Guernsey Registry

CHARITY AND NPO RISK ASSESSMENT IN GUERNSEY AND ALDERNEY

Every charity and NPO ("organisation") is required to carry out risk assessments. The aim is to ensure that all the Managing Officers are aware and informed of the organisation's risks and where appropriate reduce or manage those risks to a level that the organisation is comfortable with (risk appetite). Risk management is the process of identifying, evaluating and controlling risks.

The Managing Officers (and maybe any other organisation personnel that understand the organisation well) need to work together in a constructive and open manner to review the organisation's purpose, strategy, objectives and its activities, identifying potential risks and agreeing, wherever necessary, an appropriate cause of action. The aim is not to eliminate risks, and some may even present positive opportunities.

This guidance document provides a suggested framework and simplified process of risk management. For those organisations that may have a more evolved or sophisticated risk management framework, they should continue to use it.

Alternative risk management frameworks and risk assessment grids along with comprehensive guidance and examples of risk mitigation can be found online here:

https://www.gov.uk/government/publications/charities-and-risk-management-cc26/charities-and-risk-management-cc26#a-risk-management-model

This risk management framework and process is made up of three steps:

1. **Identification** – Think about all the things that might stop you achieving your strategy, your objectives or the undertaking of your activities. Your discussion will include financial transactions, administrative activities, interactions with people, and interactions with other organisations.
2. **Evaluation** – Analysing the risks to assess and measure the likelihood of the risk happening and the impact on the organisation if it does. The risk register template we provide enables you to articulate the consequences and derive an initial score, a risk appetite (your policy), and the residual score after considering how good your current controls are.
3. **Control** – Deciding how you will maximise and protect positive outcomes whilst also determining and prioritising what actions you might take to manage the downside (negative/ damaging outcomes) of any risk. Courses of action will be accepting, managing (tolerate, reduce, control, share, transfer), or avoidance. A record of your decisions should be maintained, and the risk register template we provide can facilitate this.

INDENTIFICATION (step 1 of 3)

The first step is to identify possible risks in all the different parts and across all aspects of your organisation's work. We encourage you to consider the following 5 categories:

- Compliance (risk of failing to comply with legislation and reporting).
- Financial (risks to your finances, financial movements, reserves and assets).
- Governance (risks in capability and how your organisation is managed and directed).
- Operational (risk in ability to undertake the tasks, activities, and utilisation of tools to achieve objectives).
- External (risks deriving from government influence, your reputation, and the environment in which you operate).

The above categories are used in the risk register template we provide. In **Appendix 3** we have provided you with further explanation and example risk areas to consider for each the five categories listed above (it is not exhaustive). There can be a range of risk possibilities within each category (what might not go as planned ie what will stop you?) and you should explore both positive and negative outcomes.

For any areas of risk pertinent to your organisation's activities and objectives, you should record the specific risks you have identified.

EVALUATION (step 2 of 3)

Evaluation takes the form of assessment, prioritisation, and risk appetite.

Assessment (Scoring)

Once a risk has been identified, you need to assess (as a rating from 1 to 5):

- the likelihood of the risk happening
- the impact of the risk on the organisation if it happens.

The risk register template we provide will assist you with this where you will first determine an Initial Risk Score (and later on a target risk/ appetite score and then a residual risk score). In **Appendix 1** we have provided you with matrices on how you can rate and score your risks when assessing likelihood and impact.

When assessing the impact of a risk, consider all the possible implications, some of which might not be obvious. For example, one of the risks may be that you're unable to articulate/ promote the benefits of your work.

- A consequence of this could be a reduction in awareness and therefore funding.
- A less obvious consequence may be that your organisation's personnel/ volunteers become disheartened or lose focus because they can't see the difference they're making.

Examples of risk mitigation can be found in the risk register template.

Types of consequences that may impact your organisation can include:

- Financial (loss of money through fraud)
- Safety/ safeguarding (the health or injury of people)
- Property (the damage to equipment and assets)
- Processes (the availability of systems from a cyber-attack)
- Reputational (inappropriate actions cause loss of public confidence)
- Regulatory (censure from failure to comply)

Thinking about this collectively as Managing Officers and maybe with any other personnel that understand the organisation well, is a valuable exercise.

Prioritisation

You can't manage every risk, so use the initial risk rating score to prioritise what you should first focus on.

It's useful to determine a cut-off point, above which you'll manage the risk and below which you won't. For example, you may decide to manage only the top five or 10 risks, or risks that score six points or more.

The cut-off point will partly depend on how much time you have to manage the risks. It's better to manage the most serious risks properly than to manage a full list weakly.

Determine your risk appetite

You need to understand how much risk your organisation is willing to accept in pursuing its objectives and activities.

Risk appetite boundaries may already be set through existing policy (for example the activities you are willing and able to do and those you cannot or will not undertake). A discussion of risk appetite may also aid your organisation in setting policy.

Your risk appetite might change depending on the activity. For example, an organisation that provides aid in a war zone and uses organisation shops to fund this work might have a low risk appetite for health and safety in its shops, but a high risk appetite for safety in the war zone.

Look at the risks (eg a top 10) that you have either prioritised or chosen to manage and discuss further and determine your risk appetite for each (ie determine a target risk

score). Discuss this with the individuals who will own and be responsible for the risk ("risk owner"). The aim is to get the residual risk (the risk that remains after you have considered your controls in place) to a level in line with the risk appetite (ie your target risk score).

CONTROL (step 3 of 3)

Control takes the form of management, assurance, and review

Management

The aim is to manage the level of each risk identified and ensure it is controlled to a level that the organisation is happy with ie within its appetite.

To do this, collective discussion is needed to determine a risk response. Your response will be one of the following: Accept; Monitor and Tolerate; Reduce (control/ mitigate); Share or Transfer; Avoidance. These responses are explained in **Appendix 2,** where you will also find a governance grid to guide you in your discussion and determination of a response based on the risk score level that has been evaluated.

The Managing Officers should work with the risk owner to think about all the controls the organisation has in place to reduce its likelihood or impact. For example, if the risk is fraud, the controls must include anti-fraud measures.

Once you've listed all the controls that you have in place for a risk, you can re-score its likelihood and impact to get a residual risk score based on how effective the controls are.

Think about whether this residual risk is:

- at an acceptable level (eg the same level as your appetite/ target risk score).
- too high, which means you'll need to identify additional actions to reduce the risk further (eg putting in place more controls, improving existing controls, stopping the activity, or insuring against or contracting out the risk) – this will give you an action plan that can be reviewed; or
- too low, (are you inhibiting opportunities with too many controls?); you might consider stopping or reducing some control, or perhaps exploiting further.

Assurance

Once the key risks have been identified, assessed and are subject to controls, it is important to make sure that these controls are being performed as expected and remain effective.

You can ask the risk owner to confirm at appropriate intervals that they've checked the controls and that they're working as planned, and to give evidence to support this.

If you have a team within your own organisation that undertakes independent and objective evaluations of its activities (internal audit), then you can also ask them to give assurance that the relevant controls are working; or alternatively ask your external auditors or other professionals to do this.

If the risk register template provided is used, you will have listed the controls that are currently in place. Their continued effectiveness will determine or redetermine a residual risk score.

Review

Once you have completed your Risk Register, you need to decide how you'll monitor and review this going forward.

The Risk management process does not stop once you have identified your key risks and decided how to deal with them. You will need to come back to it again later as your risks and plans will change and need to be adjusted to take account of changing circumstances.

Risks may come and go, or their likelihood or potential impact could change, so you may need to change the way you deal with them. It's a good idea to tie this monitor and review process into your strategic and operational planning.

Review your risk register at least once a year (perhaps more often for particular large or complex projects/ risks) and whenever there are incidents that suggest the controls you have in place aren't working well. You may wish to align any risk review with the statutory need to review Anti-Financial Crime policy.

Larger organisations may also ask that all papers which go to regular meetings include a summary of the main risks and the status of implementation of suggested mitigation.

It can be useful for the Managing Officers to pick a risk (or area of risks) to do an in-depth review of it at one of their regular meetings. This gives the Managing Officers a continual understanding of the status of their risks and controls and helps assure them that risk is being managed effectively.

