appropriate organisation rules and policies in relation to the operation and management of your ICT systems and information assets.

   There is a lot of work for your management to do in this area, in terms of quality and not quantity. Below are a list of chosen measures related to ICT systems and information security that might help you with specific risks. We advise that you discuss and work through (each of) these with your ICT advisor (whether a dealer or business partner):

- **Assign responsibility for your organisation's security to someone** (this could be you, a manager, a trustee or a reliable employee). They should make sure that all security decisions are implemented and kept to on a continuous basis.

  They should be the person responsible for keeping relevant documentation updated, available and secure (e.g. the list of access rights to ICT systems and privileges of all users, employees, and 3rd parties).

- **Classify the information and documentation**. Some might be open to all, but other sections are only for a limited audience. Enforce classification (by requiring the work "CONFIDENTIAL" to be written on all (electronic or paper) confidential documents). Store them in lockers and drawers which you control access to.

- **Prepare an access control policy**. Use a document (remember that this is a CONFIDENTIAL document) to note:
  - Who has copies of keys and open-close access to your premises.
  - Who has access to each system and at what level (e.g. access only to the area where files are stored or, as a system administration, access to everything in there).
  - Who has access to email. List the different emails that exist.
  - Who has access to internet.
  - Who has keys to lockers with confidential documents.

- **Prepare an asset control procedure**.
  - Have a list of all your ICT assets (ALL of them, not the main ones, including USBs).
  - Make sure that for every asset (documented in written form) there is a person in charge (owner). E.g. every employee is the owner of his own PC/laptop; he is responsible that it does not get lost or stolen.
  - Site door keys are an asset. Copies of these keys should be controlled.

- **Prepare an employee termination procedure** (what steps will be taken if an employee leaves the organisation: take back the assets that have been given to him, remove access to systems, inactivate his email etc.).
- **Have a signed contract with each employee** that dictates their access to NGO information and data and explains that they must follow all of the organisation's security rules and guidelines. Ask your legal advisor for assistance.
- **Prepare a password policy**. There should not even be one system in your organisation that does not require a password to be accessed. Ensure that password lengths are appropriate and that your employees use complex passwords (e.g. password that simultaneously include letters, numbers, capitals and different characters). Make clear when everybody should change their password for each system. Do not allow employees to exchange passwords.
- **Document your organisation's procedures and processes**.
- **Prepare a backup plan** (see the relevant chapter).
- **Consider (buying) a support contract from equipment and software dealers** to ensure on time and cost-controlled fixing of problems or system failures (or replacement equipment).
- Prepare a business continuity and disaster recovery plan (to deal with a loss of equipment or total disaster).
- Prepare an incident response plan so that you can deal with events and incidents (including security breaches).
- Make sure that there is an organisation communications plan in place (who will you address and what will you say if customer data is leaked?).
- Ensure that you run a risk and vulnerability assessment least once a year for your ICT systems and infrastructure.
- …

4. Training and raising the awareness of your employees about information security and your organisation's ICT systems and operations.

   This is probably the most important treatment. By keeping your employees informed, you minimise the organisation's exposure to threats and, at the same time, limit the occurrence of negative incidents.

   Prepare discussions and small training sessions within the organisation using your ICT dealer or a security expert as a coach. These sessions should contain all of the following topics:

   - The importance of information security.
   - Specific issues such as:
     - Email use
     - Websites and access to them
     - Spam, phishing and scamming
     - Use of social media and the protection of organisation information
     - Signs that your organisation's systems may have been hacked
     - A security incident management process – how to respond in case of a security incident?
     - Organisation processes and policies (e.g. access control)
     - Asset protection
     - Encryption
     - …

You are not trying to make them field experts but 'good users' of the NGO's information and information systems. Training should be held for all new employees, and discussions with employees repeated at regular intervals. Discussions should cover measures and solutions that have already been implemented, and should result in employees being fully aware of the strategies in place.

It is of great importance to let your employees and members know that security is a very significant issue that is taken seriously by your organisation, and that any

possible violations and breaches may result in not only failure, but in disciplinary and legal actions against your organisation or against them as individuals.

12.2.2.2. Technological layer

This has to do with the choice of technical solutions and set-ups to reduce risk and minimise the possibility of all kinds of negative incidents. Here is an example list to help you:

- Install an alarm system to monitor any violation of access to your premises or physical intrusion. Install a camera monitoring and video recording system.
- Use antivirus or antimalware software for your ICT systems. Make sure (and double check) that this is frequently (almost daily) updated with new virus information and shields.
- Install a firewall (a system to monitors and control incoming and outgoing network traffic based on security rules) to filter your communications.
- Keep software up-to-date. Ensure that patches[10] are frequently distributed to all systems. Demand that your IT dealers update your systems with new patches as a standard.
- Install generators, UPS[11] and power filters to minimise the impacts of public power network failures on the performance of your ICT systems.
- Implement encryption system(s) to protect all data stored, wherever it is stored (file servers, laptops, USBs, external hard disks that you use to copy and transfer files). Pay particular attention to who has encryption keys and keep a copy of them in a safe place (think about what would happen if the keys were lost or forgotten).
- Decide whether you will use a Wi-Fi system or not. Wi-Fi systems can be practical and easy to access, but they are far more vulnerable to hacking. If you

[10] Patches are software updates that usually resolve issues of previous versions of application or system software, as well as eliminate vulnerabilities and risk exposures.
[11] UPS = Uninterruptible Power Supply. See chapter: 16 Selective Glossary and Abbreviations.

do install one, ensure that there is always a Wi-Fi access key and that it is frequently changed. Control visitor access to your organisation's Wi-Fi network.

- Use software solutions and tools to monitor your system and network (very useful if you run a 24x7 web e-commerce site).
- Filter the internet access of your employees. Do not allow access to gambling, adult sites, games or similar high-risk sites.
- Use a computer room to host your ICT main systems that is equipped with an air conditioning system.

For all the above, you will definitely need to work with your ICT support dealer to help you find the best and safest implementation.

12.2.3. Business continuity (contingency) planning

Organisations create continuity (contingency) plans and implement alternative solutions when the impact of a disruption is high, cannot be reduced or is not tolerable. This concept of business continuity applies to impacts that are related (but not limited) to services, activities, infrastructures, premises, operations, staff, dealers, business partners, customers, donors, grant providers, markets, brand image and reputation.

Preparing a plan and a solution requires you to consider what alternatives there might be to balance out negative impacts in the event of a disruptive or destructive event (i.e. the destruction of equipment and premises or non-tangible disasters, such as the loss of a major donor). You will need to prepare to make that alternative available once the negative incident has occurred and within the timeframe that the organisation needs. Continuity plans and alternatives may cover any or all of the following risks:

- **Emergency response and evacuation plan** (to minimise the impact of a risk such as fire or site damage on human resources and people in the building).

- **Loss of premises and working area** (including provision for alternative working areas such as home offices).
- **Failure or loss of ICT systems** (either complete failure or loss of the systems or data or both).
- **Loss of files and archives** (whether on paper or electronic).
- **Communications failure** (including data lines and vocal communication such as your telephone centre and organisation phone line).
- **End of a provision of service to beneficiaries** (for various reasons, including disaster on the premises, malfunctioning ICT systems, staff problems etc.).
- **Loss, damage, or malfunction of production equipment**.
- **Unavailability of staff** (e.g. due to pandemic flue or an accident).
- **Lack of volunteers due to negative publicity**
- **Sudden bankruptcy or pause in business** (due to a disaster) **with a critical dealer** (who provides specific services or products) **or a partner** (with whom critical activity has been subcontracted or outsourced).
- **Loss of an important sponsor / donor** that provides more than 40% of funds.
- …

In chapter **13.3 Plans' preparation and implementation of solutions**, you will work on preparing these plans for your organisation.

12.2.4. As one risk goes, another risk comes

Most of the times, taking action to minimise or eliminate a risk will expose your organisation to another new risk.

E.g.

(1) To avoid the risk of a new operation or service failing, you might cancel the deployment of the new service or operation. This could expose you to another risk, such as your organisation losing its innovation and credibility and allowing another competitor to seize the opportunity and introduce new services, thereby gaining more of the market for his NGO and reducing your position in the field.

(2) Buying and equipping fire extinguishers in your organisation will minimise the impact of a fire if it breaks out, but it exposes the organisation to new risks such as (a) fire extinguisher material harming or killing employees and (b) the fire extinguishers not being properly maintained and therefore proving useless when needed.

You must therefore be very careful to ensure that every measure taken and risk treatment implemented does not expose your organisation to new risks that are left unattended and could result in negative impacts, perhaps even more severe than the risks that you first treated.

12.2.5. More than one treatment can apply

For each risk in your risk register, you might be able to identify more than one treatment or solution that could be implemented, either separately or in tandem with each other.

You could get good advice by discussing each case with the relevant experts (e.g. your ICT risks with your ICT consultant or solutions provider), or with your colleagues. The internet is also a good source of information.

On the other hand, although brainstorming is a good way of coming up with options, you should only consider and add to your list options that really help to mitigate risks and give maximum benefit to the NGO. Evaluate each idea to make sure that:

(a) It is feasible, applicable and appropriate for the size and context of your organisation.

(b) It will definitely mitigate the risk once implemented until it becomes acceptable for your organisation.

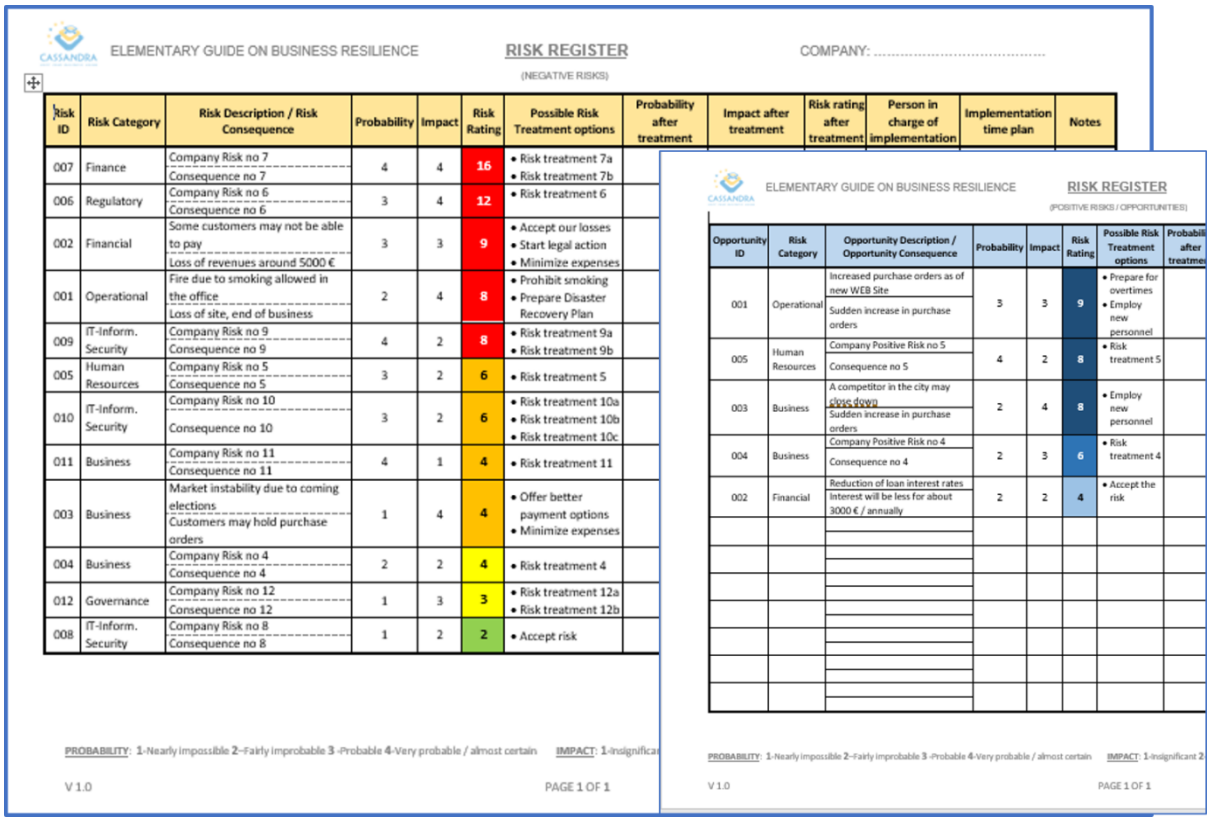
(c) It will not create another risk that is even greater for your organisation.

(d) The cost of implementing the idea is not greater than the cost of the risk's impact (with the exception of risks related to health and safety, since the value of human

life and health cannot be compared with monetary cost in the same ways as other issues can be).

12.2.6. Documenting your options

Document all the treatments that you have identified for each risk in your risk register under the column '**possible risk treatment options**'.



ELEMENTARY GUIDE ON BUSINESS RESILIENCE — RISK REGISTER — COMPANY: .....

