UNITED ARAB EMIRATES
MINISTRY OF COMMUNITY EMPOWERMENT

Guidance Manual for Non-Profit Organisations in the United Arab Emirates

A Practical Guidance Framework to Support Legal Compliance, Transparency, Effectiveness, and the Risk-Based Approach

Prepared by:

Financial Supervision and Compliance Department

Ministry of Community Empowerment

United Arab Emirates

With the participation of a sample of the Non-Profit Organisation sector

Version:

First Edition

Date: Jan 2026

Table of Contents

TOPICS	PAGES
Chapter One	15
1. Introduction	15
1.1 Purpose of the Guidance Manual	16
1.2 Importance of the Non-Profit Organisation Sector in the United Arab Emirates	16
1.3 Protecting the Sector from Abuse	16
1.4 Balancing the Enabling of Legitimate Work with the Prevention of Abuse	16
1.5 Relationship Between the Manual and Official Laws, Regulations, and Instructions	18
1.6 Methodology of the Manual	18
1.7 Who Should Use This Manual?	19
1.8 Key Message of the Manual	19
1.9 Chapter Summary	20
Chapter Two	21
2. Scope of Application	21
2.1 Purpose of this Chapter	22
2.2 Non-Profit Organisations Covered by the Manual	22
2.3 Legal Forms of Non-Profit Organisations	22
2.4 Associations	23
2.5 Civil Foundations	23
2.6 Unions	23
2.7 Social Solidarity Funds	23
2.8 Charitable and Humanitarian Entities and Entities Licensed or Authorised to Collect Donations	24
2.9 Beneficiary Entities of Donations	25
2.10 Entities Organising Voluntary Work	25
2.11 Volunteers and Volunteer Teams	26
2.12 Prohibition on Fundraising Through Volunteers Except with Approval	26
2.13 Classification Guide for Non-Profit Organisations	26
2.14 Fields of Public Benefit Activities	27
2.15 Excluded or Partially Covered Entities	27
2.16 Scope of the Manual by Subject Matter	28
2.17 Limits on the Use of the Manual	28
2.18 Practical Application within the Organisation	28
2.19 Chapter Summary	29
Chapter Three	30
3. Legislative and Regulatory Framework in the United Arab Emirates	30
3.1 Purpose of this Chapter	31
3.2 Federal Decree-Law No. (50) of 2023 on the Regulation of Public Benefit Organisations	31

3.2.1 Legal Forms and Scope of Application	31
3.3 Cabinet Decision No. (5) of 2025 on the Executive Regulation of Federal Decree-Law No. (50) of 2023	32
3.4 Cabinet Decision No. (159) of 2025 on the Approval of the Classification Guide for Public Benefit Organisations and Public Benefit Activities	33
3.5 Federal Law No. (3) of 2021 on the Regulation of Donations	34
3.6 Cabinet Decision No. (96) of 2022 on the Executive Regulation of the Donation Regulation Law	35
3.7 Federal Law No. (13) of 2018 on Voluntary Work	36
3.8 Cabinet Decision No. (70) of 2020 on the Executive Regulation of the Voluntary Work Law	38
3.9 AML/CFT Requirements in the Context of Non-Profit Organisations	38
3.10 Supervision and Inspection	39
3.11 Practical Summary of the Chapter	40
Chapter Four	41
FATF Recommendation 8 and Immediate Outcome 10 under the FATF Standards	41
4.1 Purpose of this Chapter	42
4.2 Position of Recommendation 8 within the FATF Standards	42
4.3 What is Meant by Non-Profit Organisations in the FATF Context?	42
4.4 Concept of the Sub-Set Most Exposed to Risk	42
4.5 Focused and Proportionate Measures	44
4.6 What Recommendation 8 Does Not Require	44
4.7 Relationship Between Recommendation 8 and the National Framework in the United Arab Emirates	45
4.8 Relationship Between the Classification Guide and Recommendation 8	45
4.9 What is FATF Immediate Outcome 10?	46
4.10 What Does Immediate Outcome 10 Mean for Non-Profit Organisations in Practice?	47
4.11 Difference Between Technical Compliance and Effectiveness	47
4.12 How Should the Organisation Deal with FATF Requirements in this Manual?	47
4.13 Practical Summary of the Chapter	48
Chapter Five	50
5. Understanding Terrorist Financing Risks and Abuse in the Non-Profit Organisation Sector	50
5.1 Purpose of this Chapter	51
5.2 Why Do Non-Profit Organisations Need to Understand Risks?	51
5.3 What is Meant by Abuse in the Context of Non-Profit Organisations?	52
5.4 Distinguishing Between Threat, Vulnerability, Risk, and Impact	53
5.5 Factors that May Increase Exposure to Risk	54
5.6 Potential Typologies of Abuse	54
5.7 National and International Sources for Understanding Risks	57

5.8 Risk Indicators: How Should They Be Understood?	57
5.9 Examples of General Risk Indicators	57
5.10 Distinguishing Between an Administrative Error, a Risk Indicator, and Potential Suspicion	58
5.11 Role of the Board of Directors and Executive Management in Understanding Risks	59
5.12 Common Mistakes that Increase the Risk of Abuse	59
5.13 Chapter Summary	60
Chapter Six	61
6. The Risk-Based Approach for Non-Profit Organisations	61
6.1 Purpose of this Chapter	62
6.2 Concept of the Risk-Based Approach	62
6.3 Why Does the Organisation Need an Internal Risk Assessment?	62
6.4 Core Principles of the Risk-Based Approach	63
6.5 Risk Levels	63
6.6 Key Risk Factors	64
6.7 How Should the Organisation Determine the Final Risk Rating?	64
6.8 Appropriate Measures According to Risk Level	66
6.9 When Should the Risk Assessment be Updated?	66
6.10 Responsibilities of Internal Parties	66
6.11 Common Mistakes in Applying the Risk-Based Approach	66
6.12 Applying the Approach to a New Activity	66
6.13 When Should Verification Through Approved Channels be Undertaken?	67
6.14 Chapter Summary	67
Chapter Seven	68
7. Governance, Transparency, and Internal Controls	68
7.1 Purpose of this Chapter	69
7.2 What is Meant by Governance in Non-Profit Organisations?	69
7.3 Responsibility of the Board of Directors	70
7.4 Separation Between Governance and Executive Management	70
7.5 Articles of Association and Founding Documents	70
7.6 Transparency and Accountability	71
7.7 Internal Controls	71
7.9 Authority Matrix	72
7.10 Management of Funds and Bank Accounts	73
7.11 Use of Funds for Approved Purposes	73
7.12 Final Accounts and Annual Budget	74
7.13 Conflicts of Interest	74
7.14 Confidentiality and Data Protection	75
7.15 Volunteer Management from a Governance Perspective	75
7.16 Governance of Partnerships and Contracts	75
7.17 Dealing with Breaches and Risk Indicators	76
7.18 Internal Governance and Risk Committee	76
7.19 Governance and Compliance File	76

7.20 Indicators of Weak Governance	77
7.21 Governance Self-Assessment Questions	77
7.22 Chapter Summary	78
Chapter Eight	79
8. Core Internal Policies and Procedures	79
8.1 Purpose of this Chapter	80
8.2 Why Does the Organisation Need Written Policies?	80
8.3 Characteristics of a Good Internal Policy	80
8.4 List of Core Internal Policies	81
8.5 Governance and Delegation of Authorities Policy	81
8.6 Risk Management Policy	82
8.7 Donations Policy	82
8.8 Donation Acceptance and Rejection Policy	83
8.9 Donor Due Diligence Policy	84
8.10 Partners and Implementers Policy	84
8.11 Beneficiaries and Provision of Assistance Policy	85
8.12 Financial Management and Disbursement Policy	85
8.14 Conflict of Interest Policy	86
8.15 Voluntary Work Policy	86
8.16 Data Protection and Confidentiality Policy	87
8.17 Internal Reporting and Escalation Policy	87
8.18 Record Retention Policy	88
8.19 Training and Awareness Policy	88
8.20 Use of the Organisation's Name and Logo Policy	89
8.21 Breaches and Corrective Actions Policy	89
8.22 Approval and Review of Policies	90
8.23 Common Mistakes in Internal Policies	90
8.24 Chapter Summary	90
Chapter Nine	91
9. Regulation of Donations: Collection, Receipt, and Provision	91
9.1 Purpose of this Chapter	92
9.2 Importance of Regulating Donations	92
9.3 What is Meant by Donations?	93
9.4 Who is Covered by Donation Regulation?	93
9.5 Licensed Entities and Authorised Entities	94
9.6 Prohibition on Fundraising by Natural Persons	94
9.7 Prohibition on Fundraising by Volunteers Without Approval	94
9.8 When is an Activity Considered Fundraising?	95
9.9 Conditions for Granting a Permit	95
9.10 Permit Application Procedures	96
9.11 Duration and Extension of the Permit	96
9.12 Advertising and Publicity for Fundraising	96
9.13 Means of Collecting Donations	97

9.14 In-Kind Donations	97
9.15 Electronic and Digital Donations	98
9.16 Cash Donations	99
9.17 Administrative and Operational Expenses	99
9.18 Efficiency Measurement and Assessment System	100
9.19 Use of Donations for the Specified Purpose	100
9.20 Prohibitions Relating to Donations	101
9.21 Donation Records	102
9.22 Financial and Closing Reports for Campaigns	103
9.23 Due Diligence on Donations and Donors	103
9.24 Handling Anonymous or Unclear Donations	104
9.25 Conditional Donations	104
9.26 Relationship Between Donations and Beneficiaries	105
9.27 Relationship Between Donations and Partners	105
9.28 Risk Indicators in Donations	106
9.29 What Should the Organisation Do When a Risk Indicator Appears?	106
9.30 Fundraising Campaign File	106
9.31 Self-Assessment Questions Before Launching a Fundraising Campaign	107
9.32 Chapter Summary	108
Chapter Ten	109
10. Management of Funds, Accounts, Records, and Financial Reports	109
10.1 Purpose of this Chapter	110
10.2 Special Nature of the Organisation's Funds	110
10.3 Bank Accounts	111
10.4 Use of Personal Accounts	111
10.5 Cash Funds	111
10.6 Donation Boxes	112
10.7 Financial Disbursement	112
10.8 Use of Funds for the Organisation's Purposes	112
10.10 Accounting Records for Donations	115
10.11 General Financial Records of the Organisation	115
10.12 Final Accounts and Annual Budget	116
10.13 Reports Related to Permits and Fundraising Campaigns	116
10.14 Administrative and Operational Expenses	117
10.15 Separation Between the Organisation's Funds and Restricted Donation Funds	117
10.16 Payments to Partners and Suppliers	117
10.17 Payments to Beneficiaries	118
10.18 Bank Reconciliations and Periodic Review	118
10.19 Assets and Entrusted Items	118
10.20 Handling Discrepancies, Shortages, or Losses	119
10.21 Financial Risk Indicators	119
10.22 Role of the Board of Directors in Financial Oversight	120

10.23 Role of the External Auditor	120
10.24 Retention of Supporting Documents	120
10.25 Financial Management Self-Assessment Questions	121
10.26 Chapter Summary	122
Chapter Eleven	123
11. Partners, Beneficiary Entities, and Final Beneficiaries	123
11.1 Purpose of this Chapter	124
11.2 Who is a Partner?	124
11.3 Who is a Beneficiary Entity?	124
11.4 Who is the Final Beneficiary?	125
11.5 Why Do Partnerships and Beneficiaries Present Risk Exposure?	125
11.6 Partners and Intermediaries as Potential Facilitators	126
11.7 Principle of Partner Due Diligence	126
11.8 Levels of Partner Due Diligence	127
11.8.2 Standard Due Diligence	127
11.8.3 Enhanced Due Diligence	127
11.9 Testing Partner or Beneficiary Entity Risk from a Terrorist Financing Perspective	128
11.11 Agreements and Memoranda of Understanding	128
11.12 Selection of Beneficiaries	129
11.13 Verification of Beneficiaries	130
11.14 Protecting the Dignity and Data of Beneficiaries	131
11.15 Evidence that Assistance or Services Have Reached the Intended Beneficiaries	131
11.16 Partners and Beneficiary Entities Outside the State	131
11.17 Partners in Voluntary Work	132
11.18 Conflicts of Interest in the Selection of Partners and Beneficiaries	133
11.19 Risk Indicators Related to Partners	133
11.20 Risk Indicators Related to Beneficiaries	134
11.21 Dealing with Risk Indicators	135
11.22 Follow-Up of Partners After Contracting	135
11.23 Termination of the Relationship with the Partner	136
11.24 Register of Partners, Beneficiary Entities, and Final Beneficiaries	136
Recommended Good Practice	136
11.25 Relationship of this Chapter to Recommendation 8 and the FATF Methodology	137
11.26 Self-Assessment Questions for Partners and Beneficiaries	137
11.27 Chapter Summary	138
Chapter Twelve	139
12. Donors, Contributors, and Due Diligence on Sources of Funding	139
12.1 Purpose of this Chapter	140
12.2 Importance of Donor Due Diligence	140
12.3 Who is a Donor or Contributor?	140
12.4 What is Considered a Source of Funding?	141
12.5 Risk-Based Donor Due Diligence Principle	141

12.6 Levels of Donor Due Diligence	142
12.6.1 Simplified Due Diligence	142
12.6.2 Standard Due Diligence	142
12.6.3 Enhanced Due Diligence	142
12.7 Donor Information Required According to Risk	143
12.8 Large or Unusual Donations	143
12.9 Conditional Donations	144
12.10 Anonymous or Incomplete Donations	144
12.11 Crowdfunding and Public Campaigns	144
12.12 Donations Through Personal Accounts	144
12.13 High-Value In-Kind Donations	144
12.14 Donations Linked to Foreign Entities or Foreign Non-Profit Organisations	144
12.15 Donations Through Virtual Assets or Crypto-Assets	144
12.16 Donations from Higher-Risk Jurisdictions or Areas	147
12.17 Risk Indicators Related to Donors and Donations	147
12.18 Dealing with a Risk Indicator in a Donation	148
12.19 Rejection of Donations	148
12.20 Return of Donations	149
12.21 Donor and Donation Register	149
12.22 Protection of Donor Data	150
12.23 Role of the Board of Directors and Executive Management	151
12.24 Self-Assessment Questions for Donors and Sources of Funding	151
12.25 Chapter Summary	151
Chapter Thirteen	152
13. Voluntary Work, Volunteers, and Volunteer Teams	152
13.1 Purpose of this Chapter	153
13.2 Importance of Organising Voluntary Work	153
13.3 Definition of Voluntary Work	154
13.4 Entities Organising Voluntary Work	154
13.5 Scope of Application of Voluntary Work Provisions	155
13.6 Registration and Licensing of Voluntary Work	155
13.7 Conditions for Natural Person Volunteers	156
13.8 Legal Person Volunteers and Visiting Volunteers	156
13.9 Controls for Practising Voluntary Work	156
13.10 Volunteer Charter	157
13.11 Defining Volunteer Tasks	157
13.12 Prohibition on Fundraising by Volunteers Without Approval	158
13.13 Use of the Organisation's Name and Logo by Volunteers	158
13.14 Volunteers and Access to Beneficiaries	159
13.15 Volunteers and Access to Data	159
13.16 Volunteers and Access to Funds or In-Kind Resources	159
13.17 Volunteers in Activities Outside the State	160

13.18 Virtual Voluntary Work	161
13.19 Volunteers as a Potential Risk Indicator	161
13.20 Obligations of the Entity Organising Voluntary Work	162
13.21 Obligations of Volunteers and Volunteer Teams	162
13.22 Dealing with Volunteer Breaches	163
13.23 Register of Volunteers and Volunteering Opportunities	163
13.24 Voluntary Work and Fundraising: Separating the Two Roles	164
13.25 Self-Assessment Questions for Voluntary Work	164
13.26 Chapter Summary	165
Chapter Fourteen	166
14. Transparency, Records, Reports, and Disclosure to the Competent Authority	166
14.1 Purpose of this Chapter	167
14.2 Concept of Transparency in Non-Profit Organisations	167
14.3 Core Records of the Organisation	167
14.4 National Register of Non-Profit Organisations	168
14.5 Governance Records	168
14.6 Financial and Accounting Records	168
14.7 Final Accounts and Annual Budget	169
14.8 Fundraising Campaign Reports	169
14.9 Activity and Programme Reports	170
14.10 Volunteer and Volunteering Opportunity Records	170
14.11 Partner and Beneficiary Entity Records	170
14.12 Risk and Incident Register	171
14.13 Conflict of Interest Register	171
14.14 Complaints and Observations	172
14.15 Disclosure to the Ministry or Competent Authority	172
14.16 When Should the Organisation Refer to the Ministry or Competent Authority?	172
14.17 Record Retention and Retention Periods	173
14.18 Quality of Records	173
14.19 Digital Transformation and Electronic Records	174
14.20 Public Disclosure and Transparency with the Public	174
14.21 Common Record-Keeping Mistakes	174
14.22 Self-Assessment Questions for Records and Reports	175
14.23 Chapter Summary	176
Chapter Fifteen	177
15. Risk-Based Supervision, Inspection, Follow-Up, and Corrective Actions	177
15.1 Purpose of this Chapter	178
15.2 Legal Basis for Supervision and Inspection	178
15.3 Supervision as Evidence of Effectiveness, Not Merely Compliance	178
15.4 What Does Practical Supervision Mean?	179
15.5 Risk-Based Supervision	179
15.6 Levels of Follow-Up According to Risk	180

15.7 Possible Types of Supervision and Follow-Up	180
15.8 Prior Preparation for Supervision and Inspection	181
15.9 Dealing with Data Requests	181
15.10 Inspection Visit or Field Review	182
15.11 How Should the Organisation Respond During Supervision?	182
15.12 Distinguishing Between an Administrative Observation, a Violation, and a Risk Indicator	183
15.13 Cases Requiring Immediate Escalation	183
15.14 Supervisory Observations	184
15.15 Classification of Observations by Seriousness	184
15.16 Corrective Actions	184
15.17 Root Cause, Not Only Formal Treatment	185
15.18 Dealing with Potential Violations	185
15.19 Continuous Internal Oversight	186
15.20 Use of National Risk Indicators in Internal Inspection Plans	186
15.21 Role of the Board of Directors in Supervision and Follow-Up	186
15.22 Supervision Over Donations	187
15.23 Supervision Over Voluntary Work	187
15.24 Supervision Over Partners and Beneficiaries	188
15.25 Supervision Over Records and Document Retention	188
15.26 Indicators of Weak Inspection Readiness	188
15.27 Inspection Readiness Checklist	189
15.28 Self-Assessment Questions for Supervision and Follow-Up	189
15.29 Chapter Summary	190
Chapter Sixteen	191
16. Awareness, Training, and Capacity-Building	191
16.1 Purpose of this Chapter	192
16.2 Importance of Awareness and Training	192
16.3 National Basis for Awareness in the Area of Financial Crime Prevention	192
16.4 Who Should Be Trained?	193
16.5 Core Training Topics	193
16.6 Training on National Risk Indicators	194
16.7 Training on Voluntary Work	194
16.8 Training on Donations	195
16.9 Training on Partners and Beneficiaries	195
16.10 Training on Records and Reports	195
16.11 Training Methodology: Not One Training for Everyone	196
16.12 Annual Training Plan	197
16.13 Training Register	197
16.14 Measuring Training Effectiveness	198
16.15 Awareness Materials	198
16.16 Examples of Internal Awareness Messages	198
16.17 Scenario-Based Training	199
16.18 Role of the Board of Directors in Building a Compliance Culture	199

16.19 Training and Partners	199
16.20 Common Mistakes in Training and Awareness	200
16.21 Self-Assessment Questions for Training and Awareness	200
16.22 Chapter Summary	201
Chapter Seventeen	202
17. Risk Indicators, Internal Reporting, and Escalation	202
17.1 Purpose of this Chapter	203
17.2 What is a Risk Indicator?	203
17.3 General Principles for Handling Risk Indicators	203
17.5 Risk Indicators Related to Donations and Donors	204
17.6 Risk Indicators Related to Fundraising Campaigns	204
17.7 Risk Indicators Related to Financial Channels and Accounts	205
17.8 Risk Indicators Related to Partners and Beneficiary Entities	205
17.9 Risk Indicators Related to Final Beneficiaries	206
17.10 Risk Indicators Related to Volunteers and Volunteer Teams	207
17.11 Risk Indicators Related to Activities and Projects Inside and Outside the State	208
17.12 Risk Indicators Related to Use of the Organisation's Name or Logo	208
17.13 Risk Indicators Related to Negative Information, Sanctions, and Higher-Risk Parties	209
17.14 Risk Indicators Related to Records, Reports, and Transparency	209
17.15 Additional Indicators Linked to Specialised Typologies of NPO Abuse	210
17.16 Sources for Detecting Risk Indicators	210
17.17 Internal Reporting of Risk Indicators	211
17.18 Minimum Information When Recording a Risk Indicator	211
17.19 Procedures for Handling a Risk Indicator	211
17.20 When Should Immediate Escalation Occur?	212
17.21 When Should the Ministry or Competent Authority Be Consulted?	213
17.22 Risk Indicator and Incident Register	213
17.23 Simplified Model for Assessing a Risk Indicator	214
17.24 Practical Examples	215
17.25 Using Risk Indicators to Improve Controls	216
17.26 Self-Assessment Questions	216
17.27 Chapter Summary	217
Chapter Eighteen	218
18. Protecting Access to Financial Services and Dealing with Banks	218
18.1 Purpose of this Chapter	219
18.2 Why is Access to Financial Services Important?	219
18.3 Relationship Between Financial Services and Transparency	219
18.4 Legal Basis for Bank Accounts	220
18.5 Risks of Using Cash and Informal Channels	220
18.6 What Do Banks Need to Understand About the Organisation?	221
18.7 Updated Bank File	221

18.8 How Should the Organisation Explain its Sources of Funding to the Bank?	222
Recommended Good Practice	222
18.9 How Should the Organisation Explain its Activities to the Bank?	222
18.10 Dealing with Bank Requests for Updated Information	223
18.11 Dealing with Bank Questions About Donations	223
18.12 Dealing with Digital Channels and Electronic Donations	224
18.13 Dealing with Virtual Assets and Crypto-Assets	224
18.14 How Can the Organisation Reduce the Risk of Account Restriction or Closure?	225
18.15 If the Bank Requests Additional Information or Restricts the Account	225
18.16 Relationship Between the Bank and the Competent Authority	226
18.17 Preventing Over-Compliance or Unnecessary Disclosure	226
18.18 Role of the Board of Directors in the Banking Relationship	227
18.19 Indicators that May Raise Questions from the Bank	227
18.20 Banking Readiness Checklist	228
18.21 Self-Assessment Questions for the Banking Relationship	229
18.22 Chapter Summary	229
Chapter Nineteen	230
19. Institutional Communication, Media, and the Use of Images and Humanitarian Stories	230
19.1 Purpose of this Chapter	231
19.2 Importance of Controlling Institutional Communication	231
19.3 Official Communication Channels	231
19.4 Approval of Public Messages	232
19.5 Distinguishing Awareness Content from Fundraising Content	232
19.6 Use of the Organisation's Name and Logo	232
19.7 Use of Beneficiary Images and Humanitarian Stories	233
19.8 Consent and Data Protection	233
19.9 Communication by Volunteers	234
19.10 Communication by Partners and Third Parties	234
19.11 Social Media Controls	234
19.12 Digital Fundraising Links and Public Appeals	225
19.13 Media Enquiries and Public Statements	225
19.14 Public Reporting and Impact Communication	225
19.15 Use of Before-and-After Images or Emotional Content	236
19.16 Correction of Inaccurate Public Information	236
19.17 Impersonation and Unauthorised Use	236
19.18 Communication Risk Indicators	237
19.19 Communication Approval Register	237
19.20 Crisis Communication	238
19.21 Self-Assessment Questions for Communication and Media	238
19.22 Chapter Summary	239
Chapter Twenty	240
20. Activities Outside the State, Cross-Border Partnerships, and External Assistance	240
20.1 Purpose of this Chapter	241
20.2 What is Meant by a Cross-Border Activity?	241

20.3 Why Do Cross-Border Activities Require Additional Care?	241
20.4 External Activities Are Not Prohibited in Themselves	242
20.5 Approvals and Permits Before Implementing an External Activity	242
20.6 Risk Assessment of the External Activity	243
20.7 Risk Classification of the External Activity	243
20.8 Foreign Partners and Foreign Non-Profit Organisations	244
20.9 Agreements with Foreign Partners	245
20.10 Financial Transfers Abroad	245
20.11 Prohibition on Informal Channels and Personal Accounts	246
20.12 Cross-Border In-Kind Assistance	246
20.13 Final Beneficiaries Outside the State	247
20.14 Activities or Volunteering Opportunities Outside the State	247
20.15 Fundraising for Activities Outside the State	247
20.16 Crowdfunding and Cross-Border Platforms	248
20.17 Virtual Assets and Crypto-Assets in Cross-Border Activities	248
20.18 Data Protection in Cross-Border Activities	248
20.19 Use of the Organisation's Name Abroad	249
20.20 Reports and Evidence After Implementation	249
20.21 Risk Indicators in Cross-Border Activities	250
20.22 Cross-Border Activities Register	250
20.23 Checklist Before Implementing an External Activity	250
20.24 Self-Assessment Questions for Cross-Border Activities	251
20.25 Chapter Summary	251
Chapter Twenty-One	252
21. Preparing for Mutual Evaluation and Demonstrating Effectiveness	252
21.1 Purpose of this Chapter	253
21.2 What is Meant by Demonstrating Effectiveness?	254
21.3 Relationship Between this Chapter and Immediate Outcome 10	254
21.4 Difference Between Having a System and Applying a System	255
21.5 What Evidence Demonstrates Effectiveness?	255
21.6 How Should the Organisation Explain its Risks?	256
21.7 How Can the Organisation Demonstrate that it Applies the Risk-Based Approach?	257
21.8 Strong Examples of Evidence of Effectiveness	258
21.9 Using the UAE Financial Intelligence Unit Report to Demonstrate Readiness	258
21.10 What May Assessors or Inspectors Ask About?	259
21.11 How Should the Organisation Answer Effectively?	259
21.12 Answers to Avoid	260
21.13 Effectiveness Evidence File	260
21.14 Effectiveness Matrix	261
21.15 How Should the Organisation Prepare for an Assessment Interview or Visit?	262
21.16 Key Messages the Organisation Should Demonstrate	262
21.17 Common Mistakes in Demonstrating Effectiveness	262
21.18 Role of the Board of Directors in Demonstrating Effectiveness	263
21.19 Role of the Ministry or Competent Authority	263

21.20 Self-Assessment Questions for Demonstrating Effectiveness	264
21.21 Chapter Summary	265
Chapter Twenty-Two	266
22. Roles and Responsibilities within the Organisation	266
22.1 Purpose of this Chapter	267
22.2 Principle of Shared Responsibility	267
22.3 Board of Directors	267
22.4 Executive Management	268
22.5 Finance Officer	269
22.6 Compliance Officer or Focal Point	269
22.7 Donations Officer or Fundraising Team	270
22.8 Programme and Project Officer	271
22.9 Volunteer Coordinator	271
22.10 Employees	272
22.11 Volunteers	272
22.12 Partners	273
22.13 Key Responsibilities Matrix	274
22.14 Who Approves What?	275
22.15 Segregation of Duties	276
22.16 Internal Governance, Risk, and Compliance Committee	277
22.17 Focal Point with the Ministry or Competent Authority	277
22.18 Focal Point with the Bank	278
22.19 Managing Absence or Changes in Key Persons	278
22.20 Accountability and Follow-Up	278
22.21 Common Mistakes in the Allocation of Responsibilities	279
22.22 Self-Assessment Questions for Roles and Responsibilities	279
22.23 Chapter Summary	280
Chapter Twenty-Three	281
23. Map of Legal Obligations and Good Practices	281
23.1 Purpose of this Chapter	282
23.2 How to Read this Map	283
23.4 Map of Obligations Related to Governance and Management	284
23.5 Map of Financial Obligations and Bank Accounts	285
23.6 Map of Obligations Related to Donations	286
23.9 Map of Obligations Related to Voluntary Work	289
23.10 Map of Obligations Related to Activities Outside the State	290
23.11 Map of Obligations Related to Media and Institutional Communication	291
23.12 Map of Obligations Related to Records and Reports	292
23.13 Map of Obligations Related to Supervision and Inspection	293
23.14 Map of Obligations Related to Training and Awareness	294
23.15 Map of Obligations Related to Risk Indicators and Escalation	295
23.16 Map of FATF Recommendation 8 and Immediate Outcome 10 Requirements	296
23.17 Key Matters Requiring Confirmation from the Ministry or Competent Authority	297
23.18 Practical Priorities for the Organisation	297
23.19 Practical Summary of the Chapter	298
General Conclusion of the Manual	299

Introduction

01

Introduction

1.1 Purpose of the Guidance Manual

This Guidance Manual aims to provide Non-Profit Organisations (NPOs) with an integrated guidance framework that explains the legal, regulatory, and supervisory requirements relating to governance, transparency, the regulation of donations, including their collection and distribution and related activities, and the management of risks of abuse and financial crime, in a manner proportionate to the nature of each organisation, the scope of its activities, and the level of risks associated with it.

The Manual covers, in practical terms, the key topics relevant to the work of these entities, including licensing and classification, governance and the allocation of authorities, the management of financial resources and donations, due diligence on donors, partners, and beneficiary entities, record-keeping, reporting, dealing with risk indicators, and responding to supervisory, inspection, and follow-up requirements. It also addresses matters relating to media and institutional communication, financial services, activities outside the State, and cross-border relationships.

The Manual also aims to support these entities in translating legal and regulatory obligations into clear and applicable operating procedures that help demonstrate compliance, transparency, and effectiveness, and enhance their ability to identify and manage the risks associated with their activities in a proportionate and risk-based manner.

The preparation of this Manual forms part of the wider efforts to strengthen the integrity of the Non-Profit Organisation sector, enhance its ability to perform its social, humanitarian, and developmental role efficiently and transparently, and protect it from risks of abuse. This contributes to reinforcing the trust of the community, donors, partners, beneficiaries, and supervisory authorities in the work of these organisations.

This Manual is based on the relevant federal legislation, regulations, and decisions, including Federal Decree-Law No. (50) of 2023 on the Regulation of Non-Profit Organisations, Federal Law No. (3) of 2021 on the Regulation of Donations and its Executive Regulation, as well as the relevant approved decisions, instructions, and regulatory practices. It also takes into account the principles of the risk-based approach, proportionality, and the protection of the legitimate work of Non-Profit Organisations. The Manual was prepared with the participation of a sample of the Non-Profit Organisation sector across its various forms and risk levels.

1.2 Importance of the Non-Profit Organisation Sector in the United Arab Emirates

Non-Profit Organisations represent an important part of the social development system in the United Arab Emirates. They contribute to supporting social, cultural, educational, humanitarian, professional, environmental, voluntary, and other public benefit activities that serve the community.

Federal Decree-Law No. (50) of 2023 regulates the forms of public welfare associations shall be as follows:

- associations
- National society
- unions
- social solidarity funds

any other forms determined by the executive regulations of this decree by law. It also defines the scope of public benefit activities across multiple fields, including social, cultural, scientific, educational, professional, creative, artistic, recreational, and environmental fields, as well as the provision of humanitarian services and the achievement of charitable or solidarity purposes.

From this perspective, enabling and protecting this sector is not limited to legal compliance. It is also linked to strengthening public trust, safeguarding financial and in-kind resources, protecting beneficiaries, and ensuring that assistance and services reach the purposes for which they were collected or allocated.

1.3 Protecting the Sector from Abuse

Despite the positive and vital role played by Non-Profit Organisations, the nature of some sector activities may, in certain cases, expose them to attempts of abuse, particularly where activities involve fundraising, the provision of assistance, working through partners, or implementing programmes of a humanitarian, social, or voluntary nature.

This does not mean that all Non-Profit Organisations are high risk, or that charitable or voluntary activity is inherently suspicious. Rather, the correct approach is to understand risks in a realistic and proportionate manner, and to adopt measures that are appropriate to the size of the organisation, the nature of its activities, its sources of funding, channels of disbursement, beneficiaries, partners, and operating environment.

This Manual is intended to help organisations protect themselves from risks of abuse, including the diversion of funds, unauthorised fundraising, the misuse of the organisation's name or logo for unauthorised purposes, or the misuse of volunteers, partners, or donation channels.

1.4 Balancing the Enabling of Legitimate Work with the Prevention of Abuse

This Manual is based on a fundamental principle: protecting the sector from the risks of money laundering, terrorist financing, and proliferation financing should not lead to the disruption or weakening of the legitimate work of Non-Profit Organisations.

The objective is not to impose uniform burdens on all organisations, but rather to help each organisation adopt controls that are appropriate to the nature of its work and its level of risk. A small organisation with limited local activity does not necessarily face the same level of risk as an organisation operating through multiple funding channels or implementing programmes of a more complex nature.

Accordingly, the Manual adopts a risk-based approach, whereby procedures are more detailed and robust when risks are higher, and more simplified and proportionate when risks are lower.

1.5 Relationship Between the Manual and Official Laws, Regulations, and Instructions

This Manual is a practical guidance tool intended to clarify requirements and assist organisations in implementation. It does not replace the laws, regulations, decisions, circulars, or instructions issued by the Ministry or the competent authority.

In the event of any conflict between this Manual and any applicable legal or regulatory text, the official legal or regulatory text shall prevail. Organisations must also refer to the Ministry or the competent authority where any matter is unclear, or where an approval, permit, or official procedure is required.

1.6 Methodology of the Manual

This Manual is based on four levels of requirements and recommendations:



First: Legal Obligations

These are requirements set out in laws, regulations, and official decisions, such as requirements relating to licensing, declaration, fundraising and the distribution of donations, registration, permits, and financial and administrative controls.



Second: Regulatory / Supervisory Requirements

These are requirements or recommendations issued by the Ministry or the competent authority, or which are linked to licensing, follow-up, supervision, classification, reporting, or inspection procedures.



Third: FATF Recommendation 8 and Immediate Outcome 10 Requirements

These are international standards relating to the protection of Non-Profit Organisations from terrorist financing abuse, which have been reflected in the domestic legislation of the United Arab Emirates, particularly the legal framework on anti-money laundering, countering the financing of terrorism, and counter-proliferation financing and its Executive Regulation.



Fourth: Recommended Practices

These are practical measures that help organisations strengthen governance, transparency, and risk management, such as developing internal policies, documenting Board decisions, screening partners, and training employees and volunteers.

These levels will be identified throughout the Manual using clear labels, such as:


Legal Obligation


Regulatory / Supervisory Requirement


Procedural Requirement


FATF Recommendation


Recommended Practice

1.7 Who Should Use This Manual?

This Manual has been designed as a practical reference for a wide range of users, including:

- Members of Boards of Directors and Boards of Trustees, and managers of organisations or associations.
- Financial and accounting officers.
- Compliance officers or compliance focal points, where applicable.
- Fundraising and donation distribution teams.
- Programme and project teams.
- Volunteer coordinators and volunteers.
- Partners and implementers.
- Donors and supporters.
- Internal and external auditors.
- Staff of regulatory or supervisory authorities concerned with the sector.

The Manual should be read as a practical implementation tool, rather than merely a legal presentation of statutory provisions.

1.8 Key Message of the Manual

The key message of this Manual is that effective compliance is not based solely on the existence of documents and policies. Rather, it depends on the organisation's ability to demonstrate that it has a realistic understanding of its risks, applies appropriate controls, documents its decisions, monitors the use of its resources, and acts promptly when risk indicators or breaches arise.

Effective compliance means that the organisation is able to clearly answer the following questions:

- What is the nature of our activities and sources of funding?
- Who are our donors, partners, and beneficiaries?
- What risks may we be exposed to?
- What controls do we apply to mitigate these risks?
- How do we demonstrate that funds or resources were used for the specified purposes?
- How do we document decisions, approvals, and reports?
- How do we act when a breach or suspicion indicator arises?
- When should we refer to the Ministry or the competent authority?

01 What is the nature of our activities and sources of funding?	02 Who are our donors, partners, and beneficiaries?	03 What risks may we be exposed to?	04 What controls do we apply to mitigate these risks?
05 How do we demonstrate that funds or resources were used for the specified purposes?	06 How do we document decisions, approvals, and reports?	07 How do we act when a breach or suspicion indicator arises?	08 When should we refer to the Ministry or the competent authority?

1.9 Chapter Summary

This chapter sets out the general foundation of the Manual and confirms that protecting Non-Profit Organisations from abuse must be undertaken in a balanced, proportionate, and risk-based manner, while respecting the vital role played by the sector in the United Arab Emirates.

Each organisation should view this Manual as a tool for building a stronger and more transparent internal system, rather than as a mere formal compliance requirement. The ultimate objective is to enable legitimate work, protect resources, strengthen trust, and ensure that public benefit reaches those entitled to it in a safe, organised, and transparent manner.

Scope of Application

02

Scope of Application

2.1 Purpose of this Chapter

This chapter aims to identify the entities and activities covered by this Manual, based on the legal and regulatory instruments in force in the United Arab Emirates, while distinguishing between the scope of application of:

- The legislation regulating Non-Profit Organisations;
- The legislation regulating the collection and provision of donations;
- The Classification Guide for Non-Profit Organisations and Public Benefit Activities.

This chapter is not intended to create a new scope of obligation or to expand the scope of any law or decision. Rather, it clarifies the scope of application of this Manual for the purposes of practical guidance and institutional compliance.

2.2 Non-Profit Organisations Covered by the Manual

Legal Obligation

In relation to Non-Profit Organisations, this Manual applies to Non-Profit Organisations operating and licensed in the United Arab Emirates, in accordance with the scope of application set out in Federal Decree-Law No. (50) of 2023 on the Regulation of Non-Profit Organisations. The Decree-Law also provides that certain institutions established pursuant to local decrees or laws are exempt from its provisions, while remaining, in all cases, subject to specific articles of the Decree-Law, namely Articles 7, 50, 51, 52, 53, 54, and 55.

For the purposes of this Manual, Non-Profit Organisations include private legal persons licensed under the applicable laws of the State, which are established for the purpose of carrying out one or more public benefit activities, without primarily aiming to generate profit. This definition should be treated as the legal basis for determining whether an organisation falls within the scope of Non-Profit Organisations.

2.3 Legal Forms of Non-Profit Organisations

Legal Obligation

Pursuant to Federal Decree-Law No. (50) of 2023, the forms of Non-Profit Organisations include the following:

01 Associations;

02 Civil foundations;

03 Unions;

04 Social solidarity funds;

05 Any other forms determined by the Executive Regulation of the Decree-Law.

Accordingly, this Manual addresses each of these forms according to the nature of its activity and its position within the applicable legal and supervisory framework. The forms that are relevant to the FATF definition and the relevant sub-set are referred to in this Manual as "Public Benefit Organisations".

2.4 Associations

Legal Obligation

For the purposes of this Manual, associations include entities formed by natural persons and established for a definite or indefinite period for the purpose of carrying out one or more public benefit activities, without aiming to generate profit.

Associations are subject to the legal and regulatory requirements relating to establishment, licensing, declaration, articles of association, membership, the general assembly, the board of directors, supervision, inspection, reporting, and any other requirements set out in the relevant laws, regulations, and decisions.

2.5 Civil Foundations

Legal Obligation

For the purposes of this Manual, civil foundations include a legal person established by one or more natural persons, for a definite or indefinite period, based on the allocation of funds for the purpose of carrying out one or more public benefit activities, without aiming to generate profit.

Given that this legal form is linked to the allocation of funds for the achievement of a public benefit purpose, a civil foundation should pay particular attention to financial governance controls, documentation of sources of funds, disbursement mechanisms, and the separation of the foundation's funds from any personal funds or interests of its founders or those responsible for its management.

Recommended Good Practice: Civil foundations should adopt a clear internal policy for the management of allocated funds, covering at a minimum: the purposes for which the funds may be used, authorities for approving disbursements, documentation requirements, periodic reporting, and conflict of interest controls.

2.6 Unions

Legal Obligation

This Manual covers unions as groupings comprising at least five associations or civil foundations that carry out similar public benefit activities, in accordance with the definition set out in Federal Decree-Law No. (50) of 2023.

Unions are particularly important from a governance and supervisory perspective because they may represent more than one organisation or coordinate between several entities operating in the same or related fields. Therefore, unions should have clear mechanisms for defining their roles, representing their members, documenting joint decisions, and preventing the misuse of their status or organisational umbrella.

2.7 Social Solidarity Funds

Legal Obligation

This Manual covers social solidarity funds, which are funds established by legal persons for a definite or indefinite period, with the aim of promoting solidarity and mutual support among the members affiliated with the fund.

The nature of these funds requires particular attention to controls relating to contributions, entitlements, disbursement, documentation, the identification of beneficiaries, the avoidance of conflicts of interest, and ensuring that resources are used for the purposes for which the fund was established.

Recommended Good Practice: A social solidarity fund should maintain a clear register of affiliated members, a register of contributions or resources, and a register of payments or benefits provided, while documenting the basis on which any benefit is disbursed.

2.8 Charitable and Humanitarian Entities and Entities Licensed or Authorised to Collect Donations

Legal Obligation

In relation to the regulation of donations, the scope of this Manual extends to any entity wishing to collect, receive, or provide donations within the State, including in free zones, in accordance with Federal Law No. (3) of 2021 on the Regulation of Donations, its Executive Regulation, and the relevant decisions and instructions. This framework aims to regulate donations, protect donors' funds, ensure that they are used for the purposes for which they were allocated, and prevent their misuse or collection outside approved channels.

The Donation Regulation Law distinguishes between licensed entities and authorised entities. Licensed entities are entities whose establishing laws, decrees, or decisions permit them to collect, receive, or provide donations. These generally include charitable associations and federal, local, or civil authorities and institutions whose legal powers include the collection, receipt, or provision of donations, in accordance with their instrument of establishment and the applicable legislation. Authorised entities, by contrast, are legal persons that do not initially have such authority, but are granted a specific permit by the competent authority to collect, organise, or provide donations in accordance with the provisions of the law.

Accordingly, the mere fact that an entity is non-profit or has a public benefit purpose does not automatically mean that it has the authority to collect, advertise, receive, or provide donations without observing the required licensing, permit, or approval requirements. Whether an entity is considered a licensed entity or requires a prior permit is determined based on its legal status, the scope of its licence or declaration, its establishment decisions, and the official powers or approvals in force in relation to the collection, receipt, or provision of donations.

Any Public Benefit Organisation, association, civil foundation, charitable entity, or other entity that collects, receives, provides, or advertises donations must observe the relevant legal and regulatory requirements, including permits, collection methods, the purpose of the donation, beneficiary entities, administrative and operational expenses, records, reports, and any other requirements set out in the law, its Executive Regulation, and the approved instructions.

Where donations, assistance, or programmes are connected to activities outside the State, or to entities, beneficiaries, or partners outside the State, any additional considerations, approvals, or coordination requirements of the relevant competent authorities must be observed, including those of the UAE Aid Agency or any other relevant federal or local entity, depending on the nature of the activity, the place of implementation, the beneficiary entity, and the applicable official requirements.

Where it is unclear whether an entity falls within the category of licensed entities or requires a permit, or where the requirements relating to donations or externally oriented assistance are unclear, this should be verified through the approved channels and procedures of the competent authority before collecting, advertising, or providing donations.

2.9 Beneficiary Entities of Donations

Legal Obligation

The scope of this Manual also includes beneficiary entities of donations, whether natural or legal persons to whom donations or assistance are provided within or outside the State, in accordance with the definition of beneficiary entity under the Donation Regulation Law.

The fact that an entity is a beneficiary does not necessarily mean that it is subject to all obligations applicable to the entity collecting or providing donations. However, its presence within the donation or assistance chain makes it important from the perspective of verification, documentation, tracing the use of funds or resources, and protecting donors' funds.

Recommended Good Practice: Organisations that provide assistance or donations to beneficiary entities should retain sufficient information on the beneficiary entity, the purpose of the support, the method of provision, and evidence of receipt or use, while applying a level of verification proportionate to the level of risk.

2.10 Entities Organising Voluntary Work

Legal Obligation

In relation to voluntary work, the scope of this Manual includes entities organising voluntary work, which include federal and local government entities, associations, civil institutions, and the private sector, in accordance with Federal Law No. (13) of 2018 on Voluntary Work. The law also covers voluntary work, volunteers, volunteer teams, and entities organising voluntary work.

Accordingly, any Public Benefit Organisation, association, or civil foundation that organises volunteering opportunities, engages volunteers, or forms volunteer teams must observe the requirements of the Voluntary Work Law and its Executive Regulation, including registration, licensing, controls, and relevant conditions.

2.11 Volunteers and Volunteer Teams

Legal Obligation

This Manual covers volunteers, whether natural or legal persons who are registered and carry out voluntary work without material or employment-related remuneration. It also covers volunteer teams, which are groups of registered natural or legal persons who form a team to carry out voluntary work without material or employment-related remuneration.

Volunteers should be treated as part of the governance and operational control framework, particularly where they have access to beneficiaries, funds, donations, data, partners, or the organisation's name and reputation.

2.12 Prohibition on Fundraising Through Volunteers Except with Approval

Legal Obligation

The Voluntary Work Law prohibits volunteers or volunteer teams from collecting donations, allowing donations to be collected, or advertising donations by any means, except with the prior approval of the Ministry.

Accordingly, entities organising voluntary work must clearly distinguish between "voluntary work" and "fundraising". A volunteer's participation in a social, humanitarian, or awareness activity does not automatically grant the volunteer the authority to collect funds, advertise donation campaigns, or use the organisation's name for that purpose.

Proposed Practical Measure:

Volunteer instructions, as well as the volunteer charter or undertaking, should include an explicit provision stating that no volunteer may collect funds, receive donations, advertise them, or use personal accounts, digital channels, electronic links, or the organisation's name or logo for that purpose, except where prior official approval has been obtained and in accordance with the approved procedures.

The organising entity should also ensure that volunteers are made aware of this prohibition before commencing their tasks, and should retain evidence of this within the volunteer register or the file of the volunteering opportunity. Where any breach or risk indicator arises in relation to fundraising by a volunteer or volunteer team, the case must be recorded and addressed in accordance with the approved escalation and follow-up procedures.

2.13 Classification Guide for Public Benefit Organisations

Regulatory / Supervisory Requirement

The Classification Guide applies to Public Benefit Organisations subject to the provisions of the Federal Decree by Law No. (50) of 2023 Concerning the Regulations of Public Welfare Association, and serves as a reference document for the competent authority responsible for licensing, supervising, and overseeing Public Benefit Organisations. The Guide aims to classify Public Benefit Organisations, unify the controls, procedures, conditions, and requirements for classification, and define the fields and activities of Public Benefit Organisations in a precise manner.

Public Benefit Organisations must align their activities and objectives with the fields of work specified in the Classification Guide. The Ministry, in coordination with the local authority, manages and follows up on the classification process.

This is also linked to the requirement of the National Register of Public Benefit Organisations, as a regulatory tool for recording the data of Public Benefit Organisations subject to the provisions of the Decree-Law, updating their core information, and supporting licensing, classification, follow-up, and supervision in accordance with the approved requirements and procedures.

Accordingly, the organisation should ensure the accuracy of its data, classification, and registered scope of activities, and update any material changes to its legal status, objectives, activities, or core information in accordance with the approved procedures and requirements of the Ministry or the competent authority.

2.14 Fields of Public Benefit Activities

Regulatory / Supervisory Requirement

The Classification Guide defines the fields of public benefit activities that may be practised by Public Benefit Organisations, in accordance with the approved classification and the legal status of each organisation. These fields include, among others, social, cultural, educational, scientific, professional, environmental, humanitarian, creative, artistic, recreational, and other public benefit activities specified in the applicable legal and regulatory instruments.

An organisation must ensure that its actual and proposed activities are consistent with its approved classification, its stated objectives, its articles of association or establishment instrument, and the scope of its licence or declaration. It is not sufficient for an activity to fall generally within a public benefit field; it must also be compatible with the organisation's approved objectives, powers, and permitted activities.

Any activity that does not clearly align with the organisation's approved classification, is inconsistent with its objectives, or exceeds the scope of its licence, declaration, or applicable approvals, should not be implemented or advertised before verifying its permissibility through the approved channels and procedures of the competent authority.

2.15 Excluded or Partially Covered Entities

Legal Obligation

Some entities may be excluded from the full application of certain provisions of the Decree-Law, or may be subject only to specific provisions, depending on their legal basis, the manner of their establishment, or the relevant local legislation governing them.

However, exclusion from some provisions does not necessarily mean exclusion from all obligations relating to transparency, governance, reporting, supervision, or the protection of the sector from abuse. Each entity must verify the extent to which the relevant laws, regulations, decisions, and instructions apply to it, according to its legal status and the nature of its activities.

Where the scope of application is unclear, the entity should refer to the Ministry or the competent authority before carrying out any activity that may require licensing, declaration, registration, approval, or a permit.

2.16 Scope of the Manual by Subject Matter

This Manual covers the key topics that are relevant to the work of Public Benefit Organisations and entities associated with donations or voluntary work, including:

- Licensing, declaration, classification, and public benefit activities;
- Governance, transparency, and internal controls;
- Financial management, bank accounts, donations, and disbursement;
- Donors, funding sources, partners, beneficiary entities, and final beneficiaries;
- Voluntary work, volunteers, and volunteer teams;
- Record-keeping, reporting, and disclosure to the Ministry or competent authority;
- Risk indicators, internal reporting, and escalation;
- Supervision, inspection, follow-up, and corrective measures;
- Training, awareness, and capacity-building;
- Financial services and the banking relationship;
- Institutional communication, media, and the use of images and humanitarian stories;
- Activities outside the State, cross-border partnerships, and external assistance;
- Readiness for mutual evaluation and demonstrating effectiveness.

2.17 Limits on the Use of the Manual

This Manual should not be used as a substitute for the applicable legal or regulatory texts, nor should it be relied upon to assume that any activity is permitted without verifying the relevant licence, permit, approval, or regulatory requirement.

The Manual is a practical guidance document designed to support understanding and implementation. It does not create new powers for organisations, nor does it permit activities that are restricted, conditional, or require prior approval under the applicable legislation.

In all cases, the official legal and regulatory texts, and the decisions and instructions issued by the Ministry or the competent authority, shall prevail.

2.18 Practical Application within the Organisation

Each organisation should use this Manual as a practical reference to review its internal systems, policies, records, procedures, and controls in light of its legal form, classification, sources of funding, activities, partners, beneficiaries, and risk level.

The organisation should also identify which parts of the Manual apply directly to it, which parts apply when it engages in certain activities, such as fundraising or voluntary work, and which parts constitute recommended good practices that may be adopted proportionately according to the size, nature, and risk profile of the organisation.

2.19 Chapter Summary

This chapter clarifies that the scope of the Manual is determined by the applicable legal and regulatory framework, the legal form of the organisation, the nature of its activities, and whether it engages in donations, voluntary work, partnerships, or activities inside or outside the State.

The key practical message is that each organisation should understand its legal status, classification, approved activities, and the requirements that apply to it before carrying out any activity, particularly where the activity involves fundraising, the provision of assistance, voluntary work, partnerships, beneficiaries, or cross-border activities.

Legislative and Regulatory Framework in the United Arab Emirates

03

Legislative and Regulatory Framework in the United Arab Emirates

3.1 Purpose of this Chapter

This chapter provides a practical and integrated overview of the legislative and regulatory framework governing Non-Profit Organisations, the regulation of donations, and voluntary work in the United Arab Emirates, based on the relevant laws, regulations, decisions, and official references.

It explains the relevance of each legal instrument to the work of Non-Profit Organisations and its practical impact on governance, licensing, classification, the regulation of activities, fundraising, resource management, voluntary work, supervision, records, reporting, and the protection of the sector from risks of abuse, particularly in the context of terrorist financing.

This chapter does not replace the legal texts themselves. Rather, it aims to help organisations understand the main layers of the legal framework and how these layers are reflected in their practical obligations and internal procedures.

3.2 Federal Decree-Law No. (50) of 2023 on the Regulation of Public Benefit Organisations

Legal Obligation

Federal Decree-Law No. (50) of 2023 represents the core legislative framework for regulating Public Benefit Organisations in the United Arab Emirates. It defines the legal forms of such organisations, their establishment and declaration requirements, licensing procedures, permitted public benefit activities, governance obligations, records, supervision, inspection, and other related requirements.

The Decree-Law is relevant to Non-Profit Organisations because it determines whether an entity falls within the regulated public benefit framework, the legal form under which it operates, the scope of its approved activities, the authority responsible for licensing and supervision, and the obligations it must comply with throughout its lifecycle.

3.2.1 Legal Forms and Scope of Application

The Decree-Law regulates several forms of Public Benefit Organisations, including associations, civil foundations, unions, social solidarity funds, and any other forms determined by the Executive Regulation.

Accordingly, any organisation carrying out one or more public benefit activities must verify whether it falls within the scope of the Decree-Law, whether it is subject to full or partial application of its provisions, and which competent authority is responsible for its licensing, declaration, supervision, and follow-up.

3.2.2 Licensing and Declaration

The Decree-Law prohibits any group or entity from carrying out public benefit activities before completing the licensing procedures with the competent local authority, declaration by the Ministry, registration in the relevant register, and obtaining the required approvals or permits from the competent authorities, depending on the nature of the activity.

It is therefore not sufficient for an entity to have a charitable, social, cultural, professional, educational, or humanitarian purpose. The entity must operate within the legal form, licence, declaration, classification, and approved scope of activities.

3.2.3 Governance and Legal Obligations

The Decree-Law establishes key governance and institutional obligations for for Non-profit Organisations. These include compliance with rules of good governance and sound administration, maintaining internal regulations covering procurement, financial affairs, human resources, and disciplinary measures, and having a professional code of conduct.

For practical purposes, this means that each organisation should maintain an internal governance framework that clearly defines responsibilities, authorities, approval lines, internal controls, financial management requirements, and standards of professional conduct.

3.2.4 Financial Controls and Use of Resources

The Decree-Law requires Public Benefit Organisations to use their financial and in-kind resources in line with their approved purposes and articles of association. It also regulates matters relating to bank accounts, financial records, budgets, final accounts, audits, and oversight by the competent authority.

Organisations must therefore ensure that their resources are clearly recorded, used only for approved purposes, and supported by adequate documentation that demonstrates the legitimacy of receipts, disbursements, transfers, and benefits provided.

3.2.5 Supervision, Inspection, and Accountability

Public Benefit Organisations are subject to supervision and inspection by the competent authority from administrative, technical, and financial perspectives. The competent authority may review records and documents and request data or reports from organisations.

This means that organisations must maintain accurate and up-to-date records and be able to provide evidence of their activities, funds, decisions, approvals, beneficiaries, partners, and use of resources when requested by the Ministry or the competent authority.

3.3 Cabinet Decision No. (5) of 2025 on the Executive Regulation of Federal Decree-Law No. (50) of 2023

Legal Obligation

Cabinet Decision No. (5) of 2025, issuing the Executive Regulation of Federal Decree-Law No. (50) of 2023, provides further detail on the procedures and practical controls relating to the implementation of the Decree-Law.

The Executive Regulation is important because it translates the general obligations contained in the Decree-Law into more detailed procedural requirements, including matters relating to licensing, declaration, registration, classification, governance, supervision, records, and other operational requirements.

For organisations, the Executive Regulation should be read alongside the Decree-Law. Where the Decree-Law establishes the general obligation, the Executive Regulation often explains how that obligation is to be implemented in practice.

Accordingly, Public Benefit Organisations should ensure that their internal procedures, records, governance arrangements, and communications with the Ministry or competent authority are aligned with both the Decree-Law and its Executive Regulation.

3.4 Cabinet Decision No. (159) of 2025 on the Approval of the Classification Guide for Public Benefit Organisations and Public Benefit Activities

Regulatory / Supervisory Requirement

Cabinet Decision No. (159) of 2025 approves the Classification Guide for Public Benefit Organisations and the public benefit activities they may carry out.

The Classification Guide is a key regulatory reference for determining the classification of Public Benefit Organisations, standardising classification controls and requirements, and defining the fields and activities that may be practised by such organisations.

The Guide is relevant to organisations because it helps determine the nature of their approved activities, the field within which they operate, and the extent to which their actual or proposed activities are consistent with their classification, objectives, articles of association, licence, or declaration.

3.4.1 Practical Impact of Classification

Classification is not merely an administrative label. It has practical implications for:



The activities the organisation may carry out;



The nature of approvals or permits it may need;



The level of supervision and follow-up that may apply;



The risk profile of the organisation;



The records, reports, and supporting evidence the organisation is required to maintain.

An organisation should therefore ensure that its activities, projects, communications, fundraising activities, partnerships, and external engagements are consistent with its approved classification and stated objectives.

3.4.2 Activities Outside the Approved Classification

Any activity that does not clearly fall within the organisation's approved classification, objectives, or scope of licence or declaration should not be implemented or advertised before verifying the applicable requirements through the approved channels and procedures of the Ministry or competent authority.

3.5 Federal Law No. (3) of 2021 on the Regulation of Donations

Legal Obligation

Federal Law No. (3) of 2021 on the Regulation of Donations establishes the legal framework for the collection, receipt, provision, and regulation of donations in the United Arab Emirates.

The Law is relevant to Non-Profit Organisations because many organisations may collect donations, receive donations, provide donations, advertise donation campaigns, or benefit from donated funds or in-kind resources as part of their activities.

The Law aims to regulate donations, protect donors' funds, ensure that donations are used for the purposes for which they were collected, and prevent unauthorised or misleading fundraising.

3.5.1 Licensed Entities and Authorised Entities

The Law distinguishes between licensed entities and authorised entities.

Licensed entities are entities whose establishing laws, decrees, or decisions allow them to collect, receive, or provide donations. Authorised entities are legal persons that do not have such authority by default but are granted a specific permit by the competent authority to collect, organise, or provide donations in accordance with the Law.

Accordingly, an organisation should not assume that its non-profit or public benefit status automatically allows it to collect, advertise, receive, or provide donations. The applicable authority must be determined based on the organisation's legal status, licence, declaration, establishment instrument, and the approvals or permits granted to it.

3.5.2 Donation-Related Activities

Donation-related activities may include collecting donations, receiving donations, providing donations, advertising donation campaigns, using digital or electronic fundraising channels, collecting in-kind donations, managing donation boxes, organising fundraising events, or transferring donations to beneficiary entities.

Before carrying out any such activity, the organisation must verify whether it is legally permitted to do so, whether a permit or approval is required, and which controls apply to the donation, campaign, channel, purpose, beneficiary, and reporting requirements.

3.5.3 Key Practical Obligations

The Law requires organisations involved in donations to pay particular attention to:

01 The legal basis for collecting, receiving, or providing donations;	02 The purpose for which donations are collected;	03 The approved channels and methods for collection;	04 The identity and role of beneficiary entities;
05 The use of donations for the purposes for which they were collected;	06 Records and accounting documentation;	07 Reporting to the competent authority;	08 Avoiding unauthorised or misleading fundraising.

3.6 Cabinet Decision No. (96) of 2022 on the Executive Regulation of the Donation Regulation Law

Legal Obligation

Cabinet Decision No. (96) of 2022 provides the Executive Regulation of Federal Law No. (3) of 2021 on the Regulation of Donations. It sets out detailed procedures and controls relating to fundraising permits, advertising and publicity, collection methods, administrative and operational expenses, donation records, reports, efficiency assessment, and other practical requirements.

The Executive Regulation is particularly important for organisations because it explains the practical requirements that must be observed before, during, and after a fundraising campaign or donation-related activity.

3.6.1 Permits and Fundraising Procedures

The Executive Regulation sets out requirements relating to permit applications, the information to be submitted, the timing of requests, the purpose of fundraising, the target amount, advertising materials, and the period of the permit.

Organisations should therefore ensure that no fundraising activity is launched, advertised, or implemented before verifying the applicable permit requirements and obtaining the necessary approvals where required.

3.6.2 Advertising and Publicity

The Executive Regulation regulates advertising and publicity for donations. Any public communication intended to invite the public to collect, receive, or provide donations may fall within the scope of donation advertising.

Accordingly, organisations should review donation-related content before publication, including social media posts, campaign messages, electronic links, images, videos, and public appeals, to ensure that they are consistent with the approved permit and applicable legal requirements.

3.6.3 Administrative and Operational Expenses

The Executive Regulation permits certain licensed non-governmental entities, subject to the prior approval of the competent authority, to deduct a percentage of donations to cover administrative and operational expenses necessary for fundraising, within the limits and conditions specified in the Regulation.

Organisations should not deduct any amount from donations for administrative or operational expenses unless this is permitted under the applicable rules and approved by the competent authority where required.

3.6.4 Records, Reports, and Assessment

The Executive Regulation requires entities involved in donations to maintain proper records and provide reports and information to the competent authority as required.

This includes maintaining sufficient records of donation amounts, collection channels, expenditure, beneficiary entities, and relevant approvals and supporting documents. Organisations should also be prepared to provide information required for efficiency assessment and supervisory follow-up.

3.7 Federal Law No. (13) of 2018 on Voluntary Work

Legal Obligation

Federal Law No. (13) of 2018 on Voluntary Work is relevant to the work of Non-Profit Organisations where the organisation organises voluntary work, engages volunteers or volunteer teams in the implementation of its projects or programmes, or works with volunteers as part of its activities inside or outside the State.

The relevance of the Law is not limited to defining voluntary work in general. It also creates practical obligations for an organisation when it acts as an entity organising

voluntary work, particularly in relation to the organisation of volunteer participation, the assignment of tasks, the use of the organisation's name or logo, the protection of data, and the prevention of unauthorised fundraising through volunteers.

3.7.1 Voluntary Work and the Organising Entity

The Law defines voluntary work as any individual or collective activity, carried out without material or employment-related remuneration, for the purpose of achieving a benefit for others.

For the purposes of this Manual, a Non-Profit Organisation may be considered an entity organising voluntary work when it launches a volunteering opportunity, assigns volunteers to tasks within its projects, or cooperates with volunteer teams or partners to implement activities within its approved purposes.

Accordingly, before engaging volunteers, the organisation should clearly define the nature of the volunteer task, the entity responsible for managing it, the scope of volunteer participation, and the controls governing the use of the organisation's name, logo, resources, or data during the performance of voluntary work.

3.7.2 Registration and Licensing When Engaging Volunteers

The Law establishes a register at the Ministry for volunteers and volunteer teams. The relevant legal framework also regulates the registration of volunteers and volunteer opportunities and the licensing of voluntary work.

Therefore, when a Public Benefit Organisation organises voluntary work or engages volunteers in its projects, it must ensure that the applicable registration, licensing, or approval requirements are met, depending on the nature of the activity and the requirements of the Ministry or competent authority.

No voluntary work should be carried out in the name of the organisation, whether inside or outside the State, except through the approved channels and procedures and in a manner that ensures clarity of responsibilities between the organisation, the volunteers, and any partners involved in implementation.

3.7.3 Core Obligations When Engaging Volunteers in Projects

When engaging volunteers in its projects or activities, the organisation must observe the legal obligations applicable to entities organising voluntary work. These include defining the tasks to be performed, providing appropriate orientation or training, ensuring health and safety requirements where applicable, protecting the data and information accessed by volunteers, and ensuring that volunteers comply with instructions, the Volunteer Charter, and applicable legislation.

The organisation should also retain evidence of volunteer participation, including volunteer details, the nature of the tasks, the period of participation, and any undertakings, instructions, or controls communicated to the volunteers.

3.7.4 Prohibition on Using Voluntary Work for Fundraising Without Approval

The organisation must ensure that volunteers or volunteer teams do not collect donations, allow donations to be collected, or advertise donations by any means in the name of the organisation or by relying on their status as volunteers, except after obtaining the required prior official approvals and following the approved procedures.

This prohibition should be reflected in volunteer acceptance forms, instructions issued to volunteers, and any agreements or arrangements with volunteer teams or partners participating in the implementation of activities.

3.8 Cabinet Decision No. (70) of 2020 on the Executive Regulation of the Voluntary Work Law

Legal Obligation

Cabinet Decision No. (70) of 2020 sets out the Executive Regulation of Federal Law No. (13) of 2018 on Voluntary Work. It details the practical controls and procedures relating to the practice of voluntary work, including the registration of volunteers and volunteering opportunities, conditions for voluntary work, virtual volunteering, and the obligations of entities organising voluntary work.

For Non-Profit Organisations, the Executive Regulation is particularly relevant when organising volunteering opportunities or engaging volunteers in the implementation of projects and programmes. In such cases, the organisation must observe the requirements relating to registration, licensing, allocation of responsibilities, safety, confidentiality, data protection, and the prevention of any unauthorised use of voluntary work for fundraising or the promotion of fundraising activities.

The detailed requirements relating to volunteer management, volunteer policies, and volunteering partnerships are addressed in the operational chapters of this Manual.

3.9 AML/CFT Requirements in the Context of Non-Profit Organisations

FATF Recommendation / Regulatory and Supervisory Requirement

The framework governing Non-Profit Organisations in the United Arab Emirates is also linked to the national system for anti-money laundering and countering the financing of terrorism, particularly in relation to protecting the sector from abuse for terrorist financing purposes.

The FATF Standards, particularly Recommendation 8 and Immediate Outcome 10, require countries to identify the sub-set of Non-Profit Organisations that may be at risk of terrorist financing abuse and to apply focused and proportionate measures to protect them from such abuse.

In the UAE framework, these requirements are reflected in the legal and regulatory obligations relating to risk assessment, classification, monitoring, awareness, supervision, data exchange, and the adoption of measures to ensure the integrity and accountability of organisations.

3.9.1 Role of the Ministry and the Competent Authority

The relevant legal framework requires the Ministry, in coordination with the local authority, to assess risks relating to Public Benefit Organisations periodically, classify them in accordance with the relevant requirements and classification guide, identify the relevant sub-set, monitor it, and ensure that organisations fulfil their obligations.

It also provides for the development of policies and necessary measures to ensure accountability and integrity, the implementation of awareness and education programmes, and the exchange of relevant data and information locally, regionally, and internationally for AML/CFT purposes.

3.9.2 Practical Impact on Organisations

Each organisation should be able to demonstrate the following:

01 Its understanding of the nature of its risks;

02 Its compliance with its approved classification and activities;

03 The existence of controls to protect financial and in-kind resources;

04 Documentation of funding sources and disbursement methods;

05 Sufficient records and data on donations, donors, beneficiaries, and partners, according to the nature of the activity;

06 Its response to requests from the Ministry or the competent authority;

07 Its cooperation with awareness, education, and supervisory programmes.

3.10 Supervision and Inspection

3.10.1 Supervision of Non-Profit Organisations

Legal Obligation

Non-Profit Organisations are subject to the supervision of the competent authority from administrative, technical, and financial perspectives, in order to verify expenditure and the proper direction of their financial and in-kind resources towards the purposes and projects carried out in accordance with their articles of association.

For this purpose, the competent authority may review the records and documents of organisations and request any data or reports from them. The local authority must also provide the Ministry with any reports, data, or information requested in relation to the results of supervision and inspection.

3.10.2 Supervision of Donations

Legal Obligation

Licensed entities and authorised entities are subject to the supervision and oversight of the competent authority from the financial and administrative perspectives relating to donations, without prejudice to the powers of other government supervisory authorities.

Such entities must provide any data, information, or documents requested by the competent authority.

3.11 Practical Summary of the Chapter

This chapter demonstrates that the legislative and regulatory framework in the United Arab Emirates consists of several interconnected layers:

- The Decree-Law regulating Public Benefit Organisations, which defines the entity, legal form, licensing, declaration, activities, register, supervision, and related requirements.
- The Executive Regulation of the Decree-Law, which details the applicable procedures and practical controls.
- The Classification Guide, which determines the fields of activity, classification requirements, and the link between the organisation's approved status and its permitted activities.
- The Donation Regulation Law and its Executive Regulation, which govern the collection, receipt, provision, advertising, recording, reporting, and supervision of donations.
- The Voluntary Work Law and its Executive Regulation, which apply when organisations engage volunteers, volunteer teams, or voluntary work opportunities in their activities and projects.
- The AML/CFT framework, which focuses on protecting the sector from abuse, particularly terrorist financing abuse, through risk assessment, proportionate measures, awareness, supervision, and data exchange.

The core practical rule is that each organisation should first identify and understand its legal status, the scope of its activities, and the competent authority supervising it, and should then apply the relevant legal and supervisory requirements and good practices in a manner proportionate to the nature of its work and risks.

FATF Recommendation 8 and Immediate Outcome 10: Requirements for Non-Profit Organisations

04

FATF Recommendation 8 and Immediate Outcome 10: Requirements for Non-Profit Organisations

4.1 Purpose of this Chapter

This chapter aims to explain the relationship between the work of Non-Profit Organisations, on the one hand, and the requirements of the Financial Action Task Force (FATF), on the other hand, particularly Recommendation 8 on Non-Profit Organisations, its Interpretive Note, and Core Issue 10.3 under Immediate Outcome 10.

The United Arab Emirates has reflected the requirements of Recommendation 8 in its national legislative and regulatory framework through the laws, regulations, decisions, and instructions relating to the regulation of Non-Profit Organisations, the regulation of donations, voluntary work, risk assessment, classification, supervision, awareness, and the identification of institutions or activities that may be more exposed to risks of abuse. Accordingly, this chapter does not treat FATF Standards as standalone obligations imposed directly on organisations. Rather, it explains how these standards have been reflected in the applicable national framework, and how organisations can understand and apply them in a practical and balanced manner.

This chapter also aims to help organisations understand the rationale underlying the protection of the sector from abuse, particularly in the context of terrorist financing, in a risk-based and proportionate manner that does not disrupt the legitimate work of Non-Profit Organisations.

4.2 Position of Recommendation 8 within the FATF Standards

Recommendation 8 is the FATF Recommendation that specifically addresses Non-Profit Organisations. It does not assume that all Non-Profit Organisations are high risk, nor does it require the imposition of uniform measures on all organisations without distinction. Rather, it focuses on protecting the part of the sector, or the sub-set of organisations, that is most exposed to risks of terrorist financing abuse.

Recommendation 8 is based on three core principles:

- Identifying the organisations, activities, or channels that are more exposed to risk.
- Applying focused and proportionate measures according to the level of risk.
- Protecting the legitimate work of Non-Profit Organisations without disrupting it or imposing unjustified burdens when applying requirements.

Accordingly, proper implementation of Recommendation 8 is not based on a generalised restrictive approach towards the sector, nor on assuming good faith without controls. Rather, it is based on understanding risks and directing measures towards the areas that may be more exposed to abuse.

4.3 Meaning of Non-Profit Organisations under the FATF Standards

FATF does not use the concept of Non-Profit Organisations only in its broad meaning. Rather, it focuses on organisations that fall within the functional definition relevant to Recommendation 8, namely those that collect, receive, transfer, or disburse funds or resources for charitable, religious, cultural, educational, social, humanitarian, or other similar purposes.

This distinction is important because Recommendation 8 does not assume that every non-profit entity automatically falls within the scope of its specific measures merely because it does not aim to generate profit. Similarly, organisations that fall within the functional scope of Recommendation 8 are not all treated as having the same level of risk or requiring the same degree of measures. Instead, consideration is given to the nature of their activities, sources of funding, channels, partners, beneficiaries, and geographic scope of operations.

Some organisations may have limited local activities, may not collect public donations, and may not deal with partners or beneficiaries in higher-risk environments. Their exposure to risk may therefore be limited. By contrast, other organisations may be more exposed to risk due to the nature of their activities, sources of funding, channels, partners, or geographic scope of operations.

4.4 Concept of the Sub-Set Most Exposed to Risk

One of the key requirements of Recommendation 8 is that the State identify the sub-set of Non-Profit Organisations that may be more exposed to terrorist financing abuse.

Exposure to risk may be linked to factors such as:

01 Raising donations from the public.

02 Receiving or transferring funds or resources.

03 Providing financial or in-kind assistance.

04 Working through partners or intermediaries.

05 Implementing activities outside the State.

06 Dealing with foreign entities or foreign Non-Profit Organisations.

07 Operating in higher-risk areas or environments.

08 Using cash or less transparent financial channels.

09 Weak governance, records, or internal controls.

The presence of any of these factors does not mean that the organisation is in breach or is automatically high risk. It means that the organisation or the supervisory authority needs to understand the level of risk exposure and apply appropriate and proportionate controls.

4.5 Focused and Proportionate Measures

Focused and proportionate measures mean that controls and procedures are linked to the actual risks of the organisation, activity, channel, or partner, rather than being applied generally to all organisations at the same level.

For example, a local organisation with limited cultural activities that does not collect public donations should not be treated with the same level of measures applied to an organisation implementing relief activities outside the State, collecting donations through multiple channels, or dealing with foreign partners and organisations.

The practical rule is as follows: the higher the risks, the greater the need for stronger controls, deeper documentation, and more regular follow-up. Where risks are limited, controls should remain simplified and proportionate, without imposing unjustified burdens on the organisation.

4.6 What Recommendation 8 Does Not Require

It is important to clarify that Recommendation 8 does not require the following:

Treating all Non-Profit Organisations as high risk.	Imposing the same compliance requirements on all organisations regardless of their size, activity, and risk profile.	Disrupting access to assistance or services by legitimate beneficiaries.
Using counter-terrorist financing as a reason to impose disproportionate restrictions on civil society.	Using counter-terrorist financing as a reason to impose disproportionate restrictions on civil society.	Replacing risk-based supervision with formalistic or general procedures.

Sound implementation of Recommendation 8 must balance, on the one hand, the protection of the sector from abuse and, on the other hand, enabling Non-Profit Organisations to fulfil their legitimate mission.

4.7 Relationship Between Recommendation 8 and the National Framework in the United Arab Emirates

In the United Arab Emirates, the national legislative and regulatory framework has reflected the requirements relevant to the technical compliance aspect of Recommendation 8 through the system of laws, regulations, decisions, and instructions regulating Non-Profit Organisations, donations, voluntary work, risk assessment, classification, supervision, and awareness.

The practical link between Recommendation 8 and the national framework appears through a number of key areas, including:

01 Licensing, declaration, and classification of Non-Profit Organisations.

02 Regulation of the collection, receipt, and provision of donations.

03 Regulation of voluntary work and volunteering opportunities.

04 Risk assessment and classification of organisations.

05 Identification of the sub-set most exposed to risks of abuse.

06 Awareness and education on protecting the sector.

07 Supervision, follow-up, and inspection.

08 Records, reports, and accountability.

Accordingly, this Manual does not treat FATF requirements as obligations separate from the national framework. Rather, it explains how the requirements relevant to Recommendation 8 have been translated into the applicable laws, regulations, decisions, and instructions, and how Non-Profit Organisations can apply them in practice in a risk-based and proportionate manner that preserves legitimate work.

Nevertheless, the completeness of the legislative and regulatory framework from a technical compliance perspective is not, by itself, sufficient to demonstrate effectiveness. Effectiveness remains linked to the practical implementation of these requirements, the quality of supervision and awareness, the ability of organisations to understand their risks, document their decisions, and demonstrate that the controls applied have a practical impact in protecting the sector from abuse.

4.8 Relationship Between the Classification Guide and Recommendation 8

The Classification Guide for Non-Profit Organisations helps to understand the nature of the organisation, the scope of its activities, and its fields of work. This makes it an important tool not only for licensing and supervisory purposes, but also for understanding risk.

The nature of the activity is one of the key factors in determining the extent to which an organisation may be exposed to risks of abuse. An organisation with charitable, humanitarian, or relief activities, or one that collects donations or provides assistance, may have a different risk profile from an organisation with limited local cultural, professional, or environmental activities.

Accordingly, classification should be one of the inputs to risk assessment, alongside other factors such as sources of funding, financial channels, partners, beneficiaries, volunteers, and the geographic scope of activities.

4.9 What is FATF Immediate Outcome 10?

Immediate Outcome 10 is one of the effectiveness outcomes under the FATF Methodology. It relates to the extent to which terrorists, terrorist organisations, and terrorist financiers are prevented from raising, moving, and using funds, and from abusing the Non-Profit Organisation sector.

In the context of Non-Profit Organisations, the assessment of effectiveness does not focus only on the existence of laws or policies. It considers whether measures are actually implemented and achieve a practical impact, such as:

01 Understanding the risks of abuse of the sector.

02 Identifying the sub-set or activities most exposed to risk.

03 Applying focused and proportionate measures.

04 Conducting effective and targeted outreach.

05 Undertaking risk-based supervision and follow-up.

06 Taking corrective action where needed.

07 Avoiding disproportionate disruption of legitimate activity.

4.10 What Does Immediate Outcome 10 Mean for Non-Profit Organisations in Practice?

Although Immediate Outcome 10 primarily assesses the effectiveness of the State and competent authorities, Non-Profit Organisations contribute in practice to demonstrating effectiveness through their ability to show that they apply the required controls in their day-to-day work.

In practical terms, this means that the organisation should be able to demonstrate the following:

- It understands its legal status and approved classification.
- Its activities fall within the scope of its licence or approved permissions.
- It maintains clear records of donations, resources, and expenditures.
- It has controls for dealing with unusual or conditional donations.
- It knows its partners and beneficiary entities according to the level of risk.
- It organises the work of volunteers and clarifies the limits of their roles.
- It retains evidence of activity implementation and the delivery of assistance or services.
- It responds to risk indicators and does not ignore them.

- It responds to requests from the Ministry or the competent authority.
- It reviews its procedures when observations or gaps arise.

4.11 Difference Between Technical Compliance and Effectiveness

It is important to distinguish between technical compliance and effectiveness.

Technical compliance means that laws, regulations, decisions, and systems exist to define the requirements. Effectiveness means that these requirements are applied in practice and lead to tangible results in protecting the sector.

Therefore, it is not sufficient for an organisation to have a written policy or a form kept in a file. The evidence must show that the policy or form actually influenced a decision, behaviour, or outcome.

Examples of evidence of effectiveness include:

- A donation that was suspended or rejected due to risk indicators.
- A partner that was screened before the relationship was approved.
- A fundraising campaign that was not launched before the required approvals were completed.
- Volunteers who were trained on the limits of their role.
- A supervisory observation that was addressed through corrective action.
- A risk indicator that was recorded, escalated, and closed.
- A Board of Directors that discussed material risks or observations.

4.12 How Should the Organisation Deal with FATF Requirements in this Manual?

The organisation should deal with the FATF requirements referred to in this Manual as a framework for understanding risks and effectiveness, not as an independent source that creates new legal obligations for the organisation.

Accordingly, practical application is achieved through:



Compliance with national laws, regulations, and decisions.



Using the risk-based approach in applying controls.



Distinguishing between low-, medium-, and high-risk activities.



Documenting decisions and procedures.



Increasing the level of controls when risks increase.



Communicating with the Ministry or the local authority if the Non-Profit Organisation believes that any procedures have affected, or may affect, charitable activities.

4.13 Practical Summary of the Chapter

The practical messages of this chapter can be summarised as follows:



Recommendation 8 does not assume that all Non-Profit Organisations are high risk, nor does it aim to restrict the legitimate work of such organisations.



Proper implementation of Recommendation 8 focuses on identifying the organisations, activities, channels, or relationships that are more exposed to terrorist financing abuse risks, rather than imposing uniform measures on all organisations without distinction.



Not every non-profit entity automatically falls within the scope of the measures specific to Recommendation 8. Consideration must be given to whether it falls within the functional definition of Non-Profit Organisations under the FATF Standards, as well as to the nature of its activities, resources, and channels.



The United Arab Emirates has reflected the requirements relevant to the technical compliance aspect of Recommendation 8 in its national legislative and regulatory framework, including the regulation of Non-Profit Organisations, donations, voluntary work, classification, risk assessment, supervision, and awareness.



The organisation must understand its legal status, approved classification, and authorised scope of activities, and must ensure that its actual activities are consistent with its licence, declaration, or applicable approvals.



The organisation must apply controls proportionate to the level of risk. Controls should be stronger where there are public donations, partners, activities outside the State, beneficiaries, or channels that are more exposed to risk, and simpler where risks are limited.



Protecting the sector does not mean disrupting legitimate work or imposing unjustified burdens on organisations. Rather, it means enabling them to perform their social, humanitarian, and developmental role with clear and appropriate controls.



Core Issue 10.3 under Immediate Outcome 10 focuses on effectiveness, meaning practical implementation and results, not only the existence of texts, policies, or forms.



Non-Profit Organisations contribute to demonstrating effectiveness by maintaining accurate records, documenting their decisions, training their employees and volunteers, dealing with risk indicators, and responding to requests from the supervisory authority.



It is not sufficient for an organisation to have written policies. It must be able to show that these policies have actually influenced its decisions, such as accepting or rejecting a donation, approving a partner, suspending an activity, or escalating a risk indicator.



Classification, donations, partners, volunteers, records, supervision, awareness, and risk indicators are interconnected elements in protecting the sector and should be treated as one system, not as separate requirements.



Where the scope of a local requirement is unclear, or where there is an activity, relationship, or case whose status cannot be clearly determined, this should be verified through the approved channels and procedures before a decision is made or the activity is implemented.

Accordingly, this chapter forms the bridge between the national framework of the United Arab Emirates, on the one hand, and the FATF Standards and effectiveness requirements, on the other. The operational details are addressed in the subsequent chapters covering donations, partners, volunteers, records, supervision, and cross-border activities in greater detail.

Understanding Terrorist Financing Risks and Abuse in the Non-Profit Organisation Sector

05

5.1 Purpose of this Chapter

This chapter aims to help Non-Profit Organisations understand the nature of risks of abuse, particularly in the context of terrorist financing, and how such risks may arise through resources, activities, donation channels, partners, beneficiaries, volunteers, or the use of the organisation's name and legal status.

Referring to risks does not mean that Non-Profit Organisations are under suspicion, or that the sector is inherently high risk. Rather, the objective is to enable organisations to understand where vulnerabilities may arise, and how such vulnerabilities can be prevented, detected, or addressed in a practical and proportionate manner.

This chapter should be read in light of the role assigned to the Ministry, in coordination with the local authority, in periodically assessing risks relating to Public Benefit Organisations, classifying them in accordance with international requirements and the Classification Guide, identifying the relevant sub-set, monitoring it, ensuring that organisations fulfil their obligations, and implementing awareness and education programmes on anti-money laundering and countering the financing of terrorism.

5.2 Why Do Non-Profit Organisations Need to Understand Risks?

Non-Profit Organisations need to understand risks because the nature of some activities may expose the organisation, in certain cases, to attempts of abuse, even where the organisation itself is acting in good faith and its objectives are legitimate.

Risks may arise where an organisation collects donations, receives or transfers funds, provides assistance, relies on partners or intermediaries, engages volunteers, carries out activities outside the State, or communicates with the public through digital channels or public campaigns.

A proper understanding of risk helps the organisation to:

01 Protect its resources and reputation.

02 Ensure that funds and assistance reach the intended purposes and beneficiaries.

03 Prevent the misuse of its name, logo, legal status, or donation channels.

04 Apply controls that are proportionate to the nature and level of risk.

05 Respond appropriately to risk indicators or unusual situations.

06 Demonstrate compliance and effectiveness to the Ministry or the competent authority.

Understanding risk does not mean restricting legitimate work or treating every activity as suspicious. It means knowing where exposure may arise and applying suitable controls before the issue becomes a breach, a misuse case, or a supervisory concern.

5.3 What is Meant by Abuse in the Context of Non-Profit Organisations?

In the context of Non-Profit Organisations, abuse may occur when the organisation, its resources, name, activities, channels, partners, volunteers, or legal status are used in a manner that is inconsistent with its approved purposes, applicable laws, or authorised activities.

Abuse may take several forms. It may involve the diversion of funds or in-kind resources, the misuse of a programme or project, misleading or unauthorised fundraising, the use of unclear partners or front entities, misuse of volunteers or voluntary status, the use of digital channels or crowdfunding in an unregulated manner, or the implementation of cross-border activities without sufficient controls.

In the context of terrorist financing, the risk is not limited to the clear case where funds are directly transferred to a terrorist person or organisation. Abuse may also occur indirectly, for example where funds are raised under a charitable or humanitarian cover but are then diverted, where a seemingly legitimate project is used to conceal unauthorised beneficiaries or partners, or where weaknesses in controls over partners, distribution channels, or volunteers are exploited.

Accordingly, the practical understanding of risk should focus on how the organisation, its resources, name, activities, or channels could be misused, even where the organisation or its management did not intend such misuse.

5.4 Distinguishing Between Threat, Vulnerability, Risk, and Impact

To understand risk in a practical manner, it is important to distinguish between four concepts:

Concept	Meaning	Example in the Context of Non-Profit Organisations
Threat	A person, entity, or conduct that may seek to misuse the organisation.	A person attempting to raise donations in the organisation's name without authorisation.
Vulnerability	An internal or external weakness that may be exploited.	The absence of clear procedures for approving donation links or digital publications before they are published.
Risk	The possibility that a threat will exploit a vulnerability.	Funds being collected in the organisation's name without authorisation or proper documentation.
Impact	The consequence if the risk materialises.	Misleading donors, reputational harm, supervisory accountability, or loss of public trust.

For example, if an organisation allows donation links or promotional content to be published on social media without prior internal review or approval, the vulnerability may be the absence of clear procedures for approving donation-related links and posts before publication. The threat may be a person or entity impersonating the organisation or using its logo or messaging to raise funds. The risk is that funds may be collected in the organisation's name without authorisation or documentation. The impact may include misleading donors, loss of trust, or exposing the organisation to accountability.

5.5 Factors that May Increase Exposure to Risk

Some Non-Profit Organisations may be more exposed to risk because of specific features of their activities, not merely because of their legal status.

Key exposure factors may include:

01 Dealing with funds or donations.

02 Providing cash or in-kind assistance.

03 Working with partners or intermediaries.

04 Implementing activities outside the State or in connection with external environments.

05 Carrying out large-scale humanitarian, relief, or charitable activities.

06 Relying on large numbers of volunteers.

07 Using digital channels or public fundraising campaigns.

08 Weak governance or limited administrative resources.

09 Absence of written policies or adequate records.

10 Lack of clarity in the allocation of authorities between the Board, management, employees, and volunteers.

The presence of these factors does not necessarily mean that the organisation is high risk. Rather, they are indicators that require a better understanding of the appropriate controls.

5.6 Potential Typologies of Abuse

5.6.1 Misuse of Funds or Resources

Funds may be collected for a legitimate purpose, and then all or part of them may be diverted to another unauthorised purpose, to unintended beneficiaries, or to entities that have no connection with the purpose for which the funds were collected.

Potential risk indicators may include:



No clear link between the donation and its purpose.



Disbursement of funds without supporting documents.



Transfers to personal accounts.



Failure to submit financial reports to the competent authority or the Board of Directors.



Changing the purpose for which funds are used without approval.

Appropriate controls may include linking each donation or campaign to a clear purpose, using official bank accounts, documenting approvals, retaining proof of expenditure, and preparing reports in accordance with the applicable requirements.

5.6.2 Misuse of Programmes or Projects

A programme or project may be presented as charitable, humanitarian, social, or educational, while in practice being used to reach unauthorised beneficiaries, support an undeclared purpose, or provide resources to a party that does not fall within the approved scope of the activity.

Potential risk indicators may include unclear project objectives, weak documentation of implementation, inability to verify beneficiaries, inconsistent reports, or a partner's refusal to provide information on the use of funds or resources.

Organisations should ensure that each programme or project has a defined purpose, clear approval, documented beneficiaries or beneficiary categories, implementation records, and evidence that the assistance or service reached the intended purpose.

5.6.3 Misleading or Unauthorised Fundraising

Fundraising may be misused where funds are collected without the required permit, where the public is misled about the purpose of the campaign, or where a person or entity uses the organisation's name, logo, or reputation without authorisation.

Potential risk indicators may include unauthorised donation links, social media posts inviting donations without approval, use of personal accounts, unclear campaign messaging, or failure to provide a report on the amount collected and how it was used.

Organisations should ensure that fundraising is carried out only through approved channels, in accordance with the applicable permits or approvals, and that any public messaging is reviewed before publication.

5.6.4 Use of Unclear Partners or Front Entities

Partners, intermediaries, or implementing entities may be used to conceal the real recipient of funds or resources, or to implement activities outside the approved purpose.

Potential risk indicators may include a partner with unclear legal status, refusal to provide registration or authorisation documents, unclear ownership or management, inability to provide implementation reports, or requests to transfer funds to a third party unrelated to the approved activity.

Organisations should apply due diligence on partners in a manner proportionate to risk, ensure that agreements clearly define roles and responsibilities, and retain records demonstrating how funds or resources were used.

5.6.5 Misuse of Volunteers or Voluntary Status

Volunteers may be misused where they collect donations without authorisation, use the organisation's name or logo outside their assigned task, communicate with donors or beneficiaries without approval, or fail to comply with the Volunteer Charter or the organisation's instructions.

Potential risk indicators may include a volunteer raising donations independently, using the organisation's badge or logo outside the task, publishing messages in the organisation's name without approval, refusing to return assets or materials after the assignment, or engaging with beneficiaries or donors through unauthorised individual communication.

Controls may include registering volunteers through approved procedures, defining tasks in writing, requiring volunteers to sign a charter or undertaking, prohibiting fundraising unless approvals have been obtained, training volunteers on confidentiality and professional conduct, recovering badges and entrusted items after completion of the assignment, and establishing a mechanism for reporting breaches.

5.6.6 Risks of Digital Channels, Crowdfunding, and Virtual Assets

Digital channels, crowdfunding platforms, online payment links, social media campaigns, and virtual assets may create additional risks due to speed of dissemination, difficulty of control, the possibility of impersonation, and the potential use of channels that are not sufficiently transparent.

Potential risk indicators may include donation links created without authorisation, digital campaigns without a clear responsible party, use of personal accounts or wallets, receipt of donations through unfamiliar platforms, or inability to identify the amount collected and the purpose for which it was used.

Organisations should ensure that digital fundraising is subject to the same level of governance and approval as other fundraising channels, and that no digital link, online campaign, or virtual asset-related donation mechanism is used unless this is permitted and approved under the applicable legal and regulatory framework.

5.6.7 Risks of Cross-Border Activities

Activities, programmes, partnerships, assistance, or volunteering opportunities outside the State may be more sensitive because of differences in legal environments, difficulty of monitoring, multiple partners, or the association of some regions or contexts with higher risks.

Potential risk indicators may include implementing activities outside the State without clear approvals, using foreign partners without sufficient verification, inability to

confirm the final beneficiaries, transferring funds through informal channels, or absence of post-implementation reports.

Organisations should apply enhanced review to activities outside the State, ensure that required approvals or coordination are obtained, verify partners and channels, retain evidence of implementation, and provide reports as required by the competent authority.

5.7 National and International Sources for Understanding Risks

Non-Profit Organisations should not rely only on internal assumptions when understanding risks. They should also take into account relevant national and international sources, where applicable.

These sources may include:

01 The national and sectoral risk assessments.

02 The Classification Guide and supervisory instructions.

03 Guidance issued by the Ministry or competent authority

04 Reports and guidance issued by the UAE Financial Intelligence Unit, where relevant.

05 FATF standards, guidance, and best practices relating to Recommendation 8.

06 Supervisory observations, inspection findings, and corrective action requirements.

07 Internal incident records, complaints, and risk indicators identified by the organisation.

Using these sources helps the organisation align its internal understanding of risks with the broader national understanding of the sector and with the expectations of the competent authorities.

5.8 Risk Indicators: How Should They Be Understood?

A risk indicator is not, by itself, proof that a violation, terrorist financing case, or abuse has occurred. It is a sign or circumstance that requires attention, review, documentation, and, where necessary, escalation.

Risk indicators should be understood in context. A single indicator may be explainable or administrative in nature. However, where several indicators appear together, or where an indicator is linked to unclear funds, unauthorised channels, high-risk partners, foreign activities, or refusal to provide information, the organisation should treat the matter with greater caution.

The organisation should avoid two common mistakes: ignoring risk indicators because no breach has yet been proven, and treating every minor administrative issue as suspicion. The correct approach is to review the situation, document the facts, assess the level of concern, and take proportionate action.

5.9 Examples of General Risk Indicators

Examples of general risk indicators may include:

01 A large or unusual donation that is inconsistent with the organisation's usual activity or donor profile.

02 A donation from an unclear or unknown source.

03 A condition attached to a donation that directs funds to a specific person or unclear entity.

04 Use of a personal account, informal channel, or unauthorised digital link.

05 A fundraising campaign launched without the required approval.

06 A partner refusing to provide basic legal or operational information.

07 Inability to verify that assistance reached the intended beneficiaries.

08 Requests to transfer funds to a third party not included in the approved arrangement.

09 Volunteers collecting donations or using the organisation's name without approval.

10 Weak or missing records relating to donations, beneficiaries, partners, or expenditures.

11 Negative information relating to a donor, partner, beneficiary entity, or intermediary.

12 Repeated errors or gaps in records that affect the traceability of funds or resources.

These indicators do not automatically establish suspicion, but they require review and appropriate action.

5.10 Distinguishing Between an Administrative Error, a Risk Indicator, and Potential Suspicion

Not every administrative error is an indicator of terrorist financing, and not every risk indicator proves the existence of a violation. Therefore, it is important to distinguish between three levels:

Administrative Error

This may include a missing document, delayed update of data, or an error in a register, without any indications of misuse.

Risk Indicator

This may include a large donation from an unclear source, a partner refusing to provide information, the use of a personal account, or an unauthorised campaign.

Potential Suspicion

This may arise where several indicators are combined, or where information appears suggesting possible misuse of funds, activity, legal status, partners, beneficiaries, or channels.

Where the organisation is unsure about the appropriate action, it should follow the approved internal escalation procedures and, where necessary, refer to the Ministry or competent authority in accordance with official instructions.

5.11 Role of the Board of Directors and Executive Management in Understanding Risks

Understanding risks should not be the responsibility of one employee alone. The Board of Directors or trustees is responsible for oversight and direction, executive management is responsible for implementation, and employees and volunteers are responsible for complying with instructions and reporting risks.

The Board of Directors should ensure that:

- An updated risk assessment exists.
- Appropriate policies are approved.
- Financial and operational reports are reviewed.
- Material breaches and risk indicators are followed up.
- Controls exist over donations, partners, and volunteers.
- A culture of compliance and transparency is supported.

Executive management should translate these expectations into operating procedures, assign responsibilities, maintain records, follow up on risk indicators, and ensure that staff and volunteers understand the controls relevant to their roles.

5.12 Common Mistakes that Increase the Risk of Abuse

Common mistakes that may increase the risk of abuse include:

01. Assuming that the organisation is low risk simply because it is charitable or non-profit.
02. Treating risk assessment as a formal document rather than a practical tool.
03. Launching campaigns or activities before confirming the required approvals.
04. Using personal accounts or informal channels.
05. Not documenting donations, disbursements, or beneficiary records.
06. Relying on partners without adequate due diligence.
07. Allowing volunteers to use the organisation's name or logo without clear controls.
08. Failing to review digital content or donation links before publication.
09. Ignoring unusual donations or unclear conditions.
10. Not escalating risk indicators or supervisory observations.
11. Keeping policies that are not implemented in practice.

5.13 Chapter Summary

The key message of this chapter is that protecting Non-Profit Organisations from abuse is not achieved by fearing risk or treating the entire sector as high risk. It is achieved through a realistic and balanced understanding of exposure points and vulnerabilities.

The practical approach can be summarised in five steps:



Know the organisation's activities, funding, partners, beneficiaries, and volunteers.



Identify where risks may arise.



Apply controls that are proportionate to the level of risk.



Monitor indicators and act when they arise.



Document decisions and procedures, and refer to the Ministry or the competent authority where matters are unclear.

By adopting this approach, the organisation can protect its legitimate work, safeguard its resources, strengthen trust, and demonstrate that its internal controls are not merely formal requirements but practical measures that support transparency, accountability, and effectiveness.

The Risk-Based Approach for Non-Profit Organisations

06

The Risk-Based Approach for Non-Profit Organisations

6.1 Purpose of this Chapter

This chapter aims to explain how Non-Profit Organisations can apply the risk-based approach in practice, in a manner that is proportionate to the size of the organisation, the nature of its activities, its sources of funding, its partners, beneficiaries, volunteers, and the geographic scope of its work.

The risk-based approach does not mean complicating the work of the organisation or imposing the same procedures on all activities. Rather, it means understanding where risks may arise and applying controls that are appropriate to the level of risk. Controls should be stronger where risks are higher, and simpler where risks are lower.

This chapter provides a practical framework that helps organisations move from a general understanding of risks to a structured internal process for assessing, documenting, updating, and responding to those risks.

6.2 Concept of the Risk-Based Approach

The risk-based approach means that the organisation identifies and assesses the risks associated with its activities, resources, partners, beneficiaries, volunteers, and channels, and then applies measures that are proportionate to those risks.

Under this approach, the organisation should not treat all activities, donations, partners, or projects in the same way. A small local activity that does not involve donations or external partners does not require the same level of review as a cross-border programme involving donations, foreign partners, and beneficiary entities outside the State.

The practical objective is to ensure that the organisation's controls are neither excessive nor insufficient. Excessive controls may disrupt legitimate work, while insufficient controls may expose the organisation to abuse, reputational harm, or supervisory accountability.

6.3 Why Does the Organisation Need an Internal Risk Assessment?

The risk assessment helps the organisation answer practical questions such as:

01 What activities do we carry out?

02 What sources of funding do we rely on?

03 Do we collect or receive donations?

04 Do we use cash or digital channels?

05 Who are our partners and beneficiary entities?

06 Do we work outside the State?

07 Do we use volunteers?

08 What records and controls do we maintain?

09 What are the areas where abuse, error, or non-compliance may occur?

The purpose of the assessment is not merely to produce a document, but to support decision-making. It should help the organisation determine which areas require stronger controls, where additional approvals may be needed, and what information should be documented.

6.4 Core Principles of the Risk-Based Approach

The risk-based approach is based on several core principles.

Proportionality means that the level of controls should correspond to the level of risk. Where risks are limited, simplified procedures may be sufficient. Where risks are higher, more detailed review, documentation, approval, and follow-up may be required.

Protection of legitimate activity means that controls should not prevent the organisation from carrying out its lawful social, charitable, humanitarian, cultural, educational, or voluntary activities. The purpose of controls is to protect the organisation and its beneficiaries, not to obstruct legitimate work.

Documentation means that decisions, approvals, reviews, and actions taken in response to risks should be recorded. Documentation is important because it demonstrates that the organisation understood the risk and acted reasonably and proportionately.

Continuous review means that the risk assessment should not be treated as a one-time exercise. Risks may change when the organisation launches a new activity, receives a new type of donation, works with a new partner, enters a new geographic area, or receives supervisory observations.

6.5 Risk Levels

For practical purposes, the organisation may classify risks into three broad levels: low, medium, and high.

Low Risk

Low risk may apply where the activity is local, limited in scope, does not involve public fundraising, does not involve cash or complex channels, and does not involve partners, beneficiaries, or activities in higher-risk environments. In such cases, simplified controls and basic documentation may be sufficient.

Medium Risk

Medium risk may apply where the activity involves donations, partners, beneficiaries, volunteers, or some level of operational complexity, but the organisation is able to verify the relevant parties and maintain adequate records and controls. In such cases, additional review and documentation may be required.

High Risk

High risk may apply where the activity involves large or unusual donations, unclear funding sources, complex partners, activities outside the State, higher-risk jurisdictions or environments, unclear beneficiaries, cash-intensive operations, digital fundraising, or other factors that increase exposure to abuse. In such cases, enhanced review, senior management or Board-level approval, additional documentation, and more regular follow-up may be required.

The classification of a risk as low, medium, or high should be based on the facts of the case and the organisation's operating context, not on assumptions alone.

6.6 Key Risk Factors

The organisation should consider a range of risk factors when assessing activities, donations, partners, beneficiaries, or projects.

The first factor is the **nature of the activity.** Activities involving direct assistance, donations, relief, humanitarian support, or the distribution of resources may require more careful controls than purely internal or limited administrative activities.

The second factor is the **geographic scope.** Activities outside the State, or activities connected to foreign partners, foreign beneficiaries, or cross-border transfers, may require additional review and coordination.

The third factor is the **source and nature of funding.** Donations that are large, unusual, anonymous, conditional, or received through unfamiliar channels may require additional review.

The fourth factor is the **financial channel.** Use of official bank accounts and transparent channels reduces risk, while cash, personal accounts, informal transfers, or unclear digital channels may increase risk.

The fifth factor is the **partner or implementing entity.** Partners with clear legal status, documented experience, and transparent reporting may present lower risk than partners whose status, ownership, management, or activities are unclear.

The sixth factor is the **beneficiary or beneficiary entity.** Where beneficiaries or beneficiary entities are clearly identified and the purpose of assistance is documented, risks may be lower. Where beneficiaries are unclear, difficult to verify, or linked to higher-risk environments, additional controls may be needed.

The seventh factor is the **use of volunteers.** Volunteers may increase operational reach, but they also require clear roles, instructions, and controls, particularly where they interact with donors, beneficiaries, funds, data, or the organisation's name and reputation.

The eighth factor is the **quality of governance and records.** Strong governance, clear authorities, accurate records, and documented decisions reduce risk. Weak governance, informal decision-making, missing records, or unclear accountability may increase risk.

6.7 How Should the Organisation Determine the Final Risk Rating?

The final risk rating should be based on a combined assessment of the relevant factors, rather than on a single factor in isolation.

For example, a donation may be large, but if it is received from a well-known and documented entity through an official bank channel for a clearly approved purpose, the overall risk may be manageable. Conversely, a smaller donation may require further attention if it is conditional, anonymous, repeated, linked to an unclear purpose, or received through an unusual channel.

The organisation should document the reasons for the risk rating, particularly where the case is classified as medium or high risk. The purpose is not to create lengthy documents, but to ensure that the reasoning is clear and can be reviewed later by management, the Board, auditors, or the competent authority if required.

6.8 Appropriate Measures According to Risk Level

The measures applied by the organisation should correspond to the level of risk.

For low-risk activities, the organisation may rely on basic documentation, standard approvals, ordinary record-keeping, and routine follow-up.

For medium-risk activities, the organisation may require additional information, management review, clearer documentation of the purpose and parties involved, and follow-up after implementation.

For high-risk activities, the organisation should apply enhanced measures, which may include additional due diligence, senior management or Board approval, verification of partners or beneficiary entities, review of funding channels, consultation with the Ministry or competent authority where necessary, and closer monitoring of implementation and reporting.

The organisation should avoid applying enhanced measures automatically to every case, as this may create unnecessary burdens. At the same time, it should not treat higher-risk cases as ordinary cases merely to facilitate implementation.

6.9 When Should the Risk Assessment be Updated?

The risk assessment should be updated when there are material changes in the organisation's activities, funding, partners, beneficiaries, volunteers, or operating environment.

Examples of situations that may require an update include:

01. Launching a new activity or programme.
02. Starting fundraising or using a new donation channel.
03. Receiving large, unusual, anonymous, or conditional donations.
04. Working with a new partner or implementing entity.
05. Implementing activities outside the State.
06. Expanding the use of volunteers.
07. Receiving supervisory observations or inspection findings.
08. Identifying a breach, incident, or significant risk indicator.
09. Changes in the organisation's classification, legal status, or approved scope of activities.

The organisation should also review its risk assessment periodically, even where no major incident has occurred, to ensure that it remains up to date and reflects the actual nature of its work.

6.10 Responsibilities of Internal Parties

Applying the risk-based approach is a shared responsibility within the organisation.

The Board of Directors or Board of Trustees is responsible for oversight, approving key policies, reviewing material risks, and ensuring that appropriate controls are in place.

Executive management is responsible for implementing the risk-based approach, assigning responsibilities, ensuring that staff understand the procedures, and following up on risks and corrective actions.

The finance function is responsible for maintaining financial records, monitoring receipts and disbursements, ensuring that funds are used for approved purposes, and identifying unusual financial activity.

Programme and project teams are responsible for understanding the risks associated with activities, partners, beneficiaries, and implementation arrangements.

The fundraising or donations team is responsible for applying the relevant procedures for donation channels, donor information, permits, campaign records, and reporting.

Volunteer coordinators are responsible for ensuring that volunteers are registered, assigned clear roles, trained, and prevented from using the organisation's name or status for unauthorised fundraising.

All staff and volunteers should understand that they have a role in identifying and reporting risk indicators within their area of work.

6.11 Common Mistakes in Applying the Risk-Based Approach

Common mistakes include treating the risk assessment as a formal document prepared only for inspection purposes, without using it to guide actual decisions.

Another common mistake is treating all risks as high, which leads to unnecessary complexity and may disrupt legitimate work. Conversely, treating all activities as low risk because the organisation has a charitable purpose may expose the organisation to abuse or supervisory concerns.

Other mistakes include failing to update the risk assessment when activities change, not documenting the reasons for decisions, not linking controls to the level of risk, ignoring risk indicators, and failing to involve the Board or senior management in material risk decisions.

6.12 Applying the Approach to a New Activity

Before launching a new activity, the organisation should consider the following:

01 Is the activity consistent with the organisation's approved objectives and classification?

02 Does the activity require a permit, approval, or notification?

03 Will it involve fundraising, donations, or in-kind resources?

04 Who will implement the activity?

05 Are there partners, beneficiaries, or volunteers involved?

06 Will the activity take place inside or outside the State?

07 What records and evidence will be retained?

08 What could go wrong, and what controls are needed?

This simple review helps the organisation determine whether the activity is low, medium, or high risk, and what procedures should be applied before implementation.

6.13 When Should Verification Through Approved Channels be Undertaken?

The organisation should verify matters through the approved channels and procedures of the Ministry or competent authority where the applicable requirement is unclear, where an activity may require approval, permit, or coordination, or where

the organisation is uncertain whether a donation, partner, activity, or external engagement is permissible.

Examples may include launching a fundraising campaign, accepting a large or conditional donation, implementing an activity outside the State, working with a foreign partner, using a new digital fundraising channel, or engaging volunteers in activities that may involve public communication or donations.

Verification should not be treated as a substitute for the organisation's own internal controls. Rather, it is an additional safeguard where the legal or regulatory position is unclear or where official approval is required.

6.14 Chapter Summary

The risk-based approach is a practical tool that helps Non-Profit Organisations apply controls in a balanced and proportionate manner.

The key message of this chapter is that risk should be understood, assessed, documented, and managed, not ignored or exaggerated. Organisations should apply stronger controls where risks are higher, and simpler controls where risks are limited, while ensuring that legitimate work is not disrupted.

A sound risk-based approach requires the organisation to understand its activities, funding, partners, beneficiaries, volunteers, and operating environment; classify risks reasonably; apply appropriate controls; document decisions; update the assessment when circumstances change; and refer to the Ministry or competent authority where matters are unclear or official approval is required.

By applying this approach, the organisation strengthens governance, protects its resources, supports transparency, and demonstrates that it is taking practical and proportionate measures to protect itself and the sector from abuse.

Governance, Transparency, and Internal Controls

07

Governance, Transparency, and Internal Controls

7.1 Purpose of this Chapter

This chapter aims to explain the importance of governance, transparency, and internal controls within Non-Profit Organisations, and how these elements help ensure that the organisation is managed properly, that its funds and resources are used for their approved purposes, and that risks of abuse, mismanagement, conflicts of interest, or unauthorised use of the organisation's name or resources are reduced.

Governance is not merely a formal requirement. It is a practical system that determines who decides, who approves, who implements, who reviews, and how decisions and resources are documented and monitored.

This chapter also explains the link between governance and effectiveness. An organisation that maintains clear authorities, sound records, financial oversight, transparent reporting, and effective internal controls is better able to demonstrate compliance, accountability, and protection of its legitimate work.

7.2 What is Meant by Governance in Non-Profit Organisations?

Governance means the set of rules, structures, responsibilities, authorities, procedures, and controls through which the organisation is directed and managed.

In the context of Non-Profit Organisations, governance ensures that the organisation:

01 Operates within its approved legal status, classification, and objectives;	02 Uses its funds and resources for the purposes for which it was established;	03 Maintains clear decision-making and approval processes;	04 Separates oversight from day-to-day implementation;
05 Prevents conflicts of interest and misuse of authority;	06 Maintains accurate records and reports;	07 Responds to risk indicators, breaches, or supervisory observations;	08 Cooperates with the Ministry or competent authority where required.

Good governance helps protect the organisation, its beneficiaries, donors, members, volunteers, partners, and public reputation.

7.3 Responsibility of the Board of Directors

Recommended Good Practice / Legal Obligation where applicable

The Board of Directors, or the relevant governing body, has the primary responsibility for oversight, direction, and ensuring that the organisation is managed in a manner consistent with its approved objectives, articles of association, and applicable legal and regulatory requirements.

The Board should ensure the following:

01 Approval of the organisation's core policies.

02 Review of key risks.

03 Monitoring compliance with the approved classification and activities.

04 Oversight of financial resources and donations.

05 Approval of budgets, accounts, and reports.

06 Follow-up of breaches, observations, or risk indicators.

07 Ensuring that clear authorities exist for expenditure and signature.

08 Reviewing the performance of executive management.

09 Ensuring compliance with requests from the competent authority.

10 Protecting the organisation's reputation and public trust.

The Board's role is not to carry out every operational task itself, but to ensure that there is a functioning system of management, oversight, documentation, and accountability.

7.4 Separation Between Governance and Executive Management

Recommended Good Practice

The role of the Board of Directors should be distinguished from the role of executive management.

The Board sets direction, approves policies, oversees performance, and ensures that resources are used for approved purposes.

Executive management implements plans and activities, manages staff and volunteers, maintains records, prepares reports, and applies policies and procedures.

This separation helps prevent the concentration of powers in the hands of one person and reduces the risks of mismanagement, unauthorised expenditure, conflicts of interest, or weak accountability.

7.5 Articles of Association and Founding Documents

Legal Obligation

The organisation's articles of association, founding instrument, licence, declaration, classification, and relevant approvals are core governance documents. They define the organisation's legal status, objectives, approved activities, membership or founding structure, governance bodies, authorities, and operating limits.

The organisation should ensure that its activities, fundraising, partnerships, projects, communications, and use of funds are consistent with these founding and regulatory documents.

Where the organisation intends to carry out an activity that is not clearly covered by its approved objectives, classification, or licence, it should verify the applicable requirements through the approved channels and procedures of the Ministry or competent authority before implementation.

7.6 Transparency and Accountability

Recommended Good Practice / Legal Obligation where applicable

Transparency means that the organisation maintains clear, accurate, and accessible records that show how decisions were made, how funds were received and spent, who approved key actions, and how activities were implemented.

Accountability means that the responsible persons within the organisation can explain and justify decisions, provide supporting documents, and respond to questions from the Board, auditors, the Ministry, the competent authority, donors, or other relevant stakeholders.

Transparency and accountability are particularly important in relation to:

- Donations and fundraising campaigns;
- Bank accounts and financial transactions;
- Disbursement decisions;
- Beneficiary selection;
- Partner selection and follow-up;
- Voluntary work and volunteer participation;
- Activities outside the State;
- Risk indicators and corrective actions;
- Reports submitted to the Ministry or competent authority.

Transparency does not require disclosing unnecessary personal or sensitive information to the public. Rather, it requires maintaining records and evidence that enable proper review and supervision.

7.7 Internal Controls

Recommended Good Practice

Internal controls are the procedures and mechanisms that help ensure that the organisation's activities are implemented properly, funds are protected, and errors, misuse, or breaches are prevented or detected.

Internal controls include five main elements:

7.7.1 A Sound Control Environment

This means having an institutional culture that promotes integrity, compliance, respect for the law, and zero tolerance for the use of funds or the organisation's name for purposes other than those approved.

7.7.2 Risk Assessment

This means that the organisation understands the potential vulnerabilities in its activities, donations, partners, and volunteers, and updates this assessment when circumstances change.

7.7.3 Clear Control Procedures

These include approvals, signatures, segregation of duties, limits of authority, bank reconciliations, and review of supporting documents.

7.7.4 Information and Documentation

This means maintaining records, documents, and reports in an organised manner that allows them to be retrieved and reviewed when needed.

7.7.5 Monitoring and Review

This means conducting periodic review to ensure that policies and procedures are actually applied in practice and are not merely written documents.

7.8 Segregation of Duties and Authorities

Recommended Good Practice

One of the most important internal control rules is that the same person should not be responsible for all stages of the same process.

For example, in relation to financial disbursement:



One person requests the payment.



Another person reviews the supporting documents.



Another person approves the payment.



Another person executes the payment.



Another person reconciles or reviews the records.

Segregation of duties reduces the risk of error, misuse, unauthorised expenditure, and conflicts of interest. In small organisations where full segregation is not always possible, compensating controls should be applied, such as Board review, dual approval, periodic reconciliation, or external audit review.

7.9 Authority Matrix

Recommended Good Practice

An authority matrix is a practical tool that clarifies who has the authority to approve decisions within the organisation.

The authority matrix may include matters such as:

01 Approval of budgets;

02 Approval of expenditure;

03 Signature on bank accounts;

04 Approval of contracts;

05 Acceptance of donations;

06 Rejection or suspension of higher-risk donations;

07 Approval of partners;

08 Approval of activities outside the State;

09 Approval of public communications or fundraising content;

10 Reporting to the Ministry or competent authority;

11 Escalation of breaches or risk indicators.

The matrix should be proportionate to the size of the organisation and should be approved by the Board or relevant governing body. It should also be reviewed periodically or when there are changes in management, activities, or risk profile.

7.10 Management of Funds and Bank Accounts

Legal Obligation

Funds and bank accounts are among the most sensitive areas of governance. The organisation must ensure that its funds are held and managed through official accounts and in accordance with the requirements of the applicable legal and regulatory framework.

The organisation should ensure that:


Bank accounts are opened through official procedures.


The competent authority is notified of accounts and relevant changes where required.


Cash funds are deposited into the organisation's bank accounts.


Expenditure is made in accordance with the approved authority matrix.


Accounts are subject to periodic reconciliation.


Any foreign currency account is supported by the approval of the competent authority where required.

The use of personal accounts, informal channels, or undocumented financial arrangements should be avoided, as these practices increase the risk of loss, misuse, lack of traceability, and supervisory concern.

7.11 Use of Funds for Approved Purposes

Legal Obligation

The legal framework requires that the organisation's funds be spent in a manner that achieves the purposes for which it was established. The organisation may not enter into financial speculation or distribute any revenues or returns to members of its Board, founders, members of its general assembly, or employees.

The organisation may, after obtaining the approval of the competent authority, invest funds that exceed its needs in order to generate financial returns that support the achievement of its purposes, in accordance with the controls and procedures specified in the applicable Executive Regulation and relevant instructions.

The use of personal accounts, informal channels, or undocumented financial arrangements should be avoided, as these practices increase the risk of loss, misuse, lack of traceability, and supervisory concern.

Practical Impact

Each expenditure should be linked to one of the organisation's approved purposes. Any expenditure that may be understood as a personal benefit, distribution of returns, or use outside the approved purpose should be avoided.

7.12 Final Accounts and Annual Budget

Legal Obligation

The organisation should maintain final accounts and annual budgets in accordance with the applicable legal and regulatory requirements, including the requirements relating to audit, approval, and submission to the Ministry or competent authority where applicable.

The final accounts and budget are not only accounting documents. They are also governance tools that help the Board understand the organisation's financial position, sources of funding, expenditure patterns, commitments, and ability to continue implementing its approved activities.

The Board should review financial statements, budgets, and audit observations, and should ensure that any material weaknesses or repeated observations are addressed through corrective action.

7.13 Conflicts of Interest

Recommended Good Practice / Legal Obligation where applicable

A conflict of interest arises when a Board member, manager, employee, volunteer, partner, or related person has a personal, financial, professional, or other interest that may affect, or appear to affect, the impartiality of a decision made on behalf of the organisation.

Conflicts of interest may arise in relation to:

01 Procurement and contracting;

02 Partner selection;

03 Beneficiary selection;

04 Employment or volunteer appointments;

05 Acceptance of donations;

06 Use of the organisation's resources;

07 Board or committee decisions.

The organisation should maintain clear procedures for disclosing, recording, managing, and mitigating conflicts of interest. A person affected by a conflict should not participate in the decision where the conflict may influence the outcome.

7.14 Confidentiality and Data Protection

Recommended Good Practice / Legal Obligation where applicable

The organisation may process sensitive information relating to donors, beneficiaries, volunteers, employees, partners, and financial or operational matters. Such information should be protected and used only for legitimate purposes.

The organisation should ensure that access to personal or sensitive information is limited to those who need it for their work, and that staff and volunteers are aware of their confidentiality obligations.

This is particularly important where volunteers or partners have access to beneficiary data, donor information, financial records, or internal documents.

7.15 Volunteer Management from a Governance Perspective

Recommended Good Practice

Volunteers may be an important part of the organisation's work, but they should be managed within a clear governance framework.

The organisation should ensure that volunteers have clear roles, written instructions, appropriate training, and defined limits on their authority. Volunteers should not collect donations, use the organisation's name or logo, access sensitive data, or communicate with donors or beneficiaries beyond the scope of their assigned task and approved procedures.

Volunteer records, undertakings, task descriptions, and any breaches or observations should be maintained as part of the organisation's governance and compliance records.

7.16 Governance of Partnerships and Contracts

Recommended Good Practice

Partnerships and contracts may create operational, financial, reputational, and compliance risks. Therefore, the organisation should apply clear procedures before entering into partnerships or contracts.

These procedures should include:

01 Understanding the legal status of the partner or contractor;

02 Defining roles and responsibilities;

03 Documenting the purpose of the relationship;

04 Ensuring that the relationship is consistent with the organisation's objectives;

05 Approving the relationship through the appropriate authority;

06 Including reporting, documentation, and termination provisions where appropriate;

07 Monitoring implementation.

Partnerships should not be used to bypass licensing, donation, financial, or supervisory requirements.

7.17 Dealing with Breaches and Risk Indicators

Recommended Good Practice

The organisation should have clear procedures for dealing with breaches, weaknesses, complaints, supervisory observations, or risk indicators.

These procedures should clarify:

- Who receives the report or observation;
- How the case is recorded;
- Who reviews it;
- When it should be escalated;
- What corrective action is required;
- When the Ministry or competent authority should be consulted;
- How the case is closed and documented.

Ignoring breaches or risk indicators may increase the impact of the issue and may weaken the organisation's ability to demonstrate effective governance.

7.18 Internal Governance and Risk Committee

Recommended Good Practice

Depending on the size and nature of the organisation, it may be useful to establish an internal committee or assign a focal point responsible for governance, risk, and compliance matters.

The committee or focal point may help with:

- Reviewing key risks;
- Following up on policies and procedures;
- Reviewing risk indicators;
- Monitoring corrective actions;
- Preparing reports for the Board;
- Coordinating responses to requests from the Ministry or competent authority.

In smaller organisations, this function may be simplified, provided that responsibilities are clearly assigned and documented.

7.19 Governance and Compliance File

Recommended Good Practice

The organisation should maintain a governance and compliance file that brings together the key documents demonstrating the organisation's governance framework and practical implementation.

This file may include:

01 Licence, declaration, classification, and founding documents;

02 Articles of association;

03 Board and committee decisions;

04 Policies and procedures;

05 Authority matrix;
06 Financial statements and audit reports;
07 Bank account documentation;
08 Donation and fundraising records;
09 Partner and beneficiary records;
10 Volunteer records;
11 Risk assessment and risk indicator register;
12 Training records;
13 Supervisory correspondence and inspection reports;
14 Corrective action plans and follow-up evidence.

The purpose of the file is not to create unnecessary paperwork, but to ensure that the organisation can easily demonstrate its governance, compliance, and effectiveness when required.

7.20 Indicators of Weak Governance

Indicators of weak governance may include:

01 Absence of clear policies or procedures;

02 Decisions taken informally without documentation;

03 Concentration of all authorities in one person;

04 Use of personal accounts or informal financial channels;

05 Lack of segregation between approval, payment, and review;

06 Missing or incomplete records;

07 Weak Board oversight;

08 Failure to review financial or operational reports;

09 Unclear relationship with partners or volunteers;

10 Repeated supervisory observations without corrective action;

11 Lack of response to risk indicators or complaints;

12 Conflicts of interest that are not disclosed or managed.

The presence of one indicator does not necessarily mean that the organisation is in breach, but it should prompt review and corrective action.

7.21 Governance Self-Assessment Questions

The organisation may use the following questions to assess the strength of its governance:

- Are the organisation's legal status, licence, declaration, and classification clear and up to date?
- Are the roles of the Board and executive management clearly separated?
- Are core policies approved and applied?
- Is there an authority matrix for financial and operational decisions?
- Are bank accounts official and subject to review?
- Are funds used only for approved purposes?
- Are Board decisions documented?
- Are conflicts of interest disclosed and managed?
- Are volunteers and partners subject to clear controls?
- Are records organised and retrievable?
- Are risk indicators recorded and escalated?
- Are supervisory observations followed up?
- Can the organisation demonstrate how it protects its funds, beneficiaries, donors, and reputation?

7.22 Chapter Summary

Effective governance can be summarised in five practical rules:



Clear authorities: who decides, who approves, who implements, and who reviews.



Separate and documented funds: no personal accounts and no expenditure without supporting documents.



Reviewable records: minutes, reports, accounts, permits, and registers.



Risk oversight: assessment, follow-up, escalation, and corrective action.



Transparency with the competent authority: provision of data, and referral where matters are unclear.

Governance is therefore a practical tool that ensures the organisation achieves the public benefit purposes for which it was established, protects its resources and credibility, and supports the State's effectiveness in protecting the sector from abuse.

Core Internal Policies and Procedures

08

Core Internal Policies and Procedures

8.1 Purpose of this Chapter

This chapter aims to explain the importance of having written internal policies and procedures within Non-Profit Organisations, and how such policies help translate legal, regulatory, and supervisory requirements into clear and applicable operational practices.

Internal policies are not intended to create unnecessary administrative burdens. Rather, they are practical tools that help the organisation clarify responsibilities, standardise decision-making, protect funds and resources, manage risks, document actions, and demonstrate compliance and effectiveness.

The policies and procedures referred to in this chapter should be proportionate to the size of the organisation, the nature of its activities, its resources, its risk profile, and the complexity of its operations.

8.2 Why Does the Organisation Need Written Policies?

Written policies help the organisation move from general intentions to clear procedures that can be implemented, monitored, and reviewed.

They help answer practical questions such as:

01 Who is responsible for making a decision?

02 What approvals are required?

03 What documents must be retained?

04 When should a matter be escalated?

05 What should be done if a risk indicator arises?

06 How should donations, partners, beneficiaries, volunteers, and records be managed?

07 When should the Ministry or competent authority be consulted?

Written policies also help ensure continuity when personnel change, support training and awareness, and provide evidence during inspection, supervision, audit, or assessment.

8.3 Characteristics of a Good Internal Policy

A good internal policy should be clear, practical, proportionate, and capable of implementation.

It should:

- Identify the purpose of the policy.
- Define who is responsible for applying it.
- Explain the steps to be followed.
- Identify the documents or records that must be retained.
- Clarify approval and escalation requirements.
- Be consistent with the applicable laws, regulations, decisions, and instructions.
- Be proportionate to the size and risk level of the organisation.
- Be reviewed and updated periodically.

A policy should not be written in a complex manner that prevents staff or volunteers from understanding it. The objective is to make the organisation's procedures clear and applicable in daily work.

8.4 List of Core Internal Policies

Legal Obligation / Recommended Good Practice

Article (50) of Federal Decree-Law No. (50) of 2023 on the Regulation of Public Benefit Organisations requires Public Benefit Organisations to follow the rules of governance and sound administration, to have internal regulations covering procurement, financial affairs, human resources, and disciplinary measures, and to maintain a professional code of conduct.

Accordingly, the organisation should, at a minimum, have written internal regulations or an internal framework covering the following areas:



Procurement and contracting.



Financial affairs, revenues, and expenditures.



Human resources and staff affairs.



Disciplinary measures and internal breaches.



A professional code of conduct, including integrity, conflicts of interest, confidentiality, and the use of the organisation's name and resources.

In addition to these core requirements, and depending on the size of the organisation, the nature of its activities, and its level of risk, it is recommended that the internal regulations or internal procedures manual include policies or procedures addressing matters such as governance and delegation of authorities, risk management, donations, acceptance and rejection of donations, donor due diligence, partners and implementers, beneficiaries and the provision of assistance, financial management and disbursement, cash and donation boxes, voluntary work, data protection and confidentiality, internal reporting and escalation, record retention, training and awareness, use of the organisation's name and logo, and handling breaches and corrective actions.

Each policy does not need to be a long or standalone document, particularly in small or low-risk organisations. More than one topic may be combined within a single internal regulation or simplified procedures manual, provided that roles, authorities, and requirements are clear, applicable, documented, and reviewable.

8.5 Governance and Delegation of Authorities Policy

Purpose of the Policy

This policy defines the organisation's governance structure, decision-making levels, authorities, approval lines, and the separation of responsibilities between the Board of Directors, executive management, staff, committees, and any other relevant internal parties.

Core Elements

The policy should address:

01 Roles and responsibilities of the Board of Directors or governing body.

02 Roles and responsibilities of executive management.

03 Delegation of authorities.

04 Financial and operational approval limits.

05 Authority to sign contracts and official correspondence.

06 Approval of donations, partners, activities, and expenditure.

07 Escalation of material risks, breaches, or supervisory observations.

08 Documentation of decisions and approvals.

Practical Measure

The organisation should maintain an authority matrix approved by the Board or governing body. The matrix should identify who may approve key decisions, financial transactions, contracts, fundraising activities, partners, external activities, and escalation matters.

8.6 Risk Management Policy

Purpose of the Policy

This policy explains how the organisation identifies, assesses, manages, documents, and reviews risks associated with its activities, donations, partners, beneficiaries, volunteers, financial channels, and operating environment.

Core Elements

The policy should address:

- Definition of risk.
- Risk assessment methodology.
- Risk levels: low, medium, and high.
- Key risk factors.
- When the risk assessment should be updated.
- Who is responsible for preparing the assessment.
- Who approves the assessment results.
- What measures are required for each risk level.
- How decisions are documented.

Practical Measure

The organisation should maintain an institutional risk register that is updated periodically. The register should include the key risks, the level of each risk, the existing controls, the required actions, and the person responsible for follow-up.

8.7 Donations Policy

Purpose of the Policy

This policy regulates the collection, receipt, provision, and use of donations in compliance with the Donation Regulation Law and its Executive Regulation, in a manner that protects donors' funds and ensures that donations are used for their approved purposes.

This is particularly important because the Donation Regulation Law applies to any entity wishing to collect or provide donations in the State, including in free zones, and aims to regulate donations and protect donors' funds.

Core Elements

The policy should address:

- Whether the organisation is a licensed entity or requires authorisation.
- Permit requirements.
- Approved fundraising channels.
- Advertising and publicity for donations.
- Donations received through electronic or digital channels.
- In-kind donations.
- Cash donations.
- Administrative and operational expenses.
- Donation records and reports.
- Use of donations for the purposes for which they were collected.
- Handling unusual, conditional, anonymous, or unclear donations.
- Referral to the Ministry or competent authority where requirements are unclear.

Practical Measure

No fundraising campaign should be launched or advertised unless the legal basis, required permit or approval, purpose of the campaign, collection method, and reporting requirements have been verified.

8.8 Donation Acceptance and Rejection Policy

Purpose of the Policy

This policy sets out the criteria for accepting, suspending, reviewing, or rejecting donations, particularly where the donation is large, unusual, conditional, anonymous, unclear, or linked to a higher-risk donor, channel, partner, or beneficiary.

Core Elements

The policy should address:



Acceptance of low-risk small donations through official and approved channels.



Recording donations using the available information and in a manner proportionate to their nature and value.



Additional review of large, repeated, anonymous, or unusual donations.



No acceptance of large anonymous donations without appropriate verification.



No acceptance of conditional donations from an unknown or unclear source, particularly where the condition may affect the organisation's independence or direct funds outside the approved purpose.



Documentation of the reasons for accepting or rejecting a donation.



Referral to the competent authority where the required action is unclear.

Practical Measure

Where a donation raises risk indicators, the organisation should document the facts, suspend acceptance where appropriate, review the donor, purpose, condition, channel, and intended beneficiary, and escalate the matter internally before taking a final decision.

8.9 Donor Due Diligence Policy

Purpose of the Policy

This policy defines how the organisation collects, verifies, records, and reviews donor information in a manner proportionate to the level of risk.

Donor due diligence does not mean imposing the same requirements on all donors. Rather, it means applying a level of review that corresponds to the nature, value, purpose, channel, and risk profile of the donation.

Core Elements

The policy should address:

- Information required for low-, medium-, and high-risk donations.
- How to deal with anonymous or incomplete donations.
- How to deal with large or unusual donations.
- Conditional donations.
- Donations from legal persons.
- Donations linked to third parties.
- Donations from higher-risk jurisdictions or environments.
- Documentation and record-keeping requirements.
- When a donation should be escalated or rejected.

Practical Measure

For higher-risk donations, the organisation may request additional information about the nature and purpose of the donation, the legal status of a legal person donor, the authorised signatory where applicable, the reason for the donation or relationship with the organisation, the proposed beneficiary, the channel used, and any third party connected to the donation.

8.10 Partners and Implementers Policy

Purpose of the Policy

This policy regulates how the organisation selects, approves, contracts with, monitors, and terminates relationships with partners, implementers, suppliers, service providers, or any parties involved in implementing its activities or delivering assistance.

Core Elements

The policy should include:

- Definition of partner and implementer.
- Minimum information required before approval.
- Verification of legal status.
- Review of experience and capacity.

- Assessment of risk level.
- Approval authority.
- Contracting or memorandum of understanding requirements.
- Reporting and documentation requirements.
- Monitoring during implementation.
- Termination or suspension of the relationship where risk indicators arise.

Practical Measure

The organisation should maintain a partner file that includes the partner's legal documents, purpose of the relationship, approval decision, agreement or memorandum of understanding, reports, payments or resources provided, and evidence of implementation.

8.11 Beneficiaries and Provision of Assistance Policy

Purpose of the Policy

This policy regulates how the organisation identifies beneficiaries or beneficiary entities, determines eligibility, protects dignity and personal data, provides assistance, and documents delivery of services or resources.

Core Elements

The policy should address:

- Beneficiary eligibility criteria.
- How beneficiary information is collected and protected.
- Avoidance of discrimination or unjustified exclusion.
- Approval of assistance.
- Delivery method.
- Evidence of receipt or use.
- Handling complaints or disputes.
- Protection of sