Risk management policy

Version control	Date and updates
Original	September 2019
Version 2	December 2020: no changes
Version 3	December 2021: no changes; next review December 2022

What is Risk Management?[1]

Risk is part of all our lives. As a society, we need to take risks to grow and develop. From energy to infrastructure, supply chains to airport security, hospitals to housing, effectively managed risks help societies achieve. In our fast-paced world, the risks we must manage evolve quickly. We need to make sure we manage risks so that we minimise their threats and maximise their potential.

Risk management involves understanding, analysing and addressing risk to make sure organisations achieve their objectives. So, it must be proportionate to the complexity and type of organisation involved. Enterprise Risk Management (ERM) is an integrated and joined up approach to managing risk across an organisation and its extended networks.

Types of risk[2]

Anything that could prevent your charity achieving its aims or carrying out its strategies is a risk. The types of risks your charity might face will depend on its size, funding and activities, among other factors. Some risks charities can face include:
- damage to its reputation
- receiving less funding or fewer public donations
- losing money through inappropriate investments
- change in the government's policy on a particular issue, affecting grants or contracts

Identify any potential risks that could prevent your charity from meeting the needs of its beneficiaries, and put processes in place to assess and manage those risks.

How to manage risks

You are not required by law to have a risk management process for your charity, nor to follow a particular method. But the Charity Commission strongly recommends that you have a clear risk management policy and process. This will help you identify and manage all types of risks, and embed risk management into your charity's work. The commission's detailed guidance on risk management sets out the basics of dealing with risks. It includes a risk management model made up of the following steps:
1. Establish a risk policy
2. Identify risks
3. Assess risks
4. Evaluate what action to take
5. Review, monitor and assess periodically

---

[1] https://www.theirm.org/the-risk-profession/risk-management.aspx
[2] Charity Commission: https://www.gov.uk/guidance/how-to-manage-risks-in-your-charity

The model includes a heat map grid – this is one way to assess the impact each risk could have on your charity. Your charity should have a structured approach to risk management that is appropriate for its size and complexity. Example approaches include:

- Risk assessment toolkit – KnowHow NonProfit
- Risk management standard – The Institute of Risk Management

When to report on risk management

By law, non-company charities with incomes of £500,000 or more (and charities with incomes above £250,000 plus assets worth more than £3.26 million) must include a risk management statement in their trustees' annual report. Company charities must report on their main risks and uncertainties in the directors' report (unless they are classed as a small company by law).

What to include in a risk management statement

Your risk management statement should include:

- an acknowledgement of the trustees' responsibility to identify, assess and manage risks
- an overview of your charity's process for identifying risks
- an indication that major risks have been reviewed or assessed
- confirmation of the systems and processes set up to manage risks

Larger charities or those with more complicated activities should provide a more detailed risk management statement.

BHIVA risk management strategy

1. Establish a risk policy
2. Identify risks
   2.1. Reduced income from pharmaceutical industry
   2.2. Cancellation of annual or autumn conference
   2.3. Cancellation of one-day course, such as General Medicine course
   2.4. Reduced income from membership fees
   2.5. Loss of Secretariat services
   2.6. Loss of website
   2.7. Loss of reputation of Association
   2.8. Loss of electronic information (members' database)
   2.9. Loss of electronic information (conference registration database)
   2.10. Loss of electronic information (registration database for other events)
3. Assess risks
4. Evaluate what action to take
5. Review, monitor and assess periodically

Risk area/risk identified	
	2.1 Reduced income from pharmaceutical industry
Likelihood of occurrence (score)	Probable (4)
Severity of impact (score)	Major (4)
Overall or 'gross' risk	High (20)
Control procedure	▪ Regular contact with pharma companies ▪ Sponsorship Rate Card set by trustees ▪ Quarterly reviews by trustees
Retained or 'net' risk	Medium
Monitoring process	▪ Feedback from Annual Sponsors Meeting ▪ Feedback from sponsors and exhibitors at conference ▪ Sponsorship updates reviewed quarterly by trustees ▪ Annual review of overall budget by Officers (6-monthly) ▪ Regular review of overall budget by trustees (quarterly)
Responsibility	Chair and Trustees
Further action required	Agenda item for each trustee meeting (quarterly)
Date of review	Quarterly
	2.2 Cancellation of annual or autumn conference
Likelihood of occurrence (score)	Possible (3)
Severity of impact (score)	Extreme/catastrophic (5)
Overall or 'gross' risk	High (20)