(NEGATIVE RISKS)

Risk ID	Risk Category	Risk Description / Risk Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes
007	Finance	Company Risk no 7 Consequence no 7	4	4	16	• Risk treatment 7a • Risk treatment 7b						
006	Regulatory	Company Risk no 6 Consequence no 6	3	4	12	• Risk treatment 6						
002	Financial	Some customers may not be able to pay Loss of revenues around 5000 €	3	3	9	• Accept our losses • Start legal action • Minimize expenses						
001	Operational	Fire due to smoking allowed in the office Loss of site, end of business	2	4	8	• Prohibit smoking • Prepare Disaster Recovery Plan						
009	IT-Inform. Security	Company Risk no 9 Consequence no 9	4	2	8	• Risk treatment 9a • Risk treatment 9b						
005	Human Resources	Company Risk no 5 Consequence no 5	3	2	6	• Risk treatment 5						
010	IT-Inform. Security	Company Risk no 10 Consequence no 10	3	2	6	• Risk treatment 10a • Risk treatment 10b • Risk treatment 10c						
011	Business	Company Risk no 11 Consequence no 11	4	1	4	• Risk treatment 11						
003	Business	Market instability due to coming elections Customers may hold purchase orders	1	4	4	• Offer better payment options • Minimize expenses						
004	Business	Company Risk no 4 Consequence no 4	2	2	4	• Risk treatment 4						
012	Governance	Company Risk no 12 Consequence no 12	1	3	3	• Risk treatment 12a • Risk treatment 12b						
008	IT-Inform. Security	Company Risk no 8 Consequence no 8	1	2	2	• Accept risk						

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3-Probable 4-Very probable / almost certain IMPACT: 1-Insignifica

V 1.0 PAGE 1 OF 1

ELEMENTARY GUIDE ON BUSINESS RESILIENCE — RISK REGISTER

(POSITIVE RISKS / OPPORTUNITIES)

Opportunity ID	Risk Category	Opportunity Description / Opportunity Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probabili after treatme
001	Operational	Increased purchase orders as of new WEB Site Sudden increase in purchase orders	3	3	9	• Prepare for overtimes • Employ new personnel	
005	Human Resources	Company Positive Risk no 5 Consequence no 5	4	2	8	• Risk treatment 5	
003	Business	A competitor in the city may close down Sudden increase in purchase orders	2	4	8	• Employ new personnel	
004	Business	Company Positive Risk no 4 Consequence no 4	2	3	6	• Risk treatment 4	
002	Financial	Reduction of loan interest rates Interest will be less for about 3000 € / annually	2	2	4	• Accept the risk	

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3-Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-

V 1.0 PAGE 1 OF 1

12.2.7. Examples of possible mitigation strategies

A list of possible mitigation measures that you could use for specific risks is provided at the end of this document in the annex **18.2 Examples of possible mitigation strategies and measures**.

It should be pointed out that the examples given are indicative and non-exhaustive. They may not apply to all NGOs and in all instances.

12.3. Evaluating treatments and the decision-making process

Once you have collected all the various options for treating each of the risks on your list, you should proceed to the final decision, namely which of the various treatments available (for each specific risk) you will implement.

A '**cost-benefit** or a **pros-cons analysis**'[12] can typically be used for methodologies and processes with which to compare the costs and the benefits of various options and to identify or choose possible options for treating risks. This information could include the cost of measuring risks; the time, effort, complexity and risk of implementation; the pros and cons of each alternative etc.

One of the strongest criteria for your selection decision process is establishing which measure or treatment (for a risk) will result, when implemented, in the smallest possible acceptable risk rating.

Example:

For a specific risk with a rating of 12 (i.e. probability 4 x impact 3), there are two treatment options, A and B.

- If action A is taken, then the new risk rate will be 2 (i.e. probability 2 x impact 1). This is an acceptable risk rating (see the relevant chapter above on risk acceptance).
- If measure B is implemented, then the new risk rate will be 4 (i.e. probability 2 x impact 2). This is not acceptable.

Out of the two options, including considerations of cost, you would choose measure A because it provides a lower final risk rating.

Do not forget that 'accepting' a risk is a valid treatment option. You may decide to accept certain risks and do nothing about them (primarily those located in the green area, but also some located in the yellow or even orange areas) based on an

[12] The following phrase describes one simple approach to a cost-benefit/pros-cons analysis: create a table with three columns. The rows of the first column indicate the various options or alternative solutions, actions or approaches to be compared. In the second column document the various costs, difficulties, and disadvantages related to the buying, implementation and operation of each of the alternatives given in the first column. In column 3, document the various benefits, advantages and risk ratings for each of the alternatives given in the first column. Once you have finished, use the data documented in this table to inform your decisions about the best alternatives.

'informed' decision, namely a decision that involves a consideration of all factors. You can read more about this in the relevant risk acceptance chapter above.

When you have finished this, you will have finally filled your risk register with all the treatment(s) that you have chosen for each risk and each of the risks they contain.

12.4. Financing risk treatments

No organisation has an unlimited budget or limitless resources at its disposal. A typical NGO usually has several limitations on how much it can invest in activities that appear secondary to its operations. Resources of all kinds (finance, staffing, systems, time etc.) are scarce and their reallocation (or the search for additional finance) requires a lot of energy, difficult decisions and especially commitment.

The first attempt at risk management in any organisation usually results in a long risk register at the start with a significant number of risks to be treated, all of which would require some of the organisation's allocated resources. As a result, treating risk requires a second look at prioritisation in light of budget constraints.

Although the organisation's management (owners) ultimately make the decisions and are responsible for defining priorities on the basis of their judgement and overall organisation's scope and objectives understanding, there are some points that may help your decision-making process:

A. Understand and accept that your organisation's risks treatment will require a time-consuming programme. Even if you had all of the resources available, you would still require a lot of time to implement all of the treatments that you have chosen.

B. Examine your available budget before commencing planning. Use this in conjunction with your budget for effective treatment.

C. Use the list of risk treatments to outline the budget requirements of each treatment before implementing it.

D. Refer to the results of the prioritisation that you have already carried out by using your prioritised risk register: red risks need to be treated more urgently than orange or yellow ones.

E. Use urgency as a criterion: some risks cannot wait and may have specific timelines. Bear in mind that urgent risks are always those related to health and safety.

F. Start with 'quick wins': there will usually be several risks that require minimal effort and resources (budget) to be treated. These will result in positive effects (both for your organisation and for your own morale).

G. Consider other projects that your organisation is financing but that you could postpone. Compare their importance to that of treating a significant risk (e.g. buying new office equipment might be less important than preparing a contingency solution for your servers and ICT systems).

12.5. Update your risk register

In your risk register, document which treatments you have chosen, along with the risk ratings that remain once treatment has been implemented and the parameters of the implementation project.

(a) Insert your risk treatment options into the column "**Possible Risk Treatment Options**". Clearly mark the option chosen by you.

(b) Calculate the lower, adjusted "**Risk rating after treatment**" (new probability and new potential impact after the implementation of the chosen treatment option).

(c) For each implementation measure, document the person responsible for its implementation (in the column "**Person in charge of implementation**").

(d) Set an "**Implementation time plan**" for the chosen measures.

ELEMENTARY GUIDE ON BUSINESS RESILIENCE

RISK REGISTER

(NEGATIVE RISKS)

COMPANY: .....

Risk ID	Risk Category	Risk Description / Risk Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes
007	Finance	Company Risk no 7 Consequence no 7	4	4	16	• Risk treatment 7a • Risk treatment 7b	1	2	2	Stamatis T.	Start 1/5/2016 End 15/5/2016	
006	Regulatory	Company Risk no 6 Consequence no 6	3	4	12	• Risk treatment 6	1	1	1	Thanassis S.	Start 7/2016 End 30/10/2016	
002	Financial	Some customers may not be able to pay Loss of revenues around 5000 €	3	3	9	• Accept our losses • Start legal action • Minimize expenses	2	2	4	Panayiotis P.	Start 1/8/2016 End 10/8/2016	
001	Operational	Fire due to smoking allowed in the office Loss of site, end of business	2	4	8	• Prohibit smoking • Prepare Disaster Recovery Plan	1	4	4	Alexandros S.	Start 10/7/2016 End 15/9/2016	
009	IT-Inform. Security	Company Risk no 9 Consequence no 9	4	2	8	• Risk treatment 9a • Risk treatment 9b	1	3	3	Sandra K.	Start 16/7/2016 End 30/11/2016	
005	Human Resources	Company Risk no 5 Consequence no 5	3	2	6	• Risk treatment 5	1	2	2	Pierre M.	Start 10/2016 End 11/2016	
010	IT-Inform. Security	Company Risk no 10 Consequence no 10	3	2	6	• Risk treatment 10a • Risk treatment 10b • Risk treatment 10c	1	2	2	Monika K.	Start 1/6/2016 End 15/6/2016	
011	Business	Company Risk no 11 Consequence no 11	4	1	4	• Risk treatment 11	3	1	3	Boje D.	Start 1/9/2016 End 5/9/2016	
003	Business	Market instability due to coming elections Customers may hold purchase orders	1	4	4	• Offer better payment options • Minimize expenses	1	2	2	Michael K.	Start 1/5/2016 End 5/5/2016	
004	Business	Company Risk no 4 Consequence no 4	2	2	4	• Risk treatment 4	1	1	1	Heike K..	Start 1/7/2016 End 3/7/2016	
012	Governance	Company Risk no 12 Consequence no 12	1	3	3	• Risk treatment 12a • Risk treatment 12b	1	3	3	-	-	
008	IT-Inform. Security	Company Risk no 8 Consequence no 8	1	2	2	• Accept risk	1	2	2	-	-	

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3 -Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-Minor 3-Serius 4-Severe RISK RATING = PROBABILITY x IMPACT

V 1.0 PAGE 1 OF 1

ELEMENTARY GUIDE ON BUSINESS RESILIENCE

RISK REGISTER

(POSITIVE RISKS / OPPORTUNITIES)

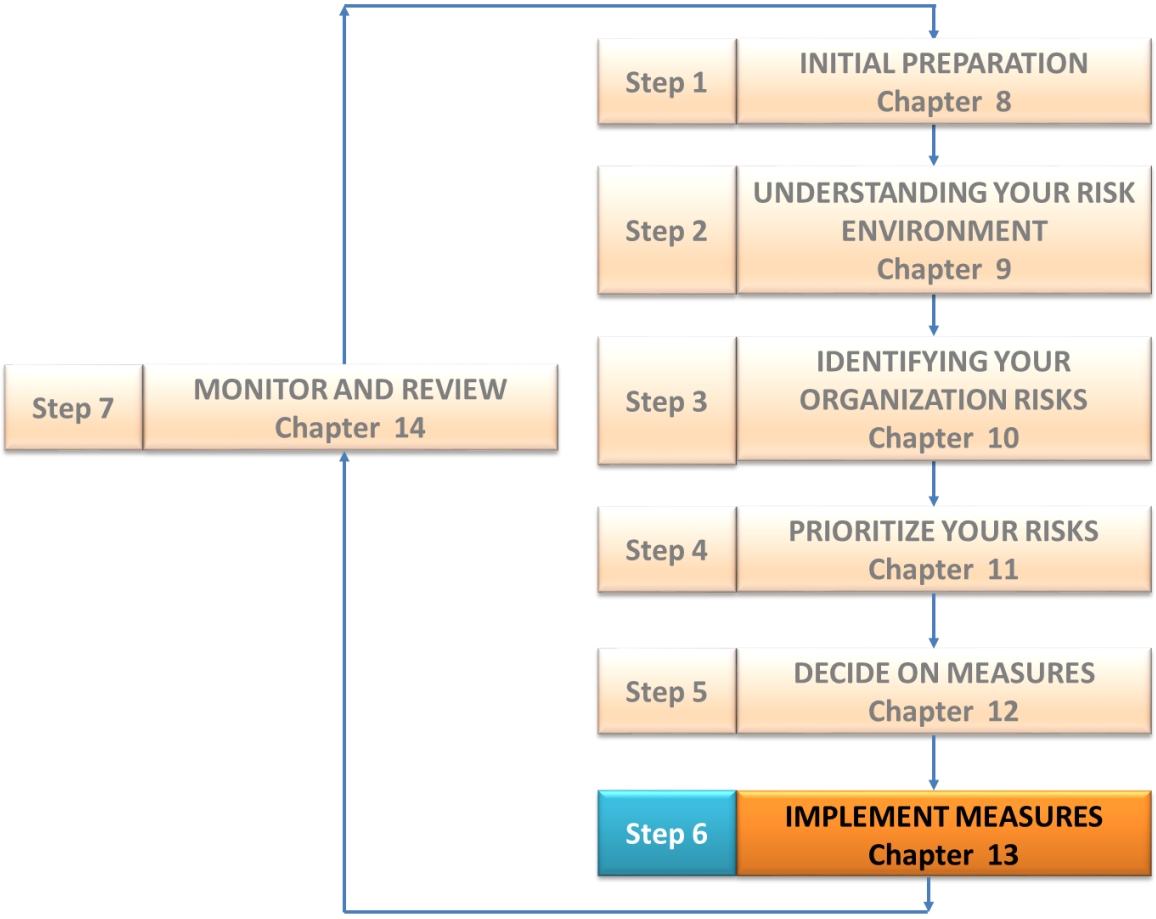
COMPANY: .....

Opportunity ID	Risk Category	Opportunity Description / Opportunity Consequence	Probability	Impact	Risk Rating	Possible Risk Treatment options	Probability after treatment	Impact after treatment	Risk rating after treatment	Person in charge of implementation	Implementation time plan	Notes
001	Operational	Increased purchase orders as of new WEB Site Sudden increase in purchase orders	3	3	9	• Prepare for overtimes • Employ new personnel	3	4	9	Pierre M.	Start 1/6/2016 End 15/6/2016	
005	Human Resources	Company Positive Risk no 5 Consequence no 5	4	2	8	• Risk treatment 5	3	2	6	Monika K.	Start 1/5/2016 End 5/5/2016	
003	Business	A competitor in the city may close down Sudden increase in purchase orders	2	4	8	• Employ new personnel • Aggressive advertisment	3	4	12	Boje D.	Start 1/8/2016 End 10/8/2016	
004	Business	Company Positive Risk no 4 Consequence no 4	2	3	6	• Risk treatment 4	2	8	8	Michael K.	Start 7/2016 End 30/10/2016	
002	Financial	Reduction of loan interest rates Interest will be less for about 3000 € / annually	2	2	4	• Accept the risk	2	2	4	-	-	

PROBABILITY: 1-Nearly impossible 2-Fairly improbable 3 -Probable 4-Very probable / almost certain IMPACT: 1-Insignificant 2-Minor 3-Serius 4-Severe RISK RATING = PROBABILITY x IMPACT

V 1.0 PAGE 1 OF 1

13. Step 6 – Implement measures



13.1. Implementation plan

Some of the decisions and measures might be very simple and not require any detailed planning preparation. Others might just require you to purchase and install specific equipment (e.g. fire extinguishers) or prepare written procedures or train your staff etc. These are measures or actions that usually only need to be taken once. In some cases they might require periodic follow-up and monitoring.