APPENDIX 1

EVALUATION

The risk register template provided uses a 5 x 5 rating (likelihood x impact) which is a standard widely used by many organisations. The following table shows the ratings used in the risk register template:

Rating	Likelihood	Frequency narrative
1	Rare	Implausible - not likely to happen or could only happen in exceptional circumstances.
2	Unlikely	Improbable - not expected to happen, but there is a remote possibility that it could occur.
3	Possible	Plausible – could occur but unable to predict any frequency.
4	**Likely**	Could happen on more occasions than not but cannot be accurately predicted.
5	**Certain**	Probable in most cases, but without 100% certainty.

Rating	Impact	Effect narrative
1	Insignificant	(Negligible or trivial). One or more of the following: no impact on service, no impact on reputation, complaint unlikely, risk of litigation remote.
2	Minor	(Small but noticeable). One or more of the following: slight impact on service, slight impact on reputation, complaint possible, litigation possible.

3	Moderate	(Evident and material). One or more of the following: some service disruption, beneficiary dissatisfaction, potential for adverse publicity (avoidable with careful handling), complaint probable, litigation probable.
4	**Significant**	(Serious and major). One or more of the following: service disrupted or seriously limited, adverse publicity unavoidable (local media), complaint and/or litigation likely. Deficiencies must be addressed to recover and rebuild.
5	**Critical**	(Catastrophic). One or more of the following: loss of service for a significant time, irrecoverable adverse publicity (national media), harmful litigation expected, resignation of management, widespread and long-term loss of beneficiary confidence.

You should give each risk a rating for likelihood and impact.

Calculating the risk score

The initial risk score is calculated by multiplying the likelihood rating by the impact rating. For example, a risk with a likelihood of 2 and an impact of 3 would have a score of 6 (2 x 3).

This is an outcome grid for this scoring method:

RISK OUTCOME SCORING						
		LIKELIHOOD				
		1	2	3	4	5
IMPACT	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Two alternative calculations reflect the impact of a risk being more important than the likelihood and so deserve more weighting. If you wish to adopt these please adjust the scoring grids accordingly:

- Likelihood x impact + impact = risk score
- Likelihood x impact + (2 x impact) = risk score

APPENDIX 2

CONTROL GOVERNANCE

This grid will assist you in your discussion and determination before reaching any conclusion or decision.

Risk Score	Guidance	Potential Action	Action Narrative
1-4	**Low Risk** – To be managed at activity level without action.	Accept	Accepted business practice OR Exploit by increasing risk to pursue opportunity.
5-8	**Low Risk** – Monitor at activity level and be further reviewed.	Monitor/ Tolerate	Tolerated business OR Exploit by increasing risk to pursue opportunity with additional controls.
9-12	**Medium risk** - Management action required to control risk.	Reduce/ Treat/ Mitigate	Containment with controls. Change the likelihood (cause/ source) or manage impact consequences.
15-16	**Medium risk** - Management action to address the risk.	Share/ Transfer	Pass risk to third party(ies) to bear or share; or contingent to enact should risk happen.
17+	**High Risk** - Managing Officers action/ intervention required.	Avoid	Terminate by deciding not to start (or continue) activity giving rise to risk.

Accept – The Managing Officers may decide that the risk does not require any action or change. It may also be the case that the risk may no longer be relevant to the objectives and activities of the organisation.

Monitor and Tolerate. The Managing Officers may decide that no immediate action is required but the risk cause (source) should be monitored so that it can be reviewed (with a determined frequency).

Reduce: This is when the organisation should introduce controls into its activities, processes and procedures to control and mitigate (treat) a risk. This may include cross checking, training, team changes etc. to reduce the likelihood of the occurrence. The impact can also be managed and mitigated through controls such as additional reconciliation and reporting or further reactive direction such as crisis management and business continuity planning.

Additional activities such as audits, feedback and surveys can provide assurance around the effectiveness of your current controls.

Share or Transfer: the risk will still exist, and the organisation will remain exposed to this risk, but the Managing Officers must enact contingencies and may decide to take out insurance or to enter into an agreement with a third party to transferring the entire activity and protect the organisation against the negative impact of the occurrence.

Avoidance: depending on the impact and likelihood the Managing Officers may decide to avoid the occurrence entirely by taking action to terminate the activity which may cause the risk. This may mean discontinuing an entire objective in its current form (eg running a loss-making café or shop as your sole income).

APPENDIX 3

IDENTIFICATION

This is a series of questions covering several risk areas which are designed to help charities and NPO's identify the particular risks to which they may be exposed. This illustrates the type of risks that may be faced but should not be used as a checklist. The questions have been classified under the five aforementioned categories (Governance, Operational, Financial, External, and Compliance):

Governance Risk

Ability to manage and meet the organisation objectives consistently and efficiently for the best possible community outcome.

- What is the strategy? Is it in line with the organisation's purpose? Are there planned objectives and activities that are consistent with achieving the strategy? Is this well communicated and understood? How are the activities to achieve those objectives being monitored, reported, and adapted?
- Is there an effective managing body/ organisational structure? (Performance, skills, and commitment).
- Does the organisation have sufficient people and skills to meets its objectives? Are the Managing Officers working efficiently and effectively as a team and do the individuals feel that they are able to contribute to the direction and management of the organisation in a satisfactory manner resulting in positive outcomes? Is too much control held by too few for too long to the detriment of the future operations and reputation of the organisation?

- Who benefits from the organisation? Who is paid by the organisation or receives reputational, lifestyle or material benefits? Are benefits in line with the objectives, transparent, understood and acceptable?
- How do you manage a conflict of interest?
- Is there a limitation in the governing document – does it do what you need to do to make the difference you want to make (aims, achievements, and activities). How will you avoid a breach of constitution?
- Does the organisation undertake activities that are not directly in line with its purpose and objectives? If so what do these cost, in terms of money, time and reputation, and are they detracting from the core purpose? Is there mission creep or a reduction in the charities and NPO's ability to meet its purpose? Are the funders aware of these subsidiary activities and are all restricted donations ringfenced and used in accordance with the donation terms?
- What is the organisation's relationship with its donors and how is this monitored, recorded and evaluated? Do the donors have any influence on the organisations activities and is this acceptable. Do the donors receive public recognition and how is this managed? Does the organisation enter into verbal or implied or written agreements with any of its donors?
- Are there any key personal whose skills and knowledge the charities and NPO's ongoing operations are dependent upon?
- How do the Managing Officers know about the activities, finances, and reputation of the organisation in order to carry out their duties and responsibilities?

Operational Risk

Ability to continue to operate safely in order to satisfactorily meet immediate demands, respond efficiently to changes in demands and supplies, and to future proof the service to meet forecast demands or to responsibly complete projects. Is the organisation set up and run in a way that allows success?

- What operational third-party relationships does the organisation have? Are they in writing and what are the risks relating to these contracts (implied, verbal or written)?
- How is the organisation's impact measured and communicated? Does the organisation collect feedback or impact reports from its beneficiaries? Is beneficiary welfare and safety considered? How can beneficiaries complain? How does the organisation respond to feedback? What is the process to bring about improvements in services/ funding?
- Is the organisation set up and run in a way that allows success?
- Who are the organisation's suppliers? Are they bona-fide, reputable, essential and dependable? Is there poor contract pricing? What happens if they cannot deliver?
- Does the organisation have the necessary capacity, skills, premises, funding and/or equipment to carry out its plans and meet its objectives? How will you respond to an unforeseen rise in demand for your services? Is the organisation confident it is aware of all factors and making the most of all opportunities in line with its objectives?
- How is the organisation funded? Is there sufficient and reliable income? Is the source of income compliant with regulations and your financial crime policies? Are the fundraising activities of the organisation effective and cost efficient? An article by Civil Society News in 2016 quoted a survey that found that respondent's ideal organisation would spend no more than 14% on costs

including fundraising. https://www.civilsociety.co.uk/news/-ideal-organisation-would-spend-42-per-cent-of-income-on-campaigning-fundraising-and-running-costs-.html#:~:text=The%20study%20shows%20that%2C%20on,including%20fundraising%20and%20staff%20costs.

- Does the organisation employ any paid staff? How are they trained, supported, reviewed and motivated? What is the staff retention? What is the sick leave policy and how is this funded and managed to limit impact on the organisation's operations? Do you have the right staff with the right capabilities? Are they in the right roles?
- Does the organisation have a sufficient number (making the best use) of staff/ volunteers and what is the moral of the organisation's team? Are there any recruitment plans and are they effective in attracting the right competences? What is being done to look after and retain your volunteers?
- What is the team training and how is it funded, assessed and recorded? Is there a safeguarding policy and are the team aware and is their training up to date? Do you have the right organisational culture? Do staff/ volunteers have the tools they need to be successful? Do they communicate in the right way and use effective processes? Is the team welcoming and inclusive to new members, staff, and volunteers? Are the team aware of the possible impact the charity is having on the community and do they feel a sense of shared achievement?
- Are there any health, safety and environment issues to consider for the protection of the team and beneficiaries? Does the organisation run any events and are risk assessments carried out for activities? Can the organisation comply with its safeguarding policy?
- What data (paperwork and digital records, documents and other media) does the organisation hold? Where is it kept, for how long and is it secure? Is insurance required? Is the data GDPR compliant and is the organisation registered with the

DPA? Are the written contracts and financial records kept for six years, secure and retrievable as may be required by law?

- What are the operational systems of the organisation? What IT systems does it rely on and how are they updated, maintained, assessed and improved? How are the IT systems backed up and who is responsible for this?
- Do any other organisations provide the same or similar benefits or have the same or similar objectives? If so, what is the relationship with these organisations and how is the organisation best positioned to act socially responsibly and for the betterment of its beneficiaries? Have we considered collaborating with other charities?
- What assets/ property does the Organisation own? Is the organisation making the best use of their assets/ property? Are there regulations and legal requirements relating to the use of these assets? Is security required? Are they essential, maintained, secure, safe, and insured. What is their lifespan, will they need replacing and if so, are there plans and funds in place?

Financial Risk

Ability to maximise funds for the greatest positive impact on the organisation's objectives, with good planning, demonstrating good stewardship, adhering to donors wishes/ restrictions, avoiding exposure to financial loss, misappropriation, or wrongful application of funds (such as through fraud, money laundering, bribery, corruption and terrorist financing).

Are there risks to your finances that might stop you from achieving your objectives (for example, are you dependent on one source of income or are your reserves low)?

- How are payments made to ensure they are the right amount, to the right person for the correct agreed use? What records are kept to evidence this? How do you manage the increased risk of fraud when transferring money to a country that has few regulations or financial checks?
- How is income received, from whom, and is it trustworthy? How is it kept secure, recorded accurately, used wisely and in accordance with any donor terms? Are any donations tied to conditions and therefore appropriately ringfenced?
- Are you making the best use of the financial benefits as an organisation. Tax relief, governmental help – for example: awareness and use of CH1 and CH2 forms in Guernsey and Alderney.
- Is the organisation holding onto assets (including funds) in excess of working capital and are there plans to ensure the good use of these assets in line with the organisation's purpose? Is the organisation making the most of its income and assets and are they exposed to unsatisfactory financial risk, how is this managed and are authorities and donors aware of the circumstances? ie currency, location, investments, contracts etc
- Do you have adequate asset (property, equipment, investment etc…) management policies? Do fluctuations in asset values matter? Are you satisfied with your current and future investment policy? Are you satisfied with your current maintenance and future replacement programme?
- Do you have adequate insurance cover – tangible assets, operational activities, indemnity, liability, obligations, and duties.
- The future of contracts - Have we reviewed our contractual commitments? Have we reviewed any contracts to deliver public services?
- Is there accurate and sufficient financial information? Is the organisation financially viable? Does the organisation have budgets? Are they reported with comparisons to actual, and how effective are the budgets? Are they used for

decision making and is there any cash flow forecasting? Has the organisation had to delay paying suppliers or make beneficiary payments?

- How is the income split across sources of income? Is the organisation dependent on one or a few sources of income and how reliable are they?
- Is there a Donors register, and is it up to date?
- Does the organisation charge for its services and who pays this fee? Is it a third-party subsidy? Is there a debt collection issue and how often are prices reviewed? If the services are free should there be a charge?
- Does the organisation have any borrowing or made any guarantees?
- Does the organisation hold or make payments or receive donations in a foreign currency?
- Does the organisation ask suppliers for quotes? Is there a competitive element to the use of suppliers?
- Does the organisation have pension commitments?
- Does the organisation have any investments and if so, how are they managed responsibility and safely?
- Are there adequate safeguards in place to prevent fraud (including segregation of duties, authorisation and 4/6 eyes checks? Risk of fraud increases where transactions may include parties outside of Guernsey and Alderney and checks are more difficult.
- What is the organisation's Reserve(s) policy - retention and use?
- Inadequate reserves and cash flow. Are there risks to your finances that might stop your services or achieving your objectives (for example, are you dependent on one source of income, benefactor or general public). Does the organisation produce cashflow forecasts to ensure it can meet current and budgeted liabilities?

External Risk

Ability to build and maintain a good public reputation and behave in an ecologically and socially responsible manner. Having the foresight to manage environmental factors – political and geographical.

- Does the organisation produce an impact report? How does the public find out about the organisation's services as a beneficiary, volunteer, potential-employee, donor or authority?
- Do you have the influence and reputation that you need? What are the risks to this reputation (eg negative publicity caused by poor service or working practices)? How is the reputation of the organisation measured and manged?
- Does the organisation communicate with the public? Does it advertise, use social media or use PR, what does this cost and how effective is it? How is negative publicity managed and does the organisation have an appointed and trained press officer or plan of how to respond to media enquiries?
- Does the organisation have sponsorship agreements (implied, verbal or written), and if so, how is this assessed and how does the organisation ensure it meets its contractual obligations and manage the reputational impact? Note: The Charities and NPO's Ordinance and Regulations require those organisations to have contracts in writing when they are significant in value or worth £5,000 or more.
- Does the organisation have an equality policy and are the team aware and trained? Are the organisation's services accessible to all abilities and backgrounds?
- Changing government policy - What future changes to government policy might affect your ability to achieve your objectives?
- What effect is the current economic climate having on our organisation and its activities? How are you affected by a turbulent economic or political environment?

- What government policies impact on the organisation's purpose/ objectives and how is the organisation engaging with these? ie volunteering, commissioning, social and tax policies.

Compliance Risk

Ability to comply with legislative, regulatory, registry and tax requirements. To be able to meet any time scales and deadlines in an accurate transparent and efficient manner to avoid both reputational damage and financial damage.

In particular, the law requires charities and NPO's to ensure they have addressed financial crime risks (fraud, money laundering, bribery, corruption and terrorist financing, proliferation of weapons of mass destruction). Please see the Anti-financial Crime Policy Guidance Document for additional explanation of this.

- Are the Managing Officers aware of their responsibilities and have all the information, resources and competence needed to comply?
- Are there adequate controls in place to comply with the Organisation Laws and regulations including reporting - which might result in both reputational damage and financial damage?
- What actions/ reporting is the organisation required to make and what additional reporting would the organisation benefit from making?
- Does the organisation need professional services and if so, what for and what is the plan and policy? Should the organisation have a contract?
- Does the organisation have an international partner or/ and affiliation? These should have agreements in writing – where are these kept (they need to be recoverable, secure and kept for 6 years), what are the obligations, how are these met and when and how will the agreement be assessed and reviewed?

- Poor knowledge of regulatory requirements to conduct particular activities (eg public fund-raising, running of care facilities, operating vehicles, employment).
- Are there adequate controls in place to enable the organisation to comply with anti-money laundering, and other financial crime legislation including bribery, corruption and terrorist financing? The risk is increased when transferring money outside of Guernsey and Alderney. Other countries can have fewer regulations or financial regulations and sufficient diligence may be more difficult to establish.
- Are there adequate controls in place to enable the organisation to comply with data protection legislation?