Risk area/risk identified

Control procedure	▪ Regular contact with conference venue and suppliers
Retained or 'net' risk	Medium
Monitoring process	▪ Regular review by Events Subcommittee ▪ Venue visits by Local Host and Secretariat
Responsibility	Events Subcommittee, Chair and Trustees
Further action required	Agenda item for each Events Subcommittee and trustee meetings (quarterly)
Date of review	Quarterly

2.3 Cancellation of one-day course, such as General Medicine course

Likelihood of occurrence (score)	Possible (3)
Severity of impact (score)	Major (4)
Overall or 'gross' risk	Major (16)
Control procedure	▪ Regular contact with study day venue and suppliers
Retained or 'net' risk	Medium
Monitoring process	▪ Regular review by Events Subcommittee ▪ Venue visits by Secretariat
Responsibility	Events Subcommittee, Chair and Trustees
Further action required	Agenda item for Events Subcommittee and trustee meetings (quarterly)
Date of review	Quarterly

2.4 Reduced income from membership fees

Likelihood of occurrence (score)	Probable (4)
Severity of impact (score)	Moderate (3)
Overall or 'gross' risk	Moderate (12)
Control procedure	▪ Useful membership benefits ▪ Set reasonable membership fees ▪ Quarterly review by trustees
Retained or 'net' risk	Moderate
Monitoring process	▪ Regular email contact with BHIVA members ▪ Regular review of membership benefits ▪ Feedback from members via questionnaires (biennially) ▪ Statistical reports to trustees (quarterly)
Responsibility	Honorary Secretary and Trustees
Further action required	Agenda item for each trustee meeting (quarterly)
Date of review	Quarterly

2.5 Loss of Secretariat services

Risk area/risk identified

Likelihood of occurrence (score)	Possible (3)
Severity of impact (score)	Moderate (3)
Overall or 'gross' risk	Moderate (12)
Control procedure	Regular meetings with secretariat 3 to 6 monthly review
Retained or 'net' risk	Moderate
Monitoring process	Regular contact with secretariat
Responsibility	Trustees and officers
Further action required	Agenda for each trustee meeting
Date of review	Quarterly

2.6 Loss of website

Likelihood of occurrence (score)	Unlikely (2)
Severity of impact (score)	Moderate (3)
Overall or 'gross' risk	Moderate (9)
Control procedure	Amazon Web services backup plan
Retained or 'net' risk	Low
Monitoring process	Notification by Amazon Web services
Responsibility	Netsynergy
Further action required	Agenda item for each Events Subcommittee and trustee meetings (quarterly)
Date of review	Quarterly

2.7 Loss of reputation of the Association

Likelihood of occurrence (score)	Possible (3)
Severity of impact (score)	Moderate (3)
Overall or 'gross' risk	Moderate (12)
Control procedure	Trustees declaration of interest; vet who speak for BHIVA, internal controls, SOPs
Retained or 'net' risk	Moderate
Monitoring process	Trustee meetings review
Responsibility	Trustees
Further action required	Agenda of trustee meeting
Date of review	quarterly

2.8 Loss of electronic information (members' database)

Likelihood of occurrence (score)	Unlikely (2)
Severity of impact (score)	Extremely Catastrophic (5)

Risk area/risk identified	
Overall or 'gross' risk	Major (15)
Control procedure	Weekly back ups
Retained or 'net' risk	Low
Monitoring process	Regular performance reports from Acumen ltd
Responsibility	Medivents (subcontracted to Acumen Ltd but Medivents retain responsibility)
Further action required	Agenda item for each Events Subcommittee and trustee meetings (quarterly)
Date of review	Quarterly

	2.9 Loss of electronic information (conference registration database)
Likelihood of occurrence (score)	Unlikely (2)
Severity of impact (score)	Major (4)
Overall or 'gross' risk	Moderate (12)
Control procedure	Weekly back ups
Retained or 'net' risk	Low
Monitoring process	Regular performance reports from Acumen ltd
Responsibility	Medivents (subcontracted to Acumen Ltd but Medivents retain responsibility)
Further action required	Agenda item for each Events Subcommittee and trustee meetings (quarterly)
Date of review	Quarterly

	2.10 Loss of electronic information (registration database for other events)
Likelihood of occurrence (score)	Unlikely (2)
Severity of impact (score)	Major (4)
Overall or 'gross' risk	Moderate (12)
Control procedure	Weekly back ups
Retained or 'net' risk	Low
Monitoring process	Regular performance reports from Acumen ltd
Responsibility	Medivents (subcontracted to Acumen Ltd but Medivents retain responsibility)
Further action required	Agenda item for each Events Subcommittee and trustee meetings (quarterly)
Date of review	Quarterly

Annex 1: Risk register template with examples of use[3]

Scale

Impact		Likelihood				
Extreme/Catastrophic	5	10	15	20	25	30
Major	4	8	12	16	20	24
Moderate	3	6	9	12	15	18
Minor	2	4	6	8	10	12
Insignificant	1	2	3	4	5	6
		1 Remote	2 Unlikely	3 Possible	4 Probable	5 Highly Probable

Example 1

Risk area/risk identified	Lack of return/diversity of investment portfolio
Likelihood of occurrence (score)	Probable (4)
Severity of impact (score)	Major (4)
Overall or 'gross' risk	High (20)
Control procedure	▪ Investment policy set by trustees ▪ Written instructions to FSA authorised investment adviser ▪ Quarterly reviews by trustees
Retained or 'net' risk	Medium
Monitoring process	Performance reports reviewed quarterly by trustees
Responsibility	Trustees and treasurer
Further action required	Quarterly agenda item for trustee meetings
Date of review	Quarterly

---

[3] Charity Commission of England and Wales, 'Charities and Risk Management', CC26

Example 2

Risk area/risk identified	Unsatisfactory fundraising
Likelihood of occurrence (score)	Probable (4)
Severity of impact (score)	Major (4)
Overall or 'gross' risk	High (20)
Control procedure	▪ Financial appraisal of new projects ▪ Benchmarking of returns achieved ▪ Budget reporting by fundraising activity
Retained or 'net' risk	Medium
Monitoring process	▪ Financial reporting by fundraising activity ▪ Quarterly reporting by fundraising manager to trustees/CEO
Responsibility	Fundraising manager/CEO
Further action required	▪ New initiatives to be approved by trustees unless included in current business plan ▪ Review of regulatory compliance of current methods
Date of review	▪ When appropriate ▪ Next trustee meeting

Annex 2: Examples of potential risk areas, their impact and mitigation[3]

The charitable sector is by its nature diverse. The nature of activities, funding base, reserves and structures will expose charities to differing areas of risk and levels of exposure. While the areas of risk identified below will deserve consideration by most charities, it is not an exhaustive list of all potential areas of risk and should not be a substitute for a charity undertaking its own processes for risk identification.

This list is intended to be an indication of some of the main areas of risk that may need to be considered by trustees. Illustrative examples of potential impact are given, as well as some illustrative examples of controls or action that might be taken to mitigate the risk or impact. Some risks will fall into more than one category. Although the list may be long, it is not exhaustive and there will be other risks that apply to a particular charity because of its own circumstances and activities.

The risks are classified as follows:

Potential risk	Potential impact	Steps to mitigate risk
Governance risks		
The charity lacks direction, strategy and forward planning	▪ the charity drifts with no clear objectives, priorities or plans ▪ issues are addressed piecemeal with no strategic reference ▪ needs of beneficiaries not fully addressed ▪ financial management difficulties ▪ loss of reputation	▪ create a strategic plan which sets out the key aims, objectives and policies ▪ create financial plans and budgets ▪ use job plans and targets ▪ monitor financial and operational performance ▪ get feedback from beneficiaries and funders
Trustee body lacks relevant skills or commitment	▪ charity becomes moribund or fails to achieve its purpose ▪ decisions are made bypassing the trustees	▪ review and agree skills required ▪ draw up competence framework and job descriptions ▪ implement trustee training and induction ▪ review and agree recruitment processes