For the most complex measures, we advise preparing a typical project implementation plan for each one that includes the following elements as a minimum:

- Who is in charge of the implementation?
- Clear objectives on the practical result expected.
- A detailed plan of action and time schedule.

- Which resources are required for implementation, for example sources of funding, equipment, people and responsibilities and accountabilities for the delivery?
- A possible communication plan that identifies key stakeholders and ways to engage with them etc.
- A calculation of the expected risk status that you believe will be reached AFTER treatment has been implemented (residual risk).

This **implementation plan** must be fully authorised by the management (who are responsible for assigning the required resources) and could be documented separately if necessary.

13.2. Implementing information security measures and solutions

As discussed, identifying information security measures and solutions requires you to work on two layers (see chapter **12.2.2. ICT and Information Security**).

Implementing these measures and solutions, however, requires three layers of effort (!):

- Implementing measures in the strategic and managerial layer.
- Implementing measures in the technological layer.
- Monitoring the measures and solutions that will be used (monitoring layer).

(a) <u>Implementing measures in the strategic and managerial layer</u>

1) <u>ICT Organisation Strategies</u>

   Once selected, most of these strategies are usually completed with standard ICT project implementation (selecting a technological solution which is then implemented and employed in conjunction with training).

   Use your technology provider (dealer) to oversee the implementation. Ensure that you have a clear picture of the deliverables and that you receive the relevant documentation (e.g. user manuals, network maps etc.).

2) <u>Selecting an ICT dealer</u>

   Once you have decided which dealers you will be working with, ensure that you document the services and parameters for collaboration in a contractual

agreement. Use your legal advisor to help you with these commitments. Do not forget to document the information security obligations of dealers.

3) Organisation rules and policies

This is perhaps the most difficult and complex project to implement because once an organisation rule or policy has been decided (e.g. implementing a classification system to identify confidential documents and store them in locked drawers), **it must be engrained within all employee and managerial daily operations, as well as in the life of your organisation. It must become a routine for all!**

This level of implementation usually requires a four-stage plan:

a) Finalise the policy and DOCUMENT it in written form.

b) Make employees aware of the policy and TRAIN them about how it will be implemented.

c) Start to implement the policy in your daily operations.

d) CONTINOUSLY MONITOR whether the policy is being used in daily operations and is respected by everyone (including management). Ensure that it becomes an organisation's standard. AT ALL TIMES!

Carry out random checks and internal audits at specific time intervals to ensure that the policy is in place and is being respected.

Use disciplinary measures if the policy neglected. You may need to repeat the training.

These stages (d) and (b) are the most important for implementing a new policy.

(b) Implementing measures in the technological layer

Because these are technical measures, you will need the help of your ICT dealer or consultant to implement them.

Alongside technical implementation and set-up, this stage may sometimes require you to introduce internal procedures and to train users accordingly (e.g. encrypting or decrypting data on their PC's etc.).

(c) Monitoring layer

As discussed above, monitoring that rules and policies (once implemented) are engrained in daily operations and respected by all is just as important as the initial implementation of the rules.

There are four ways to carry this monitoring out:

1) Assign a specific employee the responsibility of engraining the rule or policy in your organisation's daily life. During the very first implementation period ask him to monitor whether the policy is being maintained on an almost continuous basis.

   It might be the case that implementation highlights the need for some adjustments to the rule. Respond accordingly by making the necessary changes and continuing with the general implementation of the improved policy.

2) Put disciplinary actions in place (employees re-attending a training is a less severe example), especially for those that deliberately bypass or 'forget' the rules and policies.

   If you identify a breach, reapply the rule or policy that has been violated immediately and directly. Make sure that everyone understands you are committed to using this rule or policy.

3) Perform random AND frequent audits for each rule and policy. This should be quite frequent during the very first stages and at specific time intervals later on.

4) Some organisations use specific software monitoring solutions which raise an alarm (for most of the discussed security rules and policies) when these are in use, at least in relation to the ICT systems and their use. These software solutions can often prevent deviation from a policy. Discuss this option with your ICT consultant or dealer and, with a cost-benefit approach in mind, consider using these tools.

Finally, we advise you to employ an external consultant (or have a professional volunteer) to run an annual audit of existing security measures and to make you

aware of any weaknesses he identifies. Based on this report you will be able to make the necessary adjustments and keep your organisation on a safe and secure path.

Keep in mind the dynamic nature of security that can change within seconds. This is why it is essential to constantly monitor, review, audit and improve your overall system.

Last but not least: never forget the need for ongoing training and raising the awareness of your employees about security.

13.3. Preparing plans and implementing solutions

Some measures will require you to prepare what we call 'plans'. These are documented procedures and relevant important information that you can use if your organisation's operations are about to be disrupted or have already been disrupted by a specific threat or threats. These 'plans' will guide and assist your organisation in effectively responding to the negative situation and recovering and resuming operations following the disruption.

As has been discussed, it is necessary to prepare specific plans to respond to and deal with risks that have a low probability and a high impact, or a high probability and a high impact, and which cannot be treated in any other way.

A non-exhaustive list of areas to be considered could include:

- Natural hazards (flooding, fires, winter storms, extreme temperatures, earthquakes, landslides, wildfires etc.).
- Technological hazards (power cuts, equipment failures, cyber security, release of hazardous materials etc.).
- Terrorism and violence (bombings, kidnappings, chemical or biological threats, violence at work, riots, wars etc.).
- Funding risks (failure of an important donor).

You should be fully aware that some plans (e.g. the backup and disaster recovery plans below) may require the (provision and) implementation of specific technical solutions and systems (e.g. a new disk for backups or a new server in an alternative location etc.). Do not forget to budget for their implementation. A plan is only a plan if the required supporting solutions are in place and in working condition.

13.3.1. How many plans are required?

AS MANY AS YOU NEED! There is no limit on the number of the contingency plans an organisation can prepare. A non-exhaustive list of areas to be considered could include:

- Emergency response & evacuation plans[13]
- Insurance plans
- Personnel succession (substitution) plans
- Dealer, 3rd party, or partner failure plans
- Donor failure plan
- IT systems backup plans
- Communication and notification plans
- Resources and operations recovery plan (disaster recovery plan)
- Information security incident response plans

You may prepare any other plan that you consider necessary for your organisation. In the paragraphs below, we will focus on the plans mentioned above and help you to prepare them, with the aim of increasing your resilience.

[13] Emergency and evacuation plans are considered obligatory in almost all countries.

13.4. Your 'business continuity plan' – one plan to include all plans

In our approach we will 'bundle' all of these plans into an integrated plan for your whole organisation, called a 'BUSINESS CONTINUITY PLAN'. This is a single document which includes all the 'plans' mentioned as different sections, chapters or attachments.

Use the form provided in the annex **18.3 Business Continuity Plan Template** that contains all the necessary parts for all of the plans.

These master plans, once prepared, will be your reference document for dealing with emergencies, negative incidents, security issues, and any other disasters.

13.4.1. Four important considerations

You should consider four key points when preparing this document:

(a) It should be **updated regularly** (e.g. every 3, 6, or at most 12 months). Although the first version may take some time to write, updating and refreshing the information it contains will only require limited time and effort.

(b) Ensure that **your employees are aware of this plan and are trained accordingly**. Training requires very little time and effort, yet results in enormous benefits.

(c) **Store a copy of the latest version of the document outside your office area** where it can still **be accessed 'almost immediately'**.

(d) **Treat the BC plan as a confidential document**. The information it contains is confidential and important for your operations, so you do not want it to fall into the hands of a competitor.

Be careful not to miss out any of the above.

13.4.2. Structure of the business continuity plan

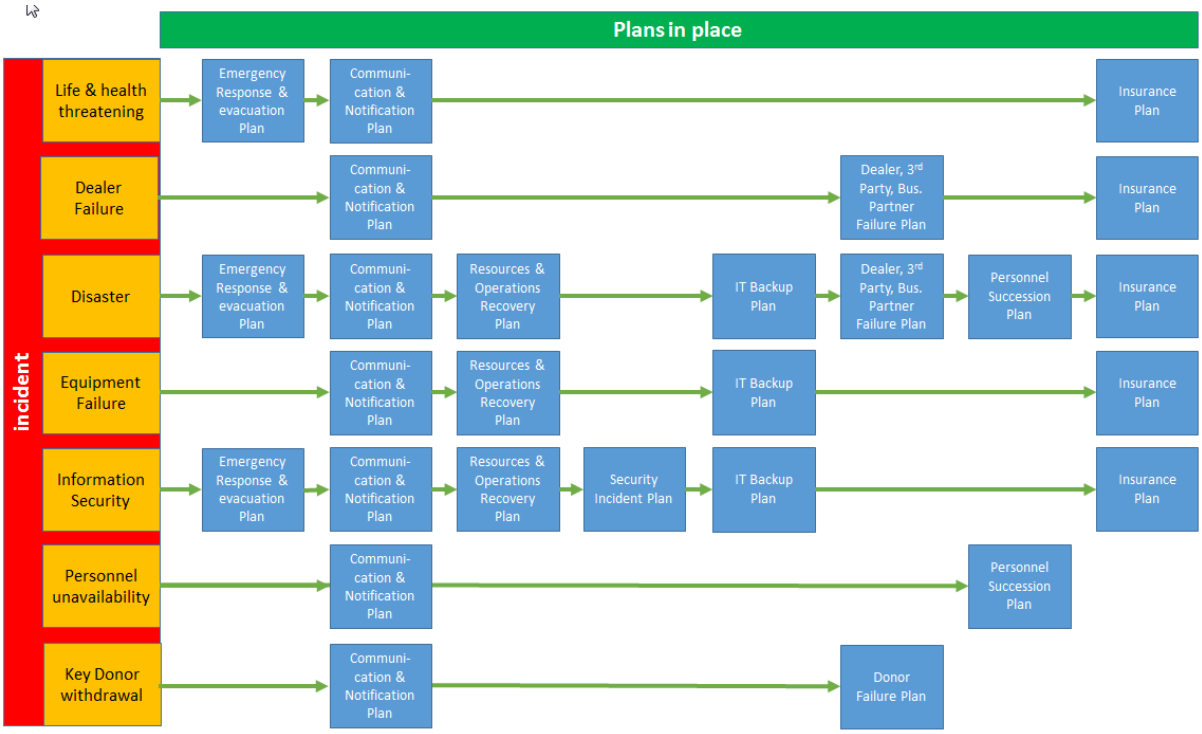
Your BC plan will be a single template document. It is divided into chapters, with the exception of the second and third chapters, labelled (B) and (C).

(B) is a general introductory chapter that refers to the whole document.

The main items to enter in chapter B:

- The address of your organisation premises.
- The storage area where you will keep a copy of the plan.
- The people responsible for each of the other plans. For a small NGO, this could be the same person for all of the plans.
- Information about the current and upcoming revision dates.

Chapter (C) contains the overarching picture of the plans you have prepared in response to the occurrence of different incidents. You might need to use more than one plan for each type of incident.



It is not always necessary to follow the exact approach above, since in some cases you will not require all plans (e.g. during a disaster you may not need your personnel succession (substitution) plan if all employees are available).

Each of the following chapters will cover one of the plans previously mentioned.

There are several tables in the template for each chapter. You can fill these in with your organisation's information. Several potential starting points are marked in yellow and some tables include examples to help you understand what is required. Not all items are applicable to every organisation, but an effort has been made to respond to

the vast majority of cases and meet most requirements. Feel free to change the requirements to match your NGO needs. Add your own columns to the tables or leave some areas empty if they are not relevant to your organisation.

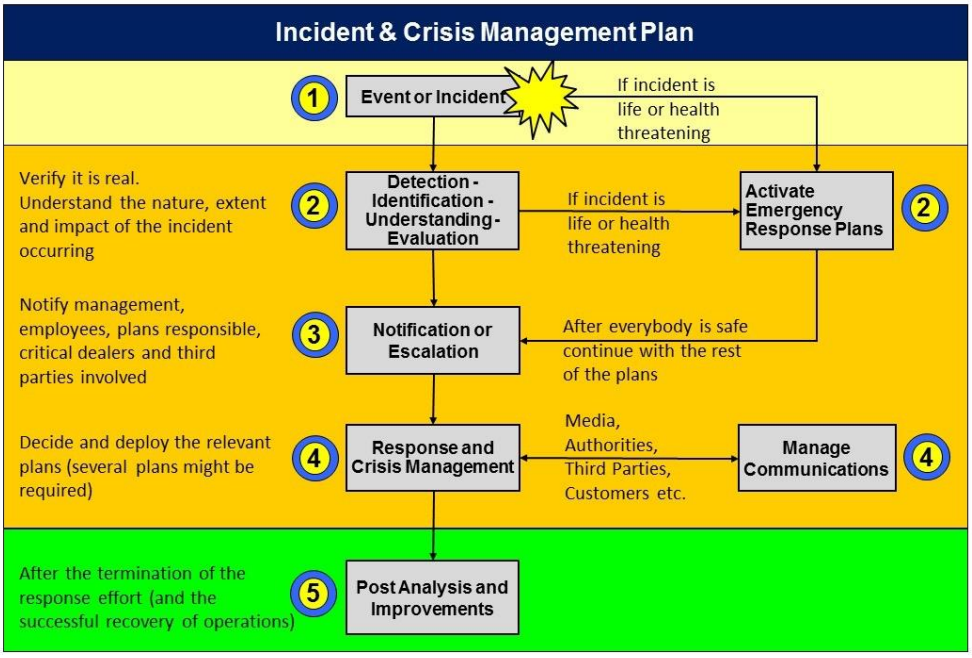
You will find information in the following paragraphs for each of the other plans separately.

There are also instructions given within the template document.

13.4.3. Incident management plan

The usual responses for dealing with an incident are shown in the picture below. Specific instructions are provided in the relevant plan document, but below are some specific necessary comments and definitions.

Depending on the type, extent and consequences of an incident, you may need to extend, slow down or speed up different steps.



For example, at step 1 the incident is either currently occurring or has already occurred. It may sometimes be minutes, hours, days or months before you realise this! For example, a fire will be identified within seconds or minutes; ERP hacking could be identified immediately, or only after several hours or days (for example if there is no user working with the ERP for a few hours or days), or even after months (e.g. if customer data has been illegally copied and provided to competitors).

In step 2, an employee has realised that there is an incident. This might be an incident related to a malfunction (e.g. technical problems with the ERP Server), or to the services of third parties (e.g. internet access disrupted due to dealer problems), or to service degradation arising as a result of hacking or simply an unplugged cable.

Diagnosis requires you to consider several factors, including:

- Is this a real or a fake incident (is it a false alarm from an exaggerating employee)?
- What is this really about?
- Is this just a server failure or have hackers hit your system and caused a denial of service? Or has a cable simply been unplugged (by mistake)?
- …

Diagnosis means understanding an incident's nature, extent and impact. It is a very important step.

Based on your diagnosis you will decide on your response strategy and next steps.

IMPORTANT DEFINITION: Whichever step you take, it is very important to remember the following: **If the incident is (or you suspect it to be) life or health threatening, you must IMMEDIATELY deploy your emergency response and evacuation plan as your first response.**

The complexity of the incident response (or whether crisis management is needed) is pictured in step 4 and can vary a lot from case to case. Some incidents might require the involvement of the state authorities (e.g. in the case of a fire, robbery, fraud etc.), whilst others just require you to repair a certain device.

Incidents that usually have an extended impact on organisation's operations, brand image, reputation or even life, will require a tailored approach. There is no single recipe for effective crisis management. Among other things, crisis management requires:

- An extended use of common sense
- An understanding of all impacts and consequences
- A combination of all resources related to the crisis (employees, legal advisors, operations managers etc.)
- Maturity
- Communication management

For incidents related to information security violations, speak to your ICT advisor or dealer (unless they are part of the problem, in which case you should refer to a different third party).

As step 5 shows, once you have managed to resume or recover your organisation's operations and are back in business, there remain important jobs to do:

- Identify the cause of the problem and work on eliminating it so that it never happens again.
- Identify which areas of your plans (that you used during the incident) require improvement. Improvements could be in relation to:
    - Poorly completed plan documentation
    - Missing (or inadequate) training of staff
    - Missing solutions that should had been in place (e.g. back up servers at an alternative site)
    - …

Make the necessary arrangements to close these gaps and ensure that these risks will not remerge, neither now nor in the future.

13.5. Emergency response & evacuation plan

This plan covers employee health and safety issues in light of life-threatening incidents such as fires or earthquakes etc.

We advise you to use **chapter D** in the template when preparing your own organisation emergency response and evacuation plan. This can be found in annex **18.3 Business Continuity Plan Template**.

13.6. Insurance planning

As has been discussed, insurance coverage is one of the most popular risk transfer strategies. By paying a small fee to an insurance firm, you will be able to get a good amount (or all) of the lost value back in the event that you suffer large losses that you cannot afford (site damage, asset loss, destruction or interruption for a long period of business, management liabilities, health recovery expenses).

It is important to make sure that:

- Your insurance coverage is in place and has not expired.
- The size of each insurance coverage contract is adequate and will be enough to cover or mitigate possible losses, because these have been decided by your organisation management or sponsors in cooperation with your insurance agents. Overestimating the amount of coverage leads to higher fees, while underestimating might not cover all your losses in the event of a negative incident.
- Insurance pay-outs cannot bring your operations back. You might get a big cheque from your insurance company, but this cannot bring back your customers or beneficiaries unless you have a continuity plan for recovering (at appropriate and pre-determined points) the services you provide to your customers. We therefore strongly advise you to prepare your insurance plan in parallel with your continuity and disaster recovery plan.

We advise you to use **chapter E** in the template when preparing your own organisation insurance plan. This can be found in annex **18.3 Business Continuity Plan Template** and will greatly help you to:

(a) Assess your current coverage status and make improvements where required.

(b) Have a list available together with your other plans when a negative incident occurs.

We strongly advise you to update it on the anniversary of every existing insurance contract, as well as once a year as a minimum.

13.7. Personnel succession (substitution) plan

A succession (substitution) plan for all your organisation's employees (including yourself) should be in place to ensure that no individual constitutes a 'single point of failure' within your NGO, especially in relation to those with critical activities or in key positions. A succession (substitution) plan is not about 'Who will take my place if or when I leave the organisation?', but rather 'Who could do my job if or when I am unavailable?'. Although a typical NGO will always have some lack of human resources and employees may have to cover several roles and responsibilities without the luxury of replacement, an effort should be made to outline your current status and, as a minimum, identify any gaps and risks in your current structure.

Document all relevant information in **chapter F** of the template provided in annex **18.3 Business Continuity Plan Template**.

13.8. Dealer, third party and partner failure plan

The failure of a key dealer or third party or partner that provides the organisation with critical funds or services could prove more than severe for your organisation's operational capability and the availability of your services.

For each important dealer or third party working alongside your organisation, we advise you to identify other alternatives or companies that could offer the same or similar services (that your quality standards require).

Document all relevant information in **chapter G** of the template provided in annex **18.3 Business Continuity Plan Template**.

13.9. Donor / Sponsor failure plan

The failure of a key donor or sponsor that provides the NGO organisation with critical funds or resources (e.g. donation money and funds, material, people, facilities etc.)

could prove more than severe for your organisation's operational capability and survival.

For each important donor or sponsor supporting or funding your organisation, we advise you to identify other alternatives and strategies that could be implemented or used in the case a donor / sponsor withdraws their support.

Though in the cases of several NGOs these depend on one main donor or sponsor, it is advised – if and where possible – to minimise the dependency on a single entity.

Document all relevant information in chapter H of the template provided in annex **18.3 Business Continuity Plan Template**.

13.10. IT backup plan

Backing up your IT data means creating and maintaining an electronic copy of all data in your ICT systems on a different media to the original data. It is more than important to have copies of your IT data. A backup copy of your data is actually as important as the original data.

There are several instances where you may need these copies. Here are some of the most common examples:

- If you lose your ICT systems for any reason (malfunction, hard disk failure, destruction following a fire etc.) you will lose all of your data. Even if you replace the lost systems with new ones, you will still need to replace your old data.
- Electronic data stored on ICT systems can be corrupted, usually due to technical causes. You may not be able to access or open existing files. This is where you may also need a backup copy.
- Users can often accidentally delete files, archives or other information stored on the system files and drives. If you have a backup copy, you will be able simply to restore the deleted files.

Begin by assigning someone the responsibility of backing your organisation data up. They will be responsible for all aspects related to backup.

Important: Unless you or an employee is competent enough with IT and your specific ICT systems and solutions, we strongly advise that you work with the agent (or dealer) responsible for your ICT systems.

Prepare your backup policy. Fill in the tables with the information required in **chapter I** of the template provided in annex **18.3 Business Continuity Plan Template**.

Ensure that this is frequently reviewed and updated.

13.11. Communication & notification plan

One of the most important issues during any emergency (and in the aftermath of a destructive or disastrous event) is effective communication with the stakeholders of your NGO. This includes communication with:

- Employees and Management
- Shareholders (if any)
- Members
- Donors
- Grant providers
- Sponsors
- Beneficiaries of your services / products
- Customers
- State authorities and emergency services
- Dealer, third parties and partners
- Neighbours and the public
- The media etc.

If the incident is directly related to your organisation, do not forget to contact and discuss it with your legal advisor.

Document all related information in **chapter J** of the template provided in annex **18.3 Business Continuity Plan Template**.

13.11.1. Responsibility for communications

Assign someone the responsibility for the organisation's internal and external communications (as well as assigning a deputy). They will be the only point of contact. Ensure that all employees are aware of this and direct all communication requests to this individual.

13.11.2. Emergency notification

If necessary (e.g. when beginning to use the disaster recovery plan), use the employee list in the communication plan to notify employees, key members, sponsors, donors etc.

13.11.3. Communication numbers for crises

It is also important to keep your existing communication lines open (NGO call centre phone lines, fax, email etc.). In the event of a disaster on your site, you may need to redirect these lines to another operational number that can be accessed from elsewhere (e.g. redirecting to your mobile phone). To this end, ensure that you have done all relevant preparations and have documented everything in your communication plan.

13.12. Resources and operations recovery plan (disaster recovery plan)

This plan covers operational interruptions. Operational interruptions can occur for many reasons, both internal and external. Equipment malfunction or failure, utility failure, unavailability of staff, failure of a key dealer, a disaster or bomb threat, to name but a few. These may disrupt or even stop operations.

13.12.1. Incident categories and response strategies

Disruptive incidents can usually be split into two main categories:

(a) **The unavailability, failure or malfunction** of any kind of resource. This includes:

- Malfunction or failure of IT infrastructure (servers, PC's, printers etc.).
- Failure of IT applications.
- Failure or malfunction of equipment (fax machine, photocopier, telephone centre etc.).
- Malfunction or loss of infrastructure (e.g. storage location, computer room etc.).
- Loss or unavailability of files and archives (whether electronic, on paper, etc.).
- Malfunction or failure of production systems.
- Failure of utilities and communications (power, data and voice communication, water etc.).
- Unavailability of staff (for several reasons, such as pandemic flu, fire injuries etc.).
- Failure of a significant third party business (dealer failure).
- Temporary unavailability of facilities (e.g. evacuation and no-access due to a bomb threat).

(b) **The total loss** of site, infrastructure and all equipment, assets, files and information due to a disastrous event (fire, flooding, earthquake etc.). This might be the most complex scenario if all of the above occur simultaneously.

In order to deal with this, you must work to prepare two different paths and alternative strategies:

(a) Path for the unavailability and failure of resources.

This is something that may happen in your organisation's everyday life: failure of a fax device, IT Server system, main computer application, or complete power loss due to problems in the local grid.

Examples of strategies that you could implement are:

- Prepare support and maintenance contracts with your key dealers.

- Procure a repair-onsite contract with an ICT dealer in case of your server failing.
- Procure a repair or replace contract in case of your photocopier failing.
- Procure a support contract for your software applications.

- Prepare or install alternative solutions, for example:
  - Have a UPS and a power generator in case of power failure.
  - Have a mirror drive in the server in case of hard disk failure.
  - Have two IT servers in a cluster set-up in case of main server failure.
- Prepare alternative processes:
  - Always have a backup policy to deal with data loss and hardware failures.
  - Work temporarily from home.
- Work with alternative service providers:
  - Use two different communication providers for internet and voice access at the same time.
  - Use two different dealers for the same service or product.

Etc.

(b) Disaster Recovery Path

This is usually managed by:

- Preparing **alternative solutions out of your site** (in case your organisation's site and all the assets it contains are lost completely).
- Prioritising activities to be recovered (you cannot recover everything at once because it is not feasible to have a 'second organisation' on standby. You therefore need to recover the most important activities for your business first).
- Preparing a structured plan of action to help you manage the disaster and recover on time.

For both paths, it is extremely important to know:

1. What would be the maximum time your organisation operations could stop without your NGO suffering severe consequences?
2. What is your planned recovery time objective following an incident?
3. How will you prioritise your activities, so you can start your recovery with what is most important?
4. Who will be responsible for what if a disaster occurs?
5. Where would your alternative office or working area be if your offices were completely lost? What would you do with your IT systems in this alternative working area? Will you buy them at that point or in advance so that they are already available? Will you use alternatives such as cloud services?

In order to answer these correctly, we advise that you read through the following paragraphs.

13.12.2. Action 1: Roles and responsibilities

Use the table provided in **chapter K** of the annex **18.3 Business Continuity Plan Template** to document the various roles and responsibilities of your staff in relation to (a) disaster recovery response and (b) equipment failure activities.

Role	Title	Responsibilities	Responsible Person Name	Deputy Name
Disaster Recovery Plan Team members	Decision maker	Responsible to decide the Plan invocation (emergency, recovery etc.)		
	Head of Crisis Management and Recovery Effort	Responsible to : Notify team members, critical vendors,		
	Team Members	Responsible to notify personnel & shareholders		
		Responsible to communicate with customers, media		
		Participate in the recovery effort		
		Participate in the recovery effort		
		Responsible for the recovery of IT systems		
Equipment Failure Response team	Responder	Failure of office equipment (fax, photocopiers etc.)		
		Failure of IT systems		
		Power & Utilities failure		

Choose someone for each area, as well as a deputy to lead the activity if the main person is unavailable. Use the examples provided in the table but also define other responsibilities that are missing.

In an NGO, the same person might be responsible for several roles, but make sure that there is still always a deputy for each role.

