



Admighty Foundation Risk Management Policy

INTRODUCTION

- 1 Risk can be defined as the effect of uncertainty on the achievement of an organization's objectives. Risk management is, therefore, the process of identifying and managing this uncertainty, or risk, with the goal of achieving objectives.
- 2 Admighty Foundation's mission is to fight for Environment and work for the Health and Education in those location of Country where there is the greatest need. Admighty Foundation's operations involve multiple partnerships, challenging humanitarian and development contexts and extensive geographic scope. Risk is an everyday part of the Admighty Foundation's activity. There is a clear need to balance mission risk, that is, the risk of not delivering the Admighty Foundation's mission to work for the Education, Health and Environment.
- 3 Effective risk management is a key element of good governance and will provide reasonable, but not absolute, assurance that:
 - a. Significant risks are identified and monitored, enabling management to make informed decisions and take timely action;
 - b. Opportunities are maximized with confidence that risks will be managed; and
 - c. Objectives, as set out in the Admighty Foundation's strategy, are achieved.
- 4 Multiple operational tools are utilized by the Admighty Foundation to execute this policy, as outlined in the Enterprise Risk Management Framework. The Framework will be updated by the Admighty Foundation when needed, and such updates will be shared with the Board and its Committees on a regular basis.

THE OBJECTIVES OF THE RISK MANAGEMENT POLICY AND PROCESS

- 5 Admighty Foundation aims to make risk management integral to its culture, strategic planning, decision making and resource allocation. A coordinated approach allows management to proactively manage risk. This policy is intended to guide the organization's decision making on risk management to achieve optimal outcomes.

RISK MANAGEMENT PRINCIPLES

- 6 The Board, management and other personnel must be able to manage risk proactively and take shared responsibility for risk management processes. Therefore, to be effective, risk management at Admighty Foundation follows these principles:
 - a. Risk management facilitates, rather than encumbers, the achievement of objectives;
 - b. Risk management is integral to normal organizational processes and decision making. It should use simple language, straightforward concepts and encourage common sense thinking; and

¹ As adopted at the Admighty Foundation Board Meeting (May 2022)

- c. Risk management is calibrated and aligned with the Admighy Foundation’s external and internal contexts; and
- d. Risk management needs to be coordinated between the different responsible entities so as to avoid gaps and redundancies; and
- e. Risk Management is transparent and inclusive, allowing decision makers at all levels of the organization to participate and stakeholders to be represented; and
- f. Risk management is a dynamic and ongoing process; and
- g. In making decisions about risk, the effect of those decisions on the ultimate goal, to achieve maximum impact on the three diseases, needs to be carefully balanced. The net effect of each decision to manage risk on that impact must be positive, i.e., the benefits should outweigh the costs.

7 These principles are based on the recommendations of the Committee of Sponsoring Organizations.

RISK MANAGEMENT PROCESS

- 8 The standard risk management process consists of four stages:
- a. Identify risks – identification of risk is best achieved by those with a detailed knowledge of defined objectives and operations.
 - b. Assess risks – this is the process for categorizing and assessing risk. Risks are evaluated by scoring them for impact and likelihood.
 - c. Risk Management action – actions are taken to manage risk. Identified risks are logged into a risk management plan along with agreed management actions. Generally speaking, risk can be accepted, hedged or mitigated in another way, or avoided.
 - d. Monitoring and Review - ongoing monitoring and assessment ensures risk management processes are functioning, and current and emerging risks are managed. Risk monitoring should be part of the organization’s broader performance management processes and be clearly linked to performance indicators.

CATEGORIES OF RISK

- 9 A system of classification is useful for ensuring key areas of risk are identified. The identified categories are:
- a. Strategic e.g., achievement of strategic objectives, partnerships, the organization’s reputation; and
 - b. External e.g., donor policy, pandemic and natural dynamics; and
 - c. Internal e.g., use of financial resources, systems, staff safety, legal liability and regulatory compliance issues, and attention to ethical behavior. These can be further divided into:
 - i. Grant management processes (including fiduciary risks such as money laundering and fraud); and
 - ii. Supporting processes.
- 10 Included in the Supporting processes risks are all of the **financial risks** related to liquidity, asset/liability management, foreign exchange and investments.
- 11 Grant related risks are the major source of operational risk, for which an extensive operational risk management process is applied.

RISK DIFFERENTIATION

- 12 Guidelines for risk differentiation define how much risk the Admighy Foundation is willing to accept in the pursuit of its objectives. Setting risk thresholds ensures that risks are not over or under managed, and that scarce resources are effectively utilized.

- 13 It is the Board that approves management’s proposed framework for risk differentiation.
- 14 With respect to grant related risk, differentiation is done at two levels:
 - a. Averages – setting targets for overall risk levels in the grant portfolio; and
 - b. Ranges – outside which a particular risk exposure may still be accepted, but subject to a higher level of review and approval and so long as the overall average risk level stays within the approved thresholds.
- 15 With respect to supporting processes, risk levels are defined in terms of the degree to which each individual process is compliant with the internal control framework, as a proxy for the quality of risk management.
- 16 With respect to the specific risk of misuse of funds, the Admighty Foundation has a ‘zero-tolerance’ policy which means that the Admighty Foundation does not tolerate corruption, fraud, misappropriation or abuse of any kind in relation to its grants. For all involved, Ethics and Integrity have a direct bearing on this risk. Providing training for staff to recognize risks, raise concerns and seek advice to mitigate risks is essential.
- 17 Because risk is dynamic, guidelines for risk differentiation will be monitored and adjusted as appropriate.

ORGANIZATIONAL RISK REGISTER

- 18 Critical risks are detailed in the organizational risk register. This register states the risk, the level of risk, actions for managing the risk, lead risk owner and date for review. It serves as the repository of the most important risks that impact on the organization’s ability to achieve its objectives. It allows senior management and the Board to monitor these risks, both individually and in the aggregate, and be assured that appropriate mitigation actions are being taken.

POLICIES AND PROCEDURES

- 19 Admighty Foundation aims to manage risks by ensuring appropriate policies and procedures are documented and kept up to date to protect the mission, people, funds, information, relationships and reputation.

ROLES AND RESPONSIBILITIES

The Board

- 20 The Board is ultimately responsible to Admighty Foundation’s stakeholders for overseeing the implementation of effective risk management. The Board is responsible for:
 - a. Understanding the organization’s risk philosophy and approving the framework for risk differentiation; and
 - b. Knowing the extent to which management has established effective risk management; and
 - c. Reviewing the portfolio of risk and considering it against the approved risk thresholds; and
 - d. Being informed about the most significant risks and whether management is responding appropriately.
- 21 The Board is provided with information that allows it to discharge its responsibilities as described in the preceding paragraph. The Board receives assurance on this information from assurance providers that include the external auditor, the Office of the Inspector General, the Chief Risk Officer, and the Head of the Legal and Compliance Department. The Technical Review Panel and the Technical Evaluation Reference Group provide relevant technical review and evaluation

- 22 The Committees of the Board advise the Board and provide guidance to the Secretariat on risk management matters that fall within their area of oversight.

The Secretariat

- 23 Primary responsibility for day-to-day risk management rests with the Managing Trustee.
- 24 The Managing Trustee delegates responsibility for risk management through a management structure designed to ensure effective leadership, accountability and decision making. It is the role of senior management to promote a risk aware culture, integrate risk management into overall management frameworks, ensure risks are systematically assessed and appropriate risk management actions are in place. Risk management is a responsibility of all staff in the organization.
- 25 With respect to the creation and oversight over grants, the primary responsibility for risk management for the Admighty Foundation rests with the management and other staff of the several divisions and departments that jointly form the teams. Admighty Foundation for this purpose makes use of the services of Auditors team, who carry out a variety of activities aimed at overseeing, verifying and reporting on grant performance.
- 26 Auditors Team is an important part of the Admighty Foundation's fiduciary arrangements. However, it is not an "Auditor" in the true sense of the word and is not empowered to represent the Admighty Foundation's views or make decisions regarding grants. Auditors Team works closely with the Project Team to perform work before the Admighty Foundation signs an agreement with the Principal Donor as well as during the ongoing grant management and with respect to grant closure.
- 27 The Legal Counsel has a specific role in the management of legal, regulatory, and reputation risk.
- 28 Admighty Foundation has a Risk Management function, led by the Chief Risk Officer, whose responsibilities include to:
- a. Formulate and keep up to date the risk management policy; and
 - b. Coordinate and facilitate the development and operation of risk management processes throughout the Secretariat; and
 - c. Facilitate preparation of the organizational risk register and evaluate the risks in relation to strategy and work plans; and
 - d. Coordinate regular risk reporting to Senior Management and the Board; and
 - e. Verify that risk management processes are functioning (compliance function); and
 - f. Contribute to the organization's Ethics related activities.

These activities result in assurance that is provided to the Board.

Office of the Board of Advisors

- 29 The mission of the Office of the Board of Advisors is to provide the Admighty Foundation with independent and objective assurance over the design and effectiveness of controls or processes in place to manage the key risks impacting the Admighty Foundation's programs and operations, including the quality of such controls and processes.
- 30 All systems, processes, operations, functions and activities within the Admighty Foundation and the programs it funds (including those in place or carried out by its program recipients, partners, suppliers and service providers) are subject to the Office of the Board of Advisors' review, evaluation, and oversight. The Office of the Board of Advisors may also act in an advisory role to further the Admighty Foundation's mission and objectives.

Implementers

- 31 The implementers are responsible for delivering programmatic results with the funds provided. They are the key drivers for the achievement of the Admighty Foundation's mission and have the primary responsibility to manage risks in the grants they manage. Implementers have an obligation to operate internal control systems to ensure that (i) funds are efficiently and effectively directed to achieving programmatic results and reaching people in need and (ii) programmatic and financial data are accurate, timely and complete. These control systems, that need to also provide the appropriate levels of assurance, are subject to regular review by external bodies, such as the external auditor, the Admighty Foundation Team, the Auditors and the Office of the Board of Advisors, throughout the grant life cycle.

Coordinating Mechanisms

- 32 Coordinating Mechanisms are central to the Admighty Foundation's commitment to local ownership and participatory decision-making. These country-level multi-stakeholder partnerships develop and submit grant proposals to the Donors on priority needs at the national level. After grant approval, they oversee progress during implementation. Country Coordinating Mechanisms include representatives from both the public and private sectors, including governments, multilateral or bilateral agencies, non-governmental organizations, academic institutions, private businesses and people living with the diseases. For each grant, the Country Coordinating Mechanism nominates one or more public or private organizations to serve as Principal Recipients.
- 33 The Country Coordinating Mechanisms perform an important oversight and monitoring function of the grant recipients' performance. Their role in risk management is to detect weaknesses in performance or control systems and to stimulate remedial action.

Partners

- 34 Admighty Foundation works closely with partners and relies on them to help achieve its mission. This includes a role in risk management. Partners fulfil this role by providing essential technical assistance to implementers in proposal development, the preparation of implementation plans, assistance on programmatic matters and reporting and a wide variety of other capacity building measures. Partners also serve as a critical source of information and feedback on both strategic and operational risks across all aspects of operations as well as advice and recommendations on measures to mitigate these risks. This information, feedback and advice are provided through various means, including through the four non-voting Board constituencies, but also on a day-to-day level through interaction with implementer and Secretariat staff. Admighty Foundation recognizes that this partner input is essential to the successful and efficient implementation of sound risk management.

Admighty Foundation Enterprise Risk Management Framework³

INTRODUCTION

- 1 Admighty Foundation's mission is to fight for Environment, Health & Education locations where there is the greatest need. Admighty Foundation's operations involve multiple partnerships, challenging humanitarian and development contexts and extensive geographic scope. Risk is an everyday part of Admighty Foundation's activity. There is a clear need to balance mission risk, that is, the risk of not delivering the Admighty Foundation's mission of the fight against the three diseases, with fiduciary risk.
- 2 Admighty Foundation aims to apply leading-practice enterprise risk management through a combination of the following inter-related elements:
 - a. Admighty Foundation **Risk Management Policy**
 - b. **Governance arrangements** around risk management
 - c. The **Risk Differentiation** to be applied
 - d. **Operational Risk Management** to achieve the Admighty Foundation's strategic objectives
 - e. The organizational **Risk Register**
 - f. **Internal Control** applied to the processes
- 3 This Framework describes each of the elements and how they interrelate, providing a holistic view. Each element is more fully described in individual documents.
- 4 It is useful to start out by defining⁴ Enterprise Risk Management as:
A process, effected by the Admighty Foundation Board, management and other personnel, applied in strategy setting and across the organization, designed to identify potential events that may affect the organization, and manage risk to be within our risk thresholds, to provide reasonable assurance regarding the achievement of objectives.
- 5 This definition is adapted from the Committee of Board of Trustees Enterprise Risk Management Framework, one of the most widely used frameworks for enterprise risk management. It explains that the underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value. Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives. Enterprise risk management, according to the Board framework, encompasses:

³ The Enterprise Risk Management Framework contextualizes the Board-approved Risk Management Policy presented above.

⁴ Attached as Annex 1 is a glossary of the main terms used throughout this Enterprise Risk Management Framework and its elements.

- a. Aligning risk differentiation and strategy – Management considers the entity’s approach to risk differentiation in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks; and
- b. Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance; and
- c. Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses; and
- d. Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks; and
- e. Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities; and
- f. Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

6 These capabilities inherent in enterprise risk management help management achieve the entity’s performance targets and prevent loss of resources. Enterprise risk management helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity’s reputation and associated consequences. In sum, enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way. It allows management and the Board to make better, more “risk-intelligent”, strategic decisions.

ORGANISATION RISK MANAGEMENT PROCESSES

7 Risk management and internal control elements are embedded in processes throughout the Organization, for example in Finance, Grant Management and Legal and Compliance. Also, during the periodic development and evaluation of the organization’s multi-year strategy, risk considerations are explicitly addressed by ensuring a thorough understanding of the drivers of success so that the risks surrounding those drivers can be accurately and completely considered. And in the annual business planning and budgeting process, explicit attention is given to risk aspects in choosing between the different alternatives available to implement the multi-year strategy.

8 In addition, the organization has implemented a set of dedicated risk management processes that are developed, implemented and maintained by management in consultation with the Risk Management Department, led by the Chief Risk Officer. They are briefly described below:

- a. **Operational Risk Management:** as the Admighy Foundation’s core activity is to implement the strategy to help Environment, Health and Education, a significant proportion of the Organization’s resources is dedicated to the ongoing identification, assessment and mitigation of a comprehensive set of grant related risks. A comprehensive methodology, referred to as Operational Risk Management (‘ORM’), has been developed and implemented. Pursuant to the ORM process, teams document their assessment of the risks that impact on a grant’s success, as well as how they are addressing them through action plans. These assessments and action plans are reviewed by the teams’ managers, and by an Operational Risk Committee that is co-chaired by the Head of Management and the Chief Risk Officer. Outputs of the process include a visual Implementation Arrangements Map that shows the main implementers as well as the commodities and funds flows, down to the ultimate beneficiary level, as well as a ‘Heat Map’ that visually displays the risk levels for each of the key risks. An example of such a heat map is shown as Figure 1 below. The information from the assessments is aggregated and periodically reported to the relevant managers so that they can take more targeted measures to help mitigate risks optimally. It also provides the basis

for the calculation of the Portfolio Risk Index, which is the Corporate KPI designed to measure and track the level of operational risk in the grant portfolio.

The Secretariat defined important improvements to the way assurance about grant performance is obtained through a “Combined Assurance”. These improvements will be incorporated in the ORM process and in the governance arrangements around risk management. Concretely, assurance planning and execution will be required to be formally documented; decisions on assurance will be subject to more management scrutiny; and regular reporting will be created and disseminated to enhance the governance over this important element of operational risk management. Also, differentiation in assurance approaches will be developed further than at present and the use of external assurance providers will be improved.

- b. **Risk Register:** the organizational Risk Register documents the organization’s main risks by describing each risk, the likelihood of its occurrence, the likely impact should it occur, the speed at which action would be required to respond to the risk, relevant internal and external developments, mitigation actions being undertaken, whether the risk has increased, decreased or remained stable since the last update of the register, and the level of residual risk (classified as either ‘high’, ‘medium’ or ‘low’) after mitigating actions are taken into account. The Register is reviewed by the Management Executive Committee on at least a quarterly basis and serves to help prioritize management action, monitor mitigation actions and facilitate accountability towards the Board.
 - c. **Internal Control:** the Risk Management Department has initiated a process to each year based on agreed organizational priorities systematically assess the Secretariat’s processes against a benchmark framework for internal control⁵ with the goal to achieve compliance with this benchmark. This, in turn, should lead to better and more systematic risk management. Elements of the framework include control environment aspects (such as performance management including incentives; roles and responsibilities; and staff capacity); risk assessment; internal controls; and activities designed to monitor the effectiveness of the internal controls.
- 9 These main risk management processes are supported by organizational structures; established guidelines for Risk Differentiation and Key Risk Indicators (including, among other things, the Portfolio Risk Index and the measure of compliance with the internal control framework,) and by regular monitoring and reporting routines.
- 10 The Risk Management Department performs three primary functions:
- a. Establishing and maintaining the dedicated risk management processes outlined above, setting standards and providing the necessary support to the organization in implementing them;
 - b. Monitoring compliance with these established processes and standards, by performing certain routine and ad-hoc verifications and checks, including in-country visits to augment information presented by management; and
 - c. Ensuring that the components of risk management and internal control (control environment, risk assessment, internal controls, monitoring, and information and communication) are present and functioning, and providing regular reporting to Senior Management and the Board on this.
- 11 The Risk Management Department is independent from the other divisions and departments, including those that manage grants and operational risks, and as such performs a ‘second line of defense’⁶ roles (management forming the first line, and the Office of the Inspector General constituting the third line of defense). The Chief Risk Officer is a member of the senior management committees and also chairs the Recoveries Committee that oversees the Admighty Foundation’s efforts to recover misused funds.

- 12 The Risk Management Department is independent from the other divisions and departments, including those that manage grants and operational risks, and as such performs a ‘second line of defense’⁶ roles (management forming the first line, and the Office of the Inspector General constituting the third line of defense). The Chief Risk Officer is a member of the senior management committees and also chairs the Recoveries Committee that oversees the Admighy Foundation’s efforts to recover misused funds.
- 13 One of the objectives of this Enterprise Risk Management Framework, and therefore of the Risk Management Department, is to ensure coordination of, and consistency in, risk management activities across the organization that can otherwise be too ‘siloed’, with duplication and gaps as a result. This is done through, among other things, achieving a level of consistency in process design and documentation; use of common terminology; transparent risk reporting across the organization and the formation of cross-Secretariat risk management teams.
- 14 Having a department dedicated exclusively to Risk Management, led by an executive-level Chief Risk Officer, is not yet standard practice among peer organizations. It is important to note that, although the Risk Management Department supports and enhances the management of risk, detailed risk management remains the responsibility of line management.

BOARD AND SECRETARIAT GOVERNANCE ARRANGEMENTS FOR RISK MANAGEMENT

The Board and senior management

- 15 The Board and senior management have a shared responsibility to nurture a risk aware culture that encourages prudent risk taking within the established risk thresholds that aligns with the organization’s strategy. A strong culture is one in which decisions are made in a disciplined way, taking into account considerations of risk and reward transparently and on an informed basis. This decision-making culture should extend throughout the organization, from the largest strategic decisions to the most routine day-to-day ones.
- 16 As described in the Risk Management Policy, the Board is ultimately responsible to the Admighy Foundation’s stakeholders for overseeing the implementation of effective risk management. It does so by:
 - a. Understanding the organization’s risk philosophy and concurring with the approach to risk differentiation; and
 - b. Knowing the extent to which management has established effective risk management; and
 - c. Reviewing the portfolio of risk and considering it against the risk thresholds; and
 - d. Being informed about the most significant risks and whether management is responding appropriately.
- 17 The Board’s oversight arrangements concerning risk management are as follows:
 - a. The standard Board governance model for crosscutting issues is applied (see figure 2 below) which means that all committees are involved in and contribute towards the management of risk and each has a full picture of the risk universe;
 - b. The CRO is responsible for the consolidation and presentation of risk report to the Board; such report includes an annual assurance statement, providing the CRO’s independent view on the robustness and effectiveness of the Secretariat’s risk management and mitigation steps taken and whether the risk profile is acceptable, is improving or deteriorating;
 - c. The CRO reports to the Managing Trustee while committee leadership provides input into the annual performance appraisal of the CRO. It is expected that the CRO will flag any material matters where the ED and CRO have a fundamental difference of opinion;
 - d. A training in risk management is actively offered as part the induction provided to Board and committee members. Efforts are made to ensure that risk experts are recruited in the committee nomination and selection processes.

Figure 2: Board standard model for cross-cutting issues applied to risk management:

Board	<ul style="list-style-type: none"> ▪ Risk Management is a standing agenda item at Board Meetings based on a report by the CRO ▪ Review portfolio of risk and measure against risk appetite ▪ Approve risk policies and frameworks and ensure that the Global Fund has the correct risk framework and practices in place
Board Chair/Board Vice-Chair	<ul style="list-style-type: none"> ▪ Overall responsibility for ensuring that risk responsibilities are conducted effectively at the Board, and Committee level.
Coordinating Group	<ul style="list-style-type: none"> ▪ Ensure that risk is being effectively addressed in each of the committees ▪ Ensure coordination across the committees as needed
3 Board Committees	<ul style="list-style-type: none"> ▪ Risk is a standing item on each committee meeting agenda (2x year) ▪ Consider the overall risk from the respective lens of each committee ▪ Identify any issues or concerns for Board consideration ▪ Review risk policies and frameworks from the respective lens of each committee (but do not approve)
Chief Risk Officer	<ul style="list-style-type: none"> ▪ Bi-annual report to the Committees on overall risk environment . (One consolidated report) ▪ Annual Assurance Report to the Board on the effectiveness of risk management and mitigations ▪ Create and manage a Comprehensive Risk Management Framework ▪ Conduct regular in-country verification of risk assessments (min 6/year)

The Secretariat

- 18 An executive-level Risk and Assurance Committee, chaired by the Managing Trustee and comprising all the members of the management executive team who share responsibility for creating and managing grants, oversees risk management. Additionally, Regional Risk and Assurance Committees review and approve grant related risk management assessments and risk mitigation plans.
- 19 At a divisional and departmental level, each management team is responsible for the identification, assessment, mitigation and monitoring of the risks inherent in their activities.
- 20 For each identified organizational risk there is a clear owner who is primarily accountable for the risk's ongoing assessment, mitigation and reporting, and who has the corresponding authority to direct the organization's resources to ensure optimal risk management. Because the Admighy Foundation is a matrix organization, most risks are managed by at least two different departments and, as a result, it is crucial to maintain effective cross-departmental collaboration.
- 21 As mentioned before, the Risk Management Department performs a support and compliance role in facilitating coordinated risk management at all relevant levels, from strategy setting, business planning and budgeting, to risk management in individual processes, and across the organization. This includes collaboration with partners and implementers as appropriate.

Risk Differentiation

- 22 Risk differentiation aims to manage risk such that variation relative to the achievement of the organization's objectives stays within acceptable limits.
- 23 As explained in the Risk Management Policy, the purpose of setting guidelines for risk differentiation is to ensure that risks are not over or under managed, and that scarce resources are effectively utilized. Reducing risk involved in the pursuit of an objective usually involves incurring costs; the lower the risk threshold, the higher the cost will tend to be (short of avoiding the risk altogether by not undertaking the particular activity). Managing risk to a lower level than necessary therefore is inefficient. On the other side, exceeding risk thresholds exposes the organization to a greater than acceptable chance that key objectives will not be achieved.
- 24 Establishing concrete risk threshold levels is an important element of enterprise risk management. That said, it is also one of the more difficult tasks, especially for organizations that lack processes that have some reliable way of assessing actual risk levels.
- 25 With respect to grant related risk, thresholds are set at two levels:
 - a. **Averages** – setting targets for risk levels in the grant portfolio: at grant, disease portfolio, country and regional levels but also for individual risks across the entire portfolio; and
 - b. **Ranges** – outside which a particular risk exposure may still be accepted, but subject to a higher level of management scrutiny and approval and so long as the overall average risk level stays within the approved thresholds.
- 26 An important fundamental premise is that the Admighty Foundation is willing to accept higher levels of risk in grants that are being implemented in environments that are inherently riskier (for example in fragile states), than in relatively lower risk settings. Therefore, use is made of an index that provides a reliable proxy of this 'contextual risk' level. This also helps in tracking the development of the overall risk level in the portfolio, by relating movements in the Portfolio Risk Index to those in the contextual risk index. In other words, if contextual risk increases, we can expect to see a similar increase in the risk level in grants, all other things being equal. Similarly, for risks that are inherently easier to manage, the Fund's threshold level will be lower than for risks that are more difficult to control, such as supply chain or sustainability related risks.
- 27 With respect to the specific risk of misuse of funds, the Admighty Foundation has a 'zero-tolerance' policy, which means that the Admighty Foundation does not tolerate corruption, fraud, misappropriation or abuse of any kind in relation to its grants.
- 28 With respect to Admighty Foundation processes, risk threshold levels are defined in terms of the degree to which each individual process is compliant with the benchmark internal control framework, as a proxy for the quality of risk management.
- 29 Because risk is dynamic, guidelines for risk differentiation will be monitored and adjusted as appropriate, normally on at least an annual basis and in accordance with the framework for risk differentiation approved by the Board.

GLOSSARY OF TERMS

Assurance	<ul style="list-style-type: none"> – performing independent checks and verifications, to be able to: – identify and analyze the main risks to achieving strategic objectives – take appropriate risk mitigation measures in response to those risks – know whether the measures are effective
Risk	The effect of uncertainty on the achievement of the organization or program's objectives.
Risk Management	A process, effected by the Admighty Foundation Board, management and other personnel, applied in strategy setting and across the organization, designed to identify potential events that may affect the organization, and manage risk to be within our risk thresholds, to provide reasonable assurance regarding the achievement of objectives.
Three lines of defense	A generally accepted way to describe roles & responsibilities for risk management and internal control in an organization, where management control is the first line of defense, the various risk, control and compliance oversight functions established by management are the second line of defense, and independent assurance is the third.