Potential risk	Potential impact	Steps to mitigate risk
	▪ resentment or apathy amongst staff ▪ poor decision making reflected in poor value for money on service delivery	
Trustee body dominated by one or two individuals, or by connected individuals	▪ trustee body cannot operate effectively as strategic body ▪ decisions made outside of trustee body ▪ conflicts of interest ▪ pursuit of personal agenda ▪ culture of secrecy or deference ▪ arbitrary over-riding of control mechanisms	▪ consider the structure of the trustee body and its independence ▪ agree mechanisms to manage potential conflicts of interest ▪ review and agree recruitment and appointment processes in line with governing document ▪ agree procedural framework for meetings and recording decisions
Trustees are benefiting from charity (e.g. remuneration)	▪ poor reputation, morale and ethos ▪ adverse impact on overall control environment ▪ conflicts of interest ▪ possibility of regulatory action	▪ ensure legal authority for payment or benefit ▪ consider alternative staffing arrangements ▪ implement terms and procedures to authorise/approve expenses and payments ▪ agree procedures and methods to establish fair remuneration conducted separately from 'interested' trustee (remuneration committee/benchmarking exercise, etc.)
Conflicts of interest	▪ charity unable to pursue its own interests and agenda	▪ agree protocol for disclosure of potential conflicts of interest

Potential risk	Potential impact	Steps to mitigate risk
	▪ decisions may not be based on relevant considerations ▪ impact on reputation ▪ private benefit	▪ put in place procedures for standing down on certain decisions ▪ review recruitment and selection processes
Ineffective organisational structure	▪ lack of information flow and poor decision-making procedures ▪ remoteness from operational activities ▪ uncertainty as to roles and duties ▪ decisions made at inappropriate level or excessive bureaucracy	▪ use organisation chart to create a clear understanding of roles and duties ▪ delegation and monitoring should be consistent with good practice and constitutional or legal requirements ▪ review structure and the need for constitutional change
Activities potentially outside objects, powers or terms of gift (restricted funds)	▪ loss of funds available for beneficiary class ▪ liabilities to repay funders ▪ loss of funder confidence ▪ potential breach of trust and regulatory action ▪ loss of beneficiary confidence ▪ taxation implications (if non-qualifying expenditure)	▪ agree protocol for reviewing new projects to ensure consistency with objects, powers and terms of funding ▪ create financial systems to identify restricted funds and their application
Loss of key staff	▪ experience or skills lost ▪ operational impact on key	▪ succession planning ▪ document systems, plans and projects

Potential risk	Potential impact	Steps to mitigate risk
	• projects and priorities • loss of contact base and corporate knowledge	• implement training programmes • agree notice periods and handovers • review and agree recruitment processes
Reporting to trustees (accuracy, timeliness and relevance)	• inadequate information resulting in poor quality decision making • failure of trustees to fulfil their control functions • trustee body becomes remote and ill informed	• put in place proper strategic planning, objective setting and budgeting processes • timely and accurate project reporting • timely and accurate financial reporting • assess and review projects and authorisation procedures • have regular contact between trustees and senior staff and managers
Operational risks		
Contract risk	• onerous terms and conditions • liabilities for non-performance • non-compliance with charity's objects • unplanned subsidy of public provision	• create cost/project appraisal procedures • agree authorisation procedures • get professional advice on terms and conditions • put in place performance monitoring arrangements • consider insurable risks cover
Service provision - customer satisfaction	• beneficiary complaints • loss of fee income • loss of significant contracts or claims under contract • negligence claims • reputational risks	• agree quality control procedures • implement complaints procedures • benchmark services and implement complaints review procedures

Potential risk	Potential impact	Steps to mitigate risk
Project or service development	▪ compatibility with objects, plans and priorities ▪ funding and financial viability ▪ project viability ▪ skills availability	▪ appraise project, budgeting and costing procedures ▪ review authorisation procedures ▪ review monitoring and reporting procedures
Competition from similar organisations	▪ loss of contract income ▪ reduced fund-raising potential ▪ reduced public profile ▪ profitability of trading activities	▪ monitor and assess performance and quality of service ▪ review market and methods of service delivery ▪ agree fund-raising strategy ▪ ensure regular contact with funders ▪ monitor public awareness and profile of charity
Suppliers, dependency, bargaining power	▪ dependency on key supplier ▪ lack of supplier to meet key operational objectives ▪ non-competitive pricing/quotes ▪ insufficient buying power	▪ use competitive tendering for larger contracts ▪ put in place procedures for obtaining quotations ▪ authorised suppliers listing ▪ monitor quality/timeliness of provision ▪ use service level agreements ▪ consider use of buying consortia
Capacity and use of resources including tangible fixed assets	▪ under-utilised or lack of building/office space ▪ plant and equipment obsolescence impacting on operational performance ▪ mismatch between staff allocations and key objectives ▪ spare capacity not being utilised or	▪ agree building and plant inspection programme ▪ agree repair and maintenance programme ▪ agree capital expenditure budgets ▪ undertake efficiency review

Potential risk	Potential impact	Steps to mitigate risk
	turned to account	
Security of assets	▪ loss or damage ▪ theft of assets ▪ infringements of intellectual property rights	▪ review security arrangements ▪ create asset register and inspection programme ▪ agree facility management arrangements ▪ have safe custody arrangements for title documents and land registration ▪ manage use of patent and intellectual property ▪ review insurance cover
Fundraising	▪ unsatisfactory returns ▪ reputational risks of campaign or methods used ▪ actions of agents and commercial fund-raisers ▪ compliance with law and regulation	▪ implement appraisal, budgeting and authorisation procedures ▪ review regulatory compliance ▪ monitor the adequacy of financial returns achieved (benchmarking comparisons) ▪ stewardship reporting in annual report
Employment issues	▪ employment disputes ▪ health and safety issues ▪ claims for injury, stress, harassment, unfair dismissal ▪ equal opportunity and diversity issues ▪ adequacy of staff training ▪ child protection issues ▪ low morale ▪ abuse of vulnerable beneficiaries	▪ review recruitment processes ▪ agree reference and qualification checking procedures, job descriptions, contracts of employment, appraisals and feedback procedures ▪ implement job training and development ▪ implement health and safety training and monitoring ▪ be aware of employment law requirements ▪ implement staff vetting and legal requirements (e.g., DBS checks) ▪ agree a whistle-blowing policy

Potential risk	Potential impact	Steps to mitigate risk
High staff turnover	▪ loss of experience or key technical skills ▪ recruitment costs and lead time ▪ training costs ▪ operational impact on staff morale and service delivery	▪ review interview and assessment processes ▪ agree fair and open competition appointment for key posts ▪ agree job descriptions and performance appraisal and feedback systems ▪ conduct 'exit' interviews ▪ review rates of pay, training, working conditions, job satisfaction
Volunteers	▪ lack of competences, training and support ▪ poor service for beneficiaries ▪ inadequate vetting and reference procedures ▪ recruitment and dependency	▪ review and agree role, competencies ▪ review and agree vetting procedures ▪ review and agree training and supervision procedures ▪ agree development and motivation initiatives
Health, safety and environment	▪ staff injury ▪ product or service liability ▪ ability to operate (see Compliance risks) ▪ injury to beneficiaries and the public	▪ comply with law and regulation ▪ train staff and compliance officer ▪ put in place monitoring and reporting procedures
Disaster recovery and planning	▪ computer system failures or loss of data ▪ destruction of property, equipment, records through fire, flood or similar damage	▪ agree IT recovery plan ▪ implement data backup procedures and security measures ▪ review insurance cover ▪ create disaster recovery plan including alternative accommodation
Procedural and systems documentation	▪ lack of awareness of	▪ properly document policies and procedures

Potential risk	Potential impact	Steps to mitigate risk
	procedures and policies ▪ actions taken without proper authority	▪ audit and review of systems
Information technology	▪ systems fail to meet operational need ▪ failure to innovate or update systems ▪ loss/corruption of data e.g. donor base ▪ lack of technical support ▪ breach of data protection law	▪ appraise system needs and options ▪ appraise security and authorisation procedures ▪ implement measures to secure and protect data ▪ agree implementation and development procedures ▪ use service and support contracts ▪ create disaster recovery procedures ▪ consider outsourcing ▪ review insurance cover for any insurable loss
Financial risks		
Budgetary control and financial reporting	▪ budget does not match key objectives and priorities ▪ decisions made on inaccurate financial projections or reporting ▪ decisions made based on unreliable costing data or income projections ▪ inability to meet commitments or key objectives ▪ poor credit control ▪ poor cash flow and treasury management	▪ link budgets to business planning and objectives ▪ monitor and report in a timely and accurate way ▪ use proper costing procedures for product or service delivery ▪ ensure adequate skills base to produce and interpret budgetary and financial reports ▪ agree procedures to review and action budget/cash flow variances and monitor and control costs ▪ regularly review reserves and investments

Potential risk	Potential impact	Steps to mitigate risk
	▪ ability to function as going concern	
Reserves policies	▪ lack of funds or liquidity to respond to new needs or requirements ▪ inability to meet commitments or planned objectives ▪ reputational risks if policy cannot be justified	▪ link reserves policy to business plans, activities and identified financial and operating risk ▪ regularly review reserves policy and reserve levels
Cash flow sensitivities	▪ inability to meet commitments ▪ lack of liquidity to cover variance in costs ▪ impact on operational activities	▪ ensure adequate cash flow projections (prudence of assumptions) ▪ identify major sensitivities ▪ ensure adequate information flow from operational managers ▪ monitor arrangements and reporting
Dependency on income sources	▪ cash flow and budget impact of loss of income source	▪ identify major dependencies ▪ implement adequate reserves policy ▪ consider diversification plans
Pricing policy	▪ reliance on subsidy funding ▪ unplanned loss from pricing errors ▪ cash flow impact on other activities ▪ loss of contracts if uncompetitive ▪ affordability of services to beneficiary class	▪ ensure accurate costing of services and contracts ▪ compare with other service providers ▪ notify and agree price variations with funders ▪ monitor funder satisfaction ▪ develop pricing policy for activities including terms of settlement and discounts
Borrowing	▪ interest rate movements	▪ appraise future income streams to service the debt

Potential risk	Potential impact	Steps to mitigate risk
	▪ ability to meet repayment schedule ▪ security given over assets ▪ regulatory requirements	▪ appraise terms (rates available fixed, capped, variable, etc.) ▪ appraise return on borrowing ▪ use appropriate professional advice
Guarantees to third parties	▪ call made under guarantee ▪ lack of reserves or liquidity to meet call ▪ consistency with objects and priorities	▪ review approval and authority procedures ▪ agree procedures to ensure consistency with objects, plans and priorities ▪ ensure financial reporting of contingency and amendment to reserves policy
Foreign currency	▪ currency exchange losses ▪ uncertainty over project costs ▪ cash flow impact on operational activities	▪ ensure proper cash flow management and reserves policy ▪ use currency matching (cost to charity in home currency) ▪ consider forward contracts for operational needs (hedging)
Pension commitments	▪ under-funded defined benefit scheme ▪ impact on future cash flows ▪ failure to meet due dates of payment ▪ regulatory action or fines	▪ use actuarial valuations ▪ review pension scheme arrangements (e.g. money purchase schemes) ▪ review procedures for admission to scheme and controls over pension administration
Inappropriate or loss-making non-charitable trading activities	▪ resources withdrawn from key objectives ▪ resources and energy diverted from profitable fund-raising or core activities	▪ monitor and review business performance and return ▪ ensure adequacy of budgeting and financial reporting within the subsidiary or activity budget ▪ review and agree adequate authorisation procedures for any funding provided by charity (prudence, proper advice, investment criteria)

Potential risk	Potential impact	Steps to mitigate risk
	▪ regulatory action, and accountability ▪ reputational risk if publicised	▪ report funding and performance as part of charity's own financial reporting system ▪ appraise viability ▪ consider transfer of undertakings to separate subsidiary
Investment policies	▪ financial loss through inappropriate or speculative investment ▪ unforeseen severe adverse investment conditions ▪ financial loss through lack of investment advice, lack of diversity ▪ cash flow difficulties arising from lack of liquidity	▪ review and agree investment policy ▪ obtain proper investment advice or management ▪ consider diversity, prudence and liquidity criteria ▪ implement adequate reserves policy ▪ use regular performance monitoring
Protection of permanent endowment	▪ loss of future income stream or capital values ▪ buildings unfit for purpose ▪ income streams inappropriate to meet beneficiary needs	▪ review and agree investment policy ▪ obtain proper investment advice or management ▪ consider diversity, prudence and liquidity criteria ▪ use regular performance monitoring ▪ ensure maintenance and surveyor inspection of buildings ▪ review insurance needs
Compliance with donor-imposed restrictions	▪ funds applied outside restriction ▪ repayment of grant ▪ future relationship with donor and beneficiaries ▪ regulatory action	▪ implement systems to identify restricted receipts ▪ agree budget control, monitoring and reporting arrangements

Potential risk	Potential impact	Steps to mitigate risk
Fraud or error	• financial loss • reputational risk • loss of staff morale • regulatory action • impact on funding	• review financial control procedures • segregate duties • set authorisation limits • agree whistle-blowing anti-fraud policy • review security of assets • identify insurable risks
Counter party risk	• financial loss • disruption to activities or operations	• research counter party's financial sustainability • contractual agreement • consider staged payments • agree performance measures • monitor and review investments • establish monitoring and review arrangements where counter party is the charity's agent ('conduit funding' arrangements
Environmental or external factors		
Public perception	• impact on voluntary income • impact on use of services by beneficiaries • ability to access grants or contract funding	• communicate with supporters and beneficiaries • ensure good quality reporting of the charity's activities and financial situation • implement public relations training/procedures
Adverse publicity	• loss of donor confidence or funding • loss of influence • impact on morale of staff • loss of beneficiary confidence	• implement complaints procedures (both internal and external) • agree proper review procedures for complaints • agree a crisis management strategy for handling - including consistency of key messages and a nominated spokesperson
Relationship with funders	• deterioration in relationship may impact on funding and support available	• ensure regular contact and briefings to major funders • report fully on projects • meet funders' terms and conditions

Potential risk	Potential impact	Steps to mitigate risk
Demographic consideration	• impact of demographic distribution of donors or beneficiaries • increasing or decreasing beneficiary class • increasing or decreasing donor class	• profile donor base • profile and understand beneficiary needs • use actuarial analysis to establish future funding requirements
Government policy	• availability of contract and grant funding • impact of tax regime on voluntary giving • impact of general legislation or regulation on activities undertaken • role of voluntary sector	• monitor proposed legal and regulatory changes • consider membership of appropriate umbrella bodies
Compliance risk (law and regulation)		
Compliance with legislation and regulations appropriate to the activities, size and structure of the charity	• fines, penalties or censure from licensing or activity regulators • loss of licence to undertake particular activity (see operational risks) • employee or consumer action for negligence • reputational risks	• identify key legal and regulatory requirements • allocate responsibility for key compliance procedures • put in place compliance monitoring and reporting • prepare for compliance visits • obtain compliance reports from regulators (where appropriate) - auditors and staff to consider and action at appropriate level
Regulatory reporting requirements: Financial and other reporting	• regulatory action	• review and agree compliance procedures and

Policies: Risk management v.3 · 7 December 2021 · Page 22 of 22

Potential risk	Potential impact	Steps to mitigate risk
requirements will be dependent on how the charity is constituted and may also vary according to funding arrangements	• reputational risks • impact on funding	allocation of staff responsibilities
Taxation	• penalties, interest and 'back duty' assessments • loss of income e.g. failure to utilise gift aid arrangements • loss of mandatory or discretionary rate relief • failure to utilise tax exemptions and reliefs	• review PAYE compliance procedures • review VAT procedures • file timely tax returns • understand exemptions and reliefs available (direct tax and VAT) • take advice on employment status and contract terms and tax • implement budget and financial reporting identifying trading receipts, and tax recoveries
Professional advice	• lack of investment strategy or management • failure to optimise fiscal position • contract risks • failure to address compliance risks	• identify and ensure access to professional advice • identify issues where advice is required • conduct compliance reviews

British HIV Association (BHIVA) · Registered Charity number: 1170707 · VAT Registration No: 345 4780 82
Secretariat: Medivents Ltd, Spirella Building, Bridge Road, Letchworth Garden City, Hertfordshire SG6 4ET
T: +44 (0)1462 530070 · E: bhiva@bhiva.org · W: www.bhiva.org · @britishhivassoc