13.12.3. Action 2: Impact analysis and calculating recovery time objective

In case of a negative incident that disrupts or completely stops your organisation's operations (and therefore also the services it provides to its customers), it is very important to identify the **maximum tolerable period of disruption** (or stoppage) (MTPD[14]). This refers to the maximum amount of time that the organisation will not provide its services to customers without suffering a severe (catastrophic) impact.

As has been discussed, this impact could be financial (loss of large amounts of sponsor income, extensive expenses etc.), legal and regulatory (contractual penalties, fines from the state etc.), reputational (loss of image and trust), or customer loss etc.

To rate an impact you can use the following scale:

- Insignificant
- Minor
- Major
- Severe

This same scale was used in the chapter on risk rating **11.5 Risk Prioritisation**.

For example: if a fire destroys an organisation's premises then, based on their operations and customer obligations, they may suffer severe (catastrophic) losses if the organisation is still closed by day 4.

Their maximum tolerable period of disruption would therefore be day 3.

As a next step, decide on your organisation's **recovery time objective (RTO[15]).** This is the time you have to recover critical operations before you reach the maximum tolerable period of disruption (MTPD), namely recovery before the impact reaches a severe (catastrophic) level or remains at a major level for quite some time.

[14] MTPD: See chapter: 16 Selective Glossary and Abbreviations.

[15] RTO: See chapter: 16 Selective Glossary and Abbreviations.

A recovery time objective is usually shorter than the maximum tolerable period of disruption (MTPD). In the example above, RTO would be day 2 (or day 3 at its extreme).

Now we will look at how to calculate your MTPD and RTO. Using the fire example given above (destruction of your office area by fire), ask yourself what the maximum time would be that your organisation could remain closed and out of operation without suffering a severe (catastrophic) impact?

There are two approaches you can take to calculating your organisation's RTO:

(a) You could just decide it alone as the manager of the organisation. This is especially pertinent to small NGOs, since managers often have a good and detailed sense of their overall environment requirements and are therefore able to give (based on experience) their organisation's recovery time objective, e.g. 'Day 2'.

(b) You could also work through the following steps:

1. Use the table provided in **chapter K** of the annex **18.3 Business Continuity Plan Template** to identify your organisation's own impacts.
2. Fill in the columns under the title '**Time of Disrupted Operations**' for each impact by considering how the impacts on your organisation relate to the length of disruption (namely 'what if your organisation remained closed for 1, 2 or more days'). You may use colours to emphasise your findings.

   The time intervals can be completely customised. You could change the timeframes provided (1-12 hours, 1 day, 2 days, 3 days, 1 week, 2 weeks, 1 month, later) and use your own ones (e.g. 1-4 hours, 4-8 hours, 8 hours - 1 day, etc.).

   The list of impacts provided in the impact column is also only indicative. You could change these to impacts that you believe are more applicable for your organisation.
3. Based on the data you entered in step (2), fill in the column '**Maximum Tolerable Period of Disruption**' (MTPD) by entering the length of time before each impact becomes severe. For example, in the 5th row ('Contract

Penalties') the impact becomes severe if the organisation cannot open until the end of day 3. The maximum tolerable period of disruption is therefore 'Less than 3 days', or 'Day 2'.

Impact	Length of disruption to operations Indicate whether the impact of stopping operations is Insignificant, Minor, Major or Severe.									Maximum Tolerable Period of Disruption	Maximum Time of Recovery
	0-12 h	1 Day	2 Days	3 Days	1 Week	2 Weeks	1 Month	Later			
Loss of membership fees and donations	Insig.	Insig	Minor	Major	Severe				→	Less than 1 week	2-3 days
Impact on cash flow	Insig	Minor	Minor	Minor	Major	Major	Severe		→	Less than 1 month	1-2 weeks
Increase in expenses	Insig	Insig	Minor	Major	Major	Severe			→	Less than 2 weeks	3-5 days
Regulatory and other legal impacts	Insig	Insig	Minor	Major	Severe				→	Less than 1 week	2-3 days
Contract penalties	Insig	Insig	Minor	Severe					→	Less than 3 days	1-2 days
Beneficiaries dissatisfaction	Insig	Insig	Minor	Major	Major	Severe			→	Less than 2 weeks	1 week
Loss of Donors	Insig	Insig	Minor	Severe					→	Less than 2 days	1-2 days
Negative brand image and reputation	Insig	Insig	Minor	Major	Major	Severe			→	Less than 2 weeks	1 week
									→		
									→		
At organisation level: use the minimum of all									↓	Less than 2 days	1-2 days

4. Based on the data entered in step (3), calculate the "**Maximum Time of Recovery**" by selecting the value immediately less than that entered as the MTPD. In our example, for an MTPD value of 'less than 3 days', the maximum time of recovery is '1-2 days'.
5. Repeat steps 2, 3 and 4 for each impact in the table. In the empty lines you could add impacts that are not provided in the form.
6. In the final row, record the minimum time period out of all the entries in the two right-hand columns.

The value in the bottom right corner is the "**Maximum Time of Recovery**" for the whole organisation. This is what we call your organisation's **recovery time objective**, the target time in which your critical operations need to recover. In the example table above, this value is '1-2 Days'. This means that your organisation must **recover within the 1st or 2nd day AFTER a disruption has occurred**.

Your next efforts and solutions should therefore be done with reference to this timeframe. Not all of your operations must recover within this specific time frame,

but clearly those that will impact your organisation as calculated above if they stop. We will work on this in the next paragraph.

13.12.4. Action 3: Mapping activities and prioritising recovery

It is very important to map your organisation's activities (processes and similar tasks that help you deliver your services to your customers) and to prioritise them on the basis of their recovery time objectives. You will need this information and prioritisation (later) to ensure an effective and efficient recovery.

Use the table provided in **chapter K** of the annex **18.3 Business Continuity Plan Template** to identify your organisation's own activities and their recovery prioritisation.

Main processes / activities	Critical dates, periods related to the activity	Internal dependencies, systems, applications, other processes	External dependencies (Dealers, Third parties etc.)	Maximum tolerable period of disruption	Recovery time objective

13.12.5. Action 4: Define and document the disaster recovery strategy

Although recovery strategies for equipment malfunctions and failures are usually easy (e.g. call the equipment dealer when necessary to repair the device, or have ongoing support and repair contracts, second systems and alternative solutions), recovering from a disaster will require you to have several pre-prepared solutions that are available at the time of the disaster. Without these your organisation might not be able to recover within the required time interval (recovery time objective).

In order to prepare a response for disastrous incidents (those that cause the loss of the organisation site and any important equipment, assets, files and archives stored there) you need to first consider:

- An alternative working area from which staff will work for the days following the disaster. This might be a second site, a home office, a temporarily rented office area, or even a pre-allocated working area in a collocation centre or an alternative area offered by a sponsor.
- The reality that pre-prepared alternative solutions for facilities and systems could require several days or weeks to be re-installed. This might not be affordable for your organisation if it takes longer that your recovery time objective and maximum tolerable period of disruption (e.g. purchasing and re-installing a big server to run the organisation's ERP may take 2-4 weeks. This length of time is not feasible for you, because being inactive for such a long time might drive your NGO out of business).
- The ad-hoc purchase of specific equipment that is easy to find, available in local stores, and fast to purchase and install (e.g. a fax device).

It is therefore important to document any existing strategies in the plan that you will use during recovery. The recovery effort will otherwise take place in an ad-hoc and try-your-best way.

In the template for this plan in **chapter K, paragraph K4a** of the Annex **18.3 Business Continuity Plan Template** fill in the relevant space after each question with existing alternative solutions.

13.12.6. Action 5: Prepare a resources and operations recovery plan

A number of tables are provided in **chapter K, paragraph K4b** of the Annex **18.3 Business Continuity Plan Template**. These will help you document the required information in the plan in connection with the recovery of key operations and resources in the event of (a) failure or malfunction and (b) loss due to disaster.

The tables include references to:

(a) Organisation staff (provide information on where each staff member will work, the expected recovery time frames and the conditions in each alternative area).

Staff (numbers during normal operations and at alternative work areas and relocations)				
Details or Employee name	**Normal Operations Status & Quantities**	**Alternative site Strategy (where they will work from)**	**Expected Recovery time**	**Describe how they will have access to applications, files, email etc**
Manager	1	Work from his home with personal laptop	Can start from day 1	Will use internet to access the cloud applications
Consultants	2	work from their home for 2 weeks. Will have to buy 2 laptops at day 1	Start from home on day 2	
Secretary	1	Will use the office at the XYZ collocation center where the company has rented an area		
Accountant	1			

(b) IT applications.

(c) ICT systems and relevant devices.

(d) Office equipment.

(e) Equipment used for production purposes (e.g. printing machines).

(f) Data and voice communication connections.

(g) Files and organisation archives.

Information can be added to meet the specific needs of your organisation. Some examples are provided to help you understanding the process better. Different columns should be used to describe your current approach and solution and how they relate to the two types of disruptions; failure or malfunction and loss due to disaster (or a war or a terrorist activity). You can be as analytical as necessary to ensure that you have documented the information that will help you recover.

13.12.7. Action 6: Prepare a disaster recovery response action list

In this paragraph you should record a list of actions to be taken and considered by you (or any other person assigned to be the recovery coordinator) in the event of a disastrous incident.

A sample list is provided in **chapter K, paragraph K5** of the annex **18.3 Business Continuity Plan Template**.

13.13. Information security incident response plan

An information security incident response is not that far away or very different from a usual incident management plan. A template for your information security response plan is provided in this guide (**chapter L** of the annex **18.3 Business Continuity Plan Template**) and may be used in conjunction with a generic incident management plan.

The response required mainly depends on the type of incident. The key areas listed below will require extra attention and effort (depending on the specific case).

13.13.1. Early warnings (sometimes neglected)

In some cases there may be evidence or indication that a security incident is likely to occur even before it actually takes place. This could include:

- Warnings provided by operating systems, such as 'data read error on disk xxx'. This might appear several times on a user's screen before the disk actually fails.
- One or several unknown agents using the organisation Wi-Fi.
- An application shows multiple failed login attempts from an unknown user or an unfamiliar remote system.
- Negative behaviour of dissatisfied employees may result in a possible future security violation in response.
- …

Employees should keep their eyes open and notify management when they become aware of these early warnings. This means that measures to monitor or mitigate risks can be considered and implemented before the incident occurs.

13.13.2. Detecting an incident

There is often a lack of knowledge and understanding about technical problems in most NGOs because their staff lacks an ICT expert. This means that the most challenging part of the effort can be:

- '**Detecting if there really is a security incident?**' and, if there is,
- '**Identifying and understanding its extent and impact**'

In the information security response plan template provided, there is a list of some warning signs or evidences that a security incident is currently taking place or has already occurred which might help.

This process can also be helped by the numerous scenarios of what could happen and what the indicators of these security incidents would be, so that your ICT Consultant can work through them with your employees. Answers to questions such as the ones mentioned below can therefore be of great assistance to you if asked by ICT experts to your employees:

- What would indicate that our website is under a denial of service attack?
- What would indicate that our database server has been compromised?
- How do I identify a phishing email?
- How will we know if that there has been unauthorised access to our ERP system?
- …

13.13.3. Finding and preserving evidence (forensics)

When a security incident is directly related to a possible legal violation (e.g. unauthorised intrusion, theft of confidential data, injection of malicious software into organisation systems etc.), then it is important not only to identify the intrusion or the malicious activity, but also to preserve relevant information and evidence about the incident (as it is captured by your ICT systems). Keep this as proof and supporting material for any future legal action.

You will need to work in direct collaboration with your ICT consultant to collect this information (e.g. by backing up infected systems, copying system logs etc.) and to keep it safe.

13.13.4. Notifying stakeholders

Some incidents may not only target your organisation's systems but also use them in order to further infect any or all of the third party systems that are connected (in different ways) to your systems.

For example:

- A virus that infects your email server may also use this server and all of the email addresses in your contact list to send spam or infected messages and further spread the infection.
- A hacker who accesses your customer data and information could also find their bank account numbers, credit card ID's and authorisation codes, since this data is stored in your systems.

It is important in such cases to follow good business practices and legal requirements by notifying all of your customers and contacts about the incident. Let them know what happened, how you have responded so far and what their risk exposure is etc.

Before proceeding with this step it is important that your organisation's management work together with a legal advisor and ICT consultant to decide whether this communication is necessary. They will also need to define what will be communicated, how it will be phrased, who will receive the messages, the extent to which you will accept responsibility, etc.

For certain incidents the state authorities should also be notified and provided with all the necessary information and (if requested) allowed access to the organisation's systems and data.

13.14. Storing the plan document

As has been discussed, do not forget to store a copy of your plan in the designated alternative location. This should be off-site and could be the manager's house, a password-accessed web page, or any location that could keep it safe and available when required.

Do not forget to communicate the storage location and access process to everyone responsible for its deployment and use. Check at least once every six months that

the copy of the plan (in whichever media format it is stored) is in place and in good condition. Make sure that the plan is stored safely at the alternative location.

13.15. Training concerning the plans

Generally speaking, having plans that no one knows exist, how they would use them, or where to find them when required, is the same as having no plans at all. Now that you have prepared your plans and implemented all the solutions and the measures that you have selected, you should proceed to train your employees in the following way:

- Organise a training session.
- Distribute the prepared documents.
- Explain roles and responsibilities.
- Explain which tasks are to be done.
- Explain about communication planning.
- Explain about decision-making and the flow of activities and steps.
- Explain the importance of the plans. Discuss the objectives, content and provisions of each plan.

A good way to strengthen the knowledge and awareness of staff is to ask them to run training sessions themselves for any new employees.

Bear in mind that this training should be repeated every time there is a new version of the plans and whenever a new employee is hired and repeat the training for all staff at least once a year.

13.16. Testing and exercising

You cannot be certain that a plan supports the objectives for which it was written unless you test it. Tests and exercises should be designed and run at frequent time intervals in order to ensure that:

(a) The plan’s provisions are checked to see if they are correct and up-to-date.

(b) The response and recovery team members and organisation employees increase their knowledge and understanding about the roles, responsibilities and activities they must carry out when an incident occurs. They should also improve their own performance and identify opportunities to expand their current capabilities.

(c) The response and recovery team members are committed to working together and to managing their response to an incident.

There are different types of exercises that you could use to evaluate continuity plans, procedures and capabilities:

- Walkthroughs and table-top exercises

  These are usually discussion-based sessions with employees and response team members where they can talk about their roles and actions during an emergency situation. It is the most simple and cost-effective form of exercise and can be accomplished within a short period of time. You can repeat it often, especially when new members of staff join your organisation.

  Scenarios can vary from simple events and incidents (e.g. losing your office keys) to more complicated examples (e.g. premises burning down).

- Functional exercises

  These are scenario-driven exercises that mainly focus on the failure of specific pieces of equipment or sections of your organisation's daily operations (e.g. the failure of your IT systems or the failure of communication systems, etc.). This exercise requires you to test any alternative solutions that are in place to ensure that they are fully functional and that your team is capable of responding as planned. This is typically the exercise used for IT and communication systems, as well as for any other operational systems and facilities.

  It is also used to practice specific functionalities, such as the notification plan for team members.

- Full-scale exercises

  A full-scale exercise is similar to a real incident. It is the most complex exercise because it requires that you test your relocation plans and use (any) alternative facilities and equipment that is in place. It requires some preparation and usually

lasts longer than any of the other forms of exercise. You will usually test all parts of the plan (including the recovery of IT systems).

Make notes during all types of exercises with which to record any improvements that are required. These could be in relation to solutions that are in place, staff engagement, activities that need to be improved or the planning process itself. Use these notes then to improve your existing plans.

13.16.1. Developing an exercise programme

This typically requires you to prepare the following steps:

- Decide on the type of the exercise (walkthrough, full-scale etc.).
- Decide which participants you will need.
- Define the scope (location, operations, systems, or activities etc.) that the exercise will cover.
- Define the scenarios (e.g. failure, fire, or earthquake, terrorist action, war etc.).
- Define the start time and duration of the exercise.
- Prepare evaluation and improvement forms for the exercise and distribute these to all participants.
- Ensure that the exercise itself does not create extra risk for your organisation. For example, do not run the exercise on a day with high business stress (such as the end of a month), because this could easily cause operational problems for your organisation. Run the exercise during off-peak hours.
- Notify the staff that you have selected to participate.

Once the exercise has been run, carry out a post-exercise meeting to discuss the results of the exercise. Note which areas were successful and which areas require improvement. Collect evaluation forms and improvement suggestions and decide on which actions and measures you will take to improve your organisation’s plans and the response capabilities of your teams.

Update the plans and let your people know about any updates you make.

13.17. Quality check for the measures implemented

Once each measure has been implemented, we strongly advise that you spend between a few seconds and a few minutes (depending on the measure) checking whether the objectives of the measure have been achieved (as they were defined when the measure was first decided and approved).

Check the quality of the work that has been done, just as you would with any other project, work, or activity that takes place within your organisation.

Ensure that the measures implemented to treat a specific risk have not created other risks that could cause more problems than those that have been mitigated.

Finally, check that **the current rating of the treated risk** is the same as the rating that was targeted during the decision-making process. Evaluate the risk's current probability and impact. Compare the resulting risk rating to the rating that you documented before the implementation started:

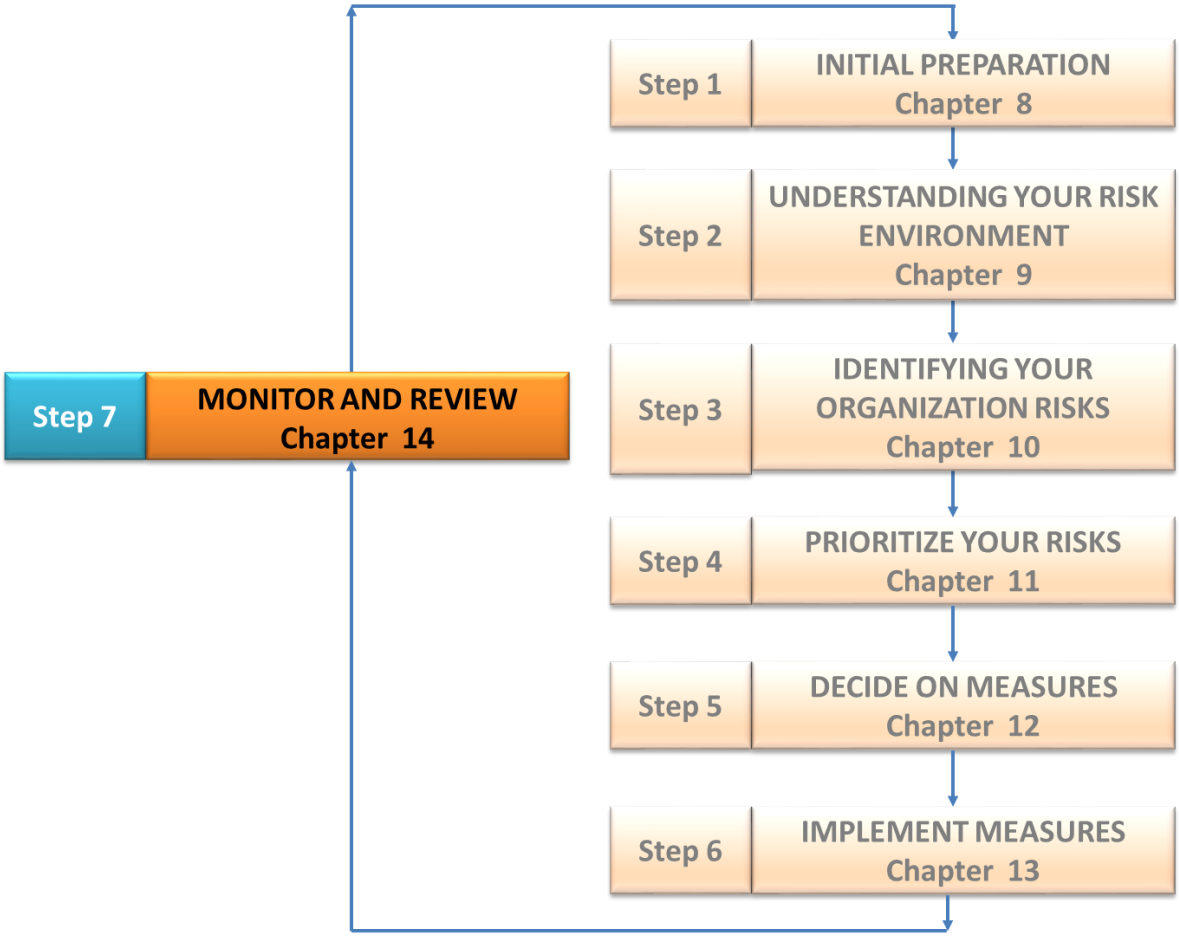
(a) If the rating is the same or better (smaller) then you have done a great job.

(b) If the rating is higher, begin by trying to understand the reasons for this and then decide whether the new risk rating is at an acceptable level for you.

- If it is at an acceptable level, **correct the "Risk Rating After Treatment" column for the specific risk in your risk register and use the column "Notes" to record this decision and any other relevant information**.
- If this is not the case then you will need to continue working and identify which extra measures or improvements you could implement to meet your initial rating objectives. Follow the relevant steps as they are presented and discussed above to do this.

You must keep improving the suitability, adequacy and effectiveness of the measures implemented. You can use the processes of your resilience management system and the CASSANDRA approach to achieve this continuous improvement.

14. Step 7 – Monitor and review



Once you have finished step 6, you will typically have completed what we call your first 'life cycle' of the risk management process.

You have identified the risks that your NGO was exposed to and have assessed and prioritised them and chosen and implemented appropriate treatments, measures and controls so that these risks have been reduced to a level deemed acceptable by your organisation's management.

Now that your organisation is more resilient than it was before, you need to ensure that you retain this higher level of resilience by working hard. If you do so, you will only retain this resilience in the future but, even more than that, you will be continuously improving.

It is necessary for you to work on the following:

(a) Prepare a resilience project **document archive**. Ensure that all project documentation is archived and, most of all, that the risk register is keep up-to-date and readily available.

Ensure that the contingency and recovery plans and information are available at the points and places agreed and can be accessed if a disaster occurs.

(b) Ensure that your **employees, management and related members are all aware of and properly trained regarding** the solutions you have implemented, the controls you have put in place, and the continuity and security plans and solutions you have prepared.

Schedule a training session to take place at least once a year (this does not have last a long time). This will help raise the awareness of staff and will ensure that the requisite knowledge about the prepared plans and solutions is shared by all those responsible.

Ensure that roles and responsibilities, as they have been defined in the various selected measures and controls, are clear and that they are followed by your employees (e.g. the person responsible for the backup should have a clear picture of their responsibilities and fulfil these on a daily basis).

(c) As an improvement to (b), you need to work on **embedding a risk awareness culture within your organisation's daily operations**.

Request that all employees (including yourself) filter every (new) process, every action taken, and every decision made through a risk management perspective. It would the greatest success for the management of your organisation if they could engrain risk management as standard for all decision-making processes.

(d) Schedule and ensure that **once every year, as a minimum, you re-run this same 'life cycle'** (steps 2 to 6), update your register, improve the risk rating of risks that remain by implementing new or improving existing measures, controls and solutions, prepare new contingencies and plans for key systems and activities, and improve your current resilience status.

Keep in mind that this effort will be easier the second time you run through it. Both the quality of your work and the results that you achieve (further improving your organisation's resilience) will also be more effective and advanced.

(e) Set up a process of **regular** (e.g. quarterly) **reviews of the solutions**, measures and controls that have been implemented to check whether they are as effective and efficient as you designed and expected to be or if they require further improvements.

Be on the lookout for changes to your external and internal environment. Identify any newly emerging risks, including changes to existing risks that may require you to revise your risk treatments and priorities.

Update your register and treat any new or changing risks in accordance with the processes described.

Ensure at frequent intervals (e.g. quarterly) that alternative contingency solutions to those already implemented are available and would function properly if required (e.g. that the alternative server is in place and functional, that backup devices and alternative working areas are available etc.).

Make sure that you have a mechanism in place **to monitor continuously whether the security rules and policies you have chosen as measures** (see chapter **12.2.2. ICT and Information Security Measures**) have become habitual and a part of everyone's daily operations.

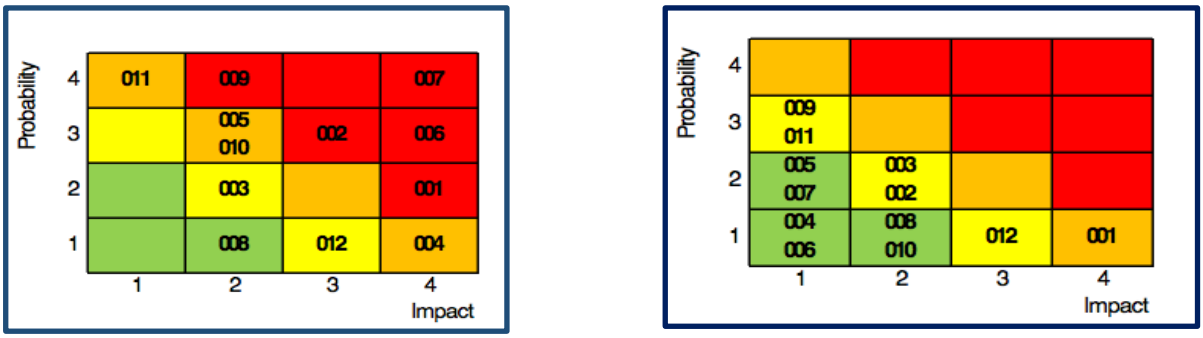
(f) Ensure that **you exercise all contingency plans at least once a year** to check that their content is really up-to-date and to help your teams to recover the systems, activities and services that they support as expected.

Check that all employees who participated in the contingency plan exercises know their roles and responsibilities as they are defined in the plans and that they know how to successfully respond when necessary.

(g) Keep a diary to **record negative events and incidents that have occurred** (including near-misses). This should also include all changes, trends, successes and failures. Analyse them and try to learn from every negative incident or failure, with the aim of improving your organisation's resilience by improving existing measures and deploying new ones when necessary.

14.1. Residual risk ('The day after')

Once mitigation measures have been implemented, each risk will have a new rating (due to a new probability or impact). This new risk rating, once you have accepted it, is called the **residual risk** and details the remaining risk ratings after the treatment has been implemented**.**



Risk Matrix BEFORE the treatment has been implemented

TREATMENT →

Risk Matrix AFTER the treatment has been implemented

These (new) risk statuses should be monitored on an ongoing basis with both old and new risks (that may be added as part of the continuous risk monitoring and control).

14.2. Resilience and risk management: daily operations

Embedding risk management in an organisation's daily operations is the best approach and objective for a project effort like this.

This is the only way to ensure that every decision, activity, process and function will take into account existing threats, risk exposures and the measures that may be required to keep the organisation on track.

The more you practice this, the more resilient your organisation will be.

15. From elementary to proficient

15.1. CASSANDRA: a major step towards resilience

CASSANDRA is a free of charge methodology that focuses on assisting SMEs and NGOs.

An NGO that follows the CASSANDRA methodology by following the roadmap and steps outlined in this guide will see major improvements in terms of minimising its exposure to risks, turning threats and vulnerabilities into opportunities, and increasing its resilience. The CASSANDRA approach is fully compliant with the requirements of relevant international standards and focuses primarily on actions that will improve that organisational resilience of their operations. It does this by utilising risk management, business continuity and information security principles in an appropriate, effective and efficient way that corresponds with the size and capabilities of average NGOs.

CASSANDRA approach is fully compliant with the requirements of relevant international standards and aims to improve practically the resilience of NGOs.

15.2. Steps and actions towards the next level of business resilience

15.2.1. International standards

Several international standards are applicable to the content objectives of this guide:

ISO 31000:2009, Risk management - Principles and guidelines[16] provides principles and a framework and process for managing risk. It can be used by any organisation, regardless of its size, activity or which sector it is in. Using ISO 31000 can help organisations increase their likelihood of achieving objectives, improve the way in which they identify opportunities and threats, and help them effectively to allocate and use risk treatment resources.

ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements is part of the ISO 27000 family of standards that helps organisations keep information assets secure. ISO/IEC 27001 is

[16] ISO, the International Organization for Standardization, www.iso.org

the most well-known standard in this family. It outlines the requirements for establishing, implementing, maintaining and continually improving an information security management system within an organisation's specific context. It also includes requirements for the assessment and treatment of information security risks that are tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.

ISO 22301:2012 Societal security - Business continuity management systems - Requirements specifies requirements for establishing and running a management system to protect against and reduce the likelihood of disruptive incidents occurring, and to prepare for, respond to, and recover from them if they arise. The requirements specified in ISO 22301:2012 are generic and intended to be applicable to all organisations and their various parts, regardless of type, size or nature.

ISO 9001:2015 Quality management systems - Requirements is the most well-known member of the ISO 9000 family. It addresses various aspects of quality management and provides guidance and tools for companies and organisations who want to ensure that their products and services consistently meet customer requirements, and that they are consistently improving in quality. ISO 9001 requires the implementation of risk management and its use in company operations. The requirements set out in ISO 9001:2015 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.

ISO/DIS 22316 Security and resilience - Guidelines for organizational resilience is a standard 'under development status' (when this guide was being written). It features a framework that helps organisations make their businesses future-proof by creating a resilience culture and improving their capacity to anticipate and respond to threats and opportunities. This enables the organisation to keep delivering on its commitments in the face of complex changes.

15.2.2. GAP Analysis

Several websites and books provide (often free of charge) an approach to help you measure your organisation's current compliance status with the relevant ISO

requirements. The following samples of links provide some helpful examples (active when this guide was being compiled)[17]:

For ISO 27001

http://advisera.com/27001academy/free-tools/free-iso-27001-gap-analysis-tool/

http://www.bsigroup.com/LocalFiles/BSI-ISOIEC27001-Assessment-Checklist-UK-EN.pdf

For ISO 22301

http://www.bsigroup.com/LocalFiles/es-MX/ISO%2022301/BSI-ISO-22301-Self-Assesment-checklist.pdf

For ISO 9001

http://advisera.com/9001academy/iso-9001-gap-analysis-tool/

https://www.bsigroup.com/Documents/iso-9001/resources/BSI-ISO-9001-self-assessment-checklist.pdf

http://www.iso9001help.co.uk/Gap%20Analysis%20Checklist.pdf

15.2.3. Compliance and certification

Full compliance to any of the above ISO certifications (in each case) requires that a number of organisation decisions be made, a number of policies, procedures and processes adopted and documented, a monitoring system implemented, a number of reports produced, and frequent internal and external audits carried out to ensure that there is a properly operating management system in place (this means a system that can guarantee the implementation of all ISO requirements and proper management

[17] As per 31 August 2017.

of all ISO controls). Although every organisation could theoretically make itself compliant with all the requirements of the above management systems by its own team efforts, this is seldom the approach taken in real life. Once an organisation has decided to proceed, it is recommended that they make use of the services of a pertinent field expert or consultant who will assist them with the appropriate, expeditious implementation.

Certification is provided by certain authorities (certification bodies) and requires the successful completion of an audit by the relevant authority. Certification is only possible for ISO/IEC 9001, ISO/IEC 22301 and ISO/IEC 27001 and it is not obligatory. Some companies and organisation choose to implement these standards so that they can benefit from the best practices it contains. Others may wish to be certified so that they can reassure customers and clients that they have been followed their recommendations.

16. Selective Glossary and Abbreviations

Activity: A process or set of processes undertaken by an organisation (or on its behalf) that produces or supports one or more products and services (ISO 22301:2012).

Availability of information: protecting information and ensuring that it is available when needed.

Business Continuity: The ability of an organisation to continue delivery of its products or services at acceptable predefined levels following a disruptive incident (ISO 22300:2012).

Business Continuity Plan: Documented procedures that guide organisations on how to respond, recover, resume and restore a predefined level of operation following disruption (ISO 22301:2012).

Crisis: A situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organisation and requires urgent action (ISO 22300:2012).

Confidentiality of information: The property that information is not to be made available or disclosed to unauthorised individuals, entities, or processes.

Cyber risk: Any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems**.**

Dealer: Also referred to as a 'vendor' or 'supplier', this term indicates the member of a supply chain who makes goods and/or services available to companies and/or consumers.

Enterprise resource planning (**ERP**): Often referred to as a category of business management software, this is typically a suite of integrated applications that an organisation can use to collect, store, manage and interpret data from their many business activities. It usually covers areas such as accounting, sales, asset management, human resources management etc.

Exposure: A situation, practice, or condition that may lead to an adverse consequence; an activity or resource; people and assets.

Hazard: A condition or circumstance that may cause harm or loss due to a particular peril; characteristics that make the likelihood of a loss from a given peril greater. A source of potential harm.

ICT: Information and communications technology (includes any computer hardware, software, communications of all kinds).

Incident: Situation that might be, or could lead to, a disruption, loss, emergency or crisis (ISO 22300:2012).

Information and information assets: All information that may be in the form of data stored electronically (in disks, CDs etc.) or IT systems (that store and process data

and information) or communication systems (that transfer data from and to your systems) or IT applications (ERP, email etc.) or in the form of paper files or archives stored in drawers or even non-tangible ones e.g. intellectual property rights.

Information security: The protection of the organisation's information and information assets (of all kinds, either tangible or intangible, paper or electronic, etc.). It refers to protecting and preserving the confidentiality, integrity, authenticity, availability, and reliability of information.

Integrity of information: Maintaining and assuring the accuracy and completeness of data, that is, protecting data from unauthorised or undetected changes, including deletion.

Issue: A problem that has happened and is already a reality that is having an impact on an organisation's objectives and operations.

Maximum Tolerable Period of Disruption (MTPD): The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. (ISO 22301:2012).

Non-Governmental Organisations (NGOs): Voluntary self-governing bodies or organisations established to pursue the essentially non-profit-making objectives of their founders or members.

Organisational Resilience: The ability to anticipate key events from emerging trends, constantly adapt to change and bounce back from disruptive and damaging incidents (The BCI, 2013).

Recovery Time Objective (RTO): The period of time following an incident within which a product or an activity must be resumed, or resources must be recovered (ISO 22301:2012).

Residual Risk: The part of a risk remaining after the initial risk has been treated (measures and controls have been implemented).

Risk: A current possibility (uncertainty) that may become a reality in the future and, if it occurs, may have a positive or negative consequence (impact) on/for your operations.

Resilience: The adaptive capacity of an organisation in a complex and changing environment.

Risk Management: Coordinated activities to direct and control an organisation in relation to risk.

SMEs: Small and Medium-sized Enterprises. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million €, and/or an annual balance sheet total not exceeding 43 million €.

UPS: Uninterruptible Power Supply (also uninterruptible power source), UPS or battery/flywheel backup, is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails. A UPS is typically used to protect hardware such as computers, data centres, telecommunication equipment or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption or data loss.

17. Selective Bibliography

BCI Good Practice Guidelines 2013, The Business Continuity Institute

ISO 9001:2015 Quality management systems – Requirements

ISO 22301:2012 Societal security – Business continuity management systems – Requirements

ISO 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements

ISO 31000 Risk Management – Principles and guidelines

ISO/DIS 22316 Security and resilience — Guidelines for organizational resilience

Risk Management Standard – The Institute of Risk Management (IRM)

The Nuclear Energy Option, Bernard L. Cohen, Plenum Press, 1990

18. Annexes

18.1. Risk register template

Attached as separate documents (Excel forms).

18.2. Examples of possible mitigation strategies and measures

Scope related and Strategic Risks	
Risks	**Possible mitigation strategies and measures**
Market risks (and business area risks)	Review Business Plan
Political environment	Review Business Plan
Competition	Market information, reports, reviews Review of services, sponsors and donors, etc.
Public safety status	Review your physical security measures or insurance coverage
Country economy	Review business plan for the short, middle and long term
Change in customer behaviour	Review marketing and sales strategy and tactics Customer satisfaction surveys
Changes in the demand for services	Review social and political environment, marketing strategy and tactics Review and change business plan Discuss with donors, sponsors and beneficiaries
Labour laws (changes in or existing problems)	Review employee engagement contracts
New disruptive technologies	Review marketing and operations strategy and tactics. Review and change sales and business plan
Rising labour costs or costs of materials	Profit and loss statements Cash flow plans Contracts with dealers/sponsors
Investment risks	Prepare a detailed business plan Review business plan with an accountant, bank or other consultant as well as sponsors & members
Brand and marketing communication	Organisation and brand communication plan
Reputation risks	Organisation and brand communication plan
Fraud and corruption	Written and documented procedures Periodic audit plan (internal or external)

Scope related and Strategic Risks	
Risks	**Possible mitigation strategies and measures**
Obsolescence of intellectual property	Review expiration dates Review marketing strategy and tactics Review and change business plan
Poor quality control and service placement	Documented procedures, forms Quality audits Beneficiaries and customers satisfaction surveys
Inadequate investment in R&D	Include R&D effort in annual budget plan

Operational and Continuity Risks	
Risks	**Possible mitigation strategies and measures**
Poor quality in services delivery	Written procedures, training of employees, quality assurance process, monitoring of delivery, discussing feedback with customers
Poor project management	Training, written procedures, monitoring
Logistics and transportation risks	Prepare contingencies in case any part of the supply chain fails, (loss of dealer, warehouse etc.) Assess or improve current insurance plan, outsource to third party
Demand changes and ability to deliver	Frequent review of project delivery Review of business plan
Contract management risks	Review existing contracts for - penalties if dealer does not provide services - if dealer has business continuity plan - if dealer respects the security of the data or information disclosed to him from your organisation - lack of penalties
Insurance management and coverage in place	Check if insurance contract exists to cover: disasters, loss of assets, loss of revenues, liabilities
Outsourcing management	Same as contract management plus service level agreements
Human error in operations	Document procedures Risk management of existing procedures
Labour dispute or strike	Clear engagement contract
Forgery	Check current authorisations assigned to employees Keep open communication with banks
Fraud	Frequent Review of accounting, balance of accounts that are payable-receivable Frequent reconciliation of accounts with customers, dealers, banks Internal or external auditing annually
Epidemic - pandemic flu	Prepare a pandemic plan Vaccinate field teams

Operational and Continuity Risks	
Risks	**Possible mitigation strategies and measures**
Succession (substitution) planning	Prepare a succession (substitution) plan
Water leak or plumbing failure	Prepare a business continuity plan Prepare an emergency response and evacuation plan Insurance coverage
Power outage – external and internal	Install UPS or generators
Heating, ventilation, air conditioning failure	Regularly service existing equipment Service contract with dealer
Machinery breakdown	Service and support contract with dealer
Loss or destruction of property	Insurance coverage Business continuity plan
Hazardous materials: chemical spill and contamination (related to nearby production, transportation, storage)	Prepare business continuity plan Prepare emergency response and evacuation plan Insurance coverage
Internal fire: severe, major, minor	Prepare business continuity plan Prepare emergency response and evacuation plan Insurance coverage
External fire: severe, major, minor	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage

Operational and Continuity Risks	
Risks	**Possible mitigation strategies and measures**
Dust storm	Prepare business continuity plan Prepare emergency response and evacuation plan Insurance coverage Maintenance of heating, ventilation, A/C systems
Earthquake: major or minor damage	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage
Flooding or drought	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage
Landslide	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage Follow up weather report Communicate with state authorities
Heat wave	Install or check maintenance of A/C systems Check alternative power supplies Prepare business continuity plan
Hurricane, typhoon, windstorm	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage Follow up weather report Communicate with state authorities
Snow or ice storm	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage Follow up weather report Communicate with state authorities
Volcano	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage

Operational and Continuity Risks	
Risks	**Possible mitigation strategies and measures**
Strong winds, hurricane, tornado	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage Follow up weather report Communicate with state authorities
Tides and tidal waves	Prepare business continuity plan Prepare emergency response and evacuation plan Review insurance coverage Follow up weather report Communicate with state authorities
Physical security and site access	List of personnel with door key copies Cameras and alarm systems Site risk assessment
Health and safety equipment and measures	Annually review expiration date of fire extinguishers Test health and safety equipment Train staff to use health and safety equipment Ensure that staff use personal protection equipment
Theft, burglary	Enhance physical security Check insurance coverage Install an intrusion alarm and CCTV system
Bomb threat	Enhance physical security Check insurance coverage Install an alarm and CCTV system Emergency response and evacuation plan
Kidnapping	Enhance physical security Check insurance coverage Emergency response and evacuation plan Install a CCTV System

Operational and Continuity Risks	
Risks	**Possible mitigation strategies and measures**
Terrorist attacks	Enhance physical security Check insurance coverage Install an alarm and CCTV system Emergency response and evacuation plan
Traffic or vehicle accidents	Train employees to drive safely Insurance and road assistance coverage Employee succession (substitution) planning
Rail, aviation and maritime accidents	Insurance coverage Employee succession (substitution) planning Prepare a safe travel guide for employees

Financial Risks	
Risks	**Possible mitigation strategies and measures**
Organisation capital	Review monthly results with finance manager or accountant Review cash flow and business planning
Supplier payments	Prepare a cash flow programme and monitor it on an ongoing basis Reconcile accounts often
Customer / members debt collection	Review accounts receivable every day or week Review collection progress on a daily basis Keep in frequent contact with members
Operating expenses management risks	Prepare an annual and monthly budget and follow it up with actual vs budgeted reporting Discuss deviations and deploy corrective actions when required
Capital expenditures	Prepare an annual and monthly budget and follow it up with actual vs budgeted reporting Discuss deviations and deploy corrective actions when required
Budget management	Prepare an annual and monthly budget and follow it up with actual vs budgeted reporting Discuss deviations and deploy corrective actions when required
Accounting and financial management	Request and review monthly and year-to-date reports every month
Taxation	Review accounting balance sheet at least once a month
Tax and social insurance payments	Review accounting balance sheet at least once a month Reconcile this with payroll system
Cash flow and liquidity	Prepare a cash flow programme and monitor it on an ongoing base
Access to credit: credibility	Communicate with bank, sponsors
Interest rates risk	Consult your bank often: review loan status
Currency risks	Consult your bank often Take political news into account

Financial Risks	
Risks	**Possible mitigation strategies and measures**
Cost estimation	Often review cost estimation of services with your accountant
Sales pricing structure (if relevant)	Often check costs and profit margins Use market research to compare your pricing with market information Discuss with customers to get feedback on the pricing of services
Profit margins (if relevant)	Often check costs and profit margins Use market research to compare your pricing with market information Discuss with customers to get feedback on the pricing of services

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Accidental deletion of data	Implement backup
Incorrect data entry	Implement backup Improve software controls to check for incorrect data entries Data reconciliation
Workstations or computers that do not require password access	Implement password and access control and policy
Insufficient or non-existent software licences	Check all organisation software licences. Have a list of legal software and the number of licences
Insufficient training of new or temporary employees / volunteers	Written procedure training plan for new employees / volunteers
Need to access critical file when employee is absent (locked in his computer)	Personnel succession (substitution) planning backup policy
Files lost or misplaced by users	Proper archiving system Use (scanned) electronic copies of documents

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Sending PC's for repair to third parties with their disks full of organisation data	Prepare an equipment removal procedure for all assets leaving organisation office area that requires authorisation
Lack of user and administrator documentation	Ask your software dealer for the user's manual
Application software failure (due to software or hardware problems, employee errors etc.)	Sign a support contract with the software dealer Implement backup
Central computer equipment failure	Sign a support contract with the software or hardware dealer Implement backup Prepare a business continuity plan
Communications failure (voice): problems with telephone centre or provider	Prepare alternative solutions (e.g. redirect to mobile, use mobile tethering)
Hardware malfunction	Sign a support contract with the hardware dealer Implement backup Prepare a business continuity plan
Power failures affecting information and data	Install UPS or generators
Equipment failure	Sign a support contract with the hardware dealer Implement backup Prepare a business continuity plan
New or upgraded software corrupting documents or files	Back data up Business continuity plan Sign a support contract with your software dealer
Software malfunction	Back data up Business continuity plan Sign a support contract with your software dealer
Software upgrades affecting availability of data or other programmes	Back data up Business continuity plan Sign a support contract with your software dealer

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Availability of files stored in PC directories and PC drive failure	Sign a support contract with the software or hardware dealer Implement backup for all PC's: use central storage for all files
Poor (no one is sure what is backed up) or no backup at all	Document backup plan (what is backed up, when, where etc.) Assign responsibility Check daily backup process successful completion Test by frequently restoring
Backup not verified	Assign backup responsibility Check correct backup completion daily Test by frequently restoring
Backup media never verified	Assign backup responsibility Check correct backup completion daily Test by frequently restoring
Backup is stored in the office	Ensure backup is transferred daily to a remote location
Faulty hardware	Sign a support contract with the hardware dealer Implement backup Prepare a business continuity plan
Faulty programming	Sign a support contract with the software dealer Implement backup Prepare a business continuity plan
Loss of availability of systems and equipment	Sign a support contract with the software or hardware dealer Implement backup Prepare a business continuity plan
Approval of unauthorised or fictitious transactions	Check authorisation (with banks, online system access etc.) Reconcile accounting and banking statements Implement a two-stage authorisation process (e.g. password plus USB) for online bank transactions
Access to information by cleaning staff in the evening	Implement a clear desk policy (no papers on desks at the end of the business day)

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Former employee access to premises or information	Prepare termination procedure to remove keys, PC's, email access etc. for ex-employees Implement an access control policy (to solve issues regarding office key copies and alarm codes)
Physical access in confidential or restricted areas by unauthorised people	Implement physical security measures (including intrusion alarms, CCTV etc.) Implement an access control policy (to solve issues regarding office key copies and alarm codes)
Physical disclosure of sensitive or privileged information	Install CCTV system Lock sensitive information in lockers Train employees
Physical intrusion by unauthorised people	Implement physical security measures (including intrusion alarms, CCTV etc.) Implement an access control policy (to solve issues regarding office key copies and alarm codes)
Poor security in the working area	Implement physical security measures (including intrusion alarms, CCTV etc.) Implement health and safety measures
Incorrect or inappropriate employee file access	Access control policy and procedures for users Procedure for granting access to file storage areas and systems

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Forgery of documents sent out for authorisation	Only allow access to critical documents and papers to a very limited number of people (lockers with keys) Access control policy for the IT system area where documents are stored Use sealed envelopes and courier services to send documents for authorisation to third parties
Fraudulent programming that impacts data integrity	Access control policy for programmers of software dealer Non-disclosure agreement with software dealers Document all software changes (including the reason, what was changed etc.)
Access of malicious internet sites	Install antivirus software Restrict web access to block risky sites Train employees
Hacking	Install antivirus software and a firewall Run a penetration test to improve security Train employees Use VPN services when using public networks Prepare an incident management plan Prepare a communication plan to deal with the incident Prepare a business continuity plan
Computer viruses	Install antivirus software Restrict web access to block risky sites Train employees
Disclosure of reports to unauthorised or unintended people	Implement access control Train your staff about information security Prepare an incident management plan Prepare a communication plan to deal with the incident
Denial of service attacks (against organisation website)	Install antivirus software and a firewall Run a penetration test to improve security Train employees
Email security	Implement access control policy Install antivirus software Train your staff about email security

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Employees sharing passwords	Change passwords frequently Train employees Access control policy that bans password exchange Impose penalties

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Sensitive information disclosed during casual conversations	Train employees
Internal theft of information	Documented access control procedure and policy Sign a non-disclosure agreement Change passwords frequently Classify information and encrypt or lock away sensitive information
Network sniffing	Install a firewall or antimalware software Use VPN services when using public networks Run a penetration test
Cyber attack	Install a firewall or antimalware software Run a penetration test Prepare an incident management plan Change passwords frequently Enforce the use of strong passwords
Exploitation of system usernames and default passwords	Run a penetration test Prepare an incident management plan Change passwords frequently Enforce the use of strong passwords
Confidential information exchanged between interoffice messengers and employees	Train employees Sign a non-disclosure agreement Install an information and document exchange or delivery protocol with third parties
Confidential information handled by interoffice messengers	Train employees Sign a non-disclosure agreement Install an information and document exchange or delivery protocol with third parties
Data stored off site not encrypted and compromised	Implement information security measures (access control, encryption etc.) Prepare an incident management plan Prepare a communication plan to deal with the incident Train employees
Firewall configured inadequately	Periodic audits and reviews of security set-ups with dealer Run a penetration test

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Identity theft (various forms: customer, supplier, employee, etc.)	Train employees Implement information security measures (access control, encryption etc.) Change passwords frequently Install a CCTV system
Information corrupted by a former employee	Documented access control procedure and policy Change passwords frequently Remove access privileges at the end of collaboration Sign an information disclosure contract with employees
Launch of unauthorised programmes by users causing major problems in the main systems	Implement information security measures (access control, encryption etc.) Limit user ability to install software on their PCs (only administrators allowed) Back your data up Business continuity plan Prepare an incident management plan
Attempts to vandalise or sabotage the network	Implement information security measures (access control, encryption etc.) Prepare an incident management plan Install network monitoring software Install a firewall
Sensitive information taken outside of the organisation	Implement information security measures (access control, encryption etc.) Prepare an incident management plan Prepare a communication plan to deal with the incident Train your staff about scenario analysis
Dealer or supplier support unavailable due to dealer failure	Prepare a continuity plan Request that the dealer has a continuity plan
Dependence on a single individual's knowledge of IT systems	Prepare written documentation Prepare succession (substitution) planning

Technology, IT and Information Security Risks	
Risks	**Possible mitigation strategies and measures**
Third party (dealer) that supports systems has access to confidential information	Documented access control procedure and policy Sign non-disclosure agreements Change passwords frequently Remove access privileges at the end of collaboration

Regulatory and Legal Risks	
Risks	**Possible mitigation strategies and measures**
Compliance with legal requirements (related to the specific business or services)	Assess status frequently Implement measures to comply Insurance coverage
Compliance with regulatory requirements (related to the specific business or services)	Assess status frequently Implement measures to comply
Health and safety compliance in the working area (firehoses, fire extinguishers, labels etc.)	Implement health and safety fully as required by the state and by good business practices
Contractual risks (contracts with customers and dealers)	Review all contracts to assess the obligations and provisions they cover
Negative court decision in pending trial	Prepare for negative scenario before trial
Fulfil state and tax requirements on time	Maintain a control process to monitor state and tax requirements Review accounting statements in light of fulfilling tax office obligations Have an annual audit by a third party
Changes in regulations and laws	Follow business news related to your sector Prepare a contingency plan and change of business plan

Human Resources Risks	
Risks	**Possible mitigation strategies and measures**
Availability of competent personnel in the organisation and in the market	Prepare succession (substitution) plan Outsource Frequent volunteer campaigns
Current personnel number	Check and enhance capacity planning
Current personnel competences	Assess current capabilities and implement training
Health and safety issues	Implement health and safety as required by the state
Workplace accidents	Implement health and safety as required by the state and by good business practices
Travel safety	Prepare and distribute safe travel instructions to all staff in training Insurance coverage
Maternity leave	Prepare succession (substitution) plan
Loss of key staff (due to illness, resignation etc.)	Prepare a succession (substitution) plan Document processes and procedures Discuss with employees
Employment practices are inadequate or unclear	Document and implement a code of conduct
Employee dishonesty	Check backgrounds before hiring Confront the employee: let them know directly Impose consequences: terminate their contract Monitor closely
Missing succession (substitution) planning (who can replace any employees that are unavailable)	Prepare succession (substitution) plan
Accidents at workplace	Implement health and safety fully as required by the state and by good business practices Run a root-cause analysis for accidents

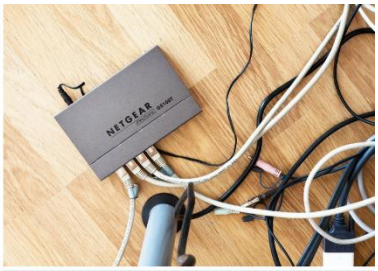
Human Resources Risks	
Risks	**Possible mitigation strategies and measures**
Workplace violence	Define and communicate a clear code of conduct, for example 'zero-tolerance' of moral harassment and other types of workplace violence Set up effective lines of communication Do not allow conflicts to escalate into harassment
Lack of training for organisation IT systems	Prepare and implement training for all staff Repeat this for all new employees
Lack of safety training	Prepare and implement training for all staff Repeat this for all new employees
Lack of training to organisation procedures and processes	Prepare and implement training for all staff Repeat this for all new employees
Pandemic flu	Prepare a pandemic plan
Non-adherence to safety practices	Prepare and implement training for all staff Repeat this for all new employees Define penalties for non-compliance
Resignation, termination, retirement	Prepare a succession (substitution) plan Document processes and procedures Discuss with employees
Strikes or labour unrest	Physical security plan Succession (substitution) plan Business continuity plan Insurance coverage
Poor morale or poor performance	Business plan Discuss with sponsors, beneficiaries Discuss with employees

Governance and Stakeholders Risks	
Risks	**Possible mitigation strategies and measures**
Organisation structure and chart	Prepare organisation chart
Clear roles and responsibilities for all staff	Document the roles and responsibilities of all staff
Management skills	Arrange or attend frequent management training sessions
Management competence	Arrange or attend frequent management training sessions
Authorisation process (including access to IT systems)	Prepare a documented process to assign authorisation (including IT access)
Poor management or micro management	Delegate and assign responsibilities
Office politics	Discourage office politics: prepare a code of conduct
Business values and principles lacking	Work with dealers to define and document them Make them known to employees: embed them in organisation life
Evaluation and management of suppliers and dealers	Evaluate current dealers in relation to the quality of their services and business continuity capability
Interests of employees	Compliance with legal and regulatory requirements in HR issues
Communication management with employees	Run an employee satisfaction survey
Customer management and communications (communication with and dependence on key customers)	Implement a communication plan to enhance customer relations Implement a satisfaction survey
Relationships with local community (and neighbourhood)	Implement a communication plan to enhance community relations

18.3. Business continuity plan template

Attached as a separate MS-Word document.







Erasmus+

CASSANDRA
KEEP YOUR BUSINESS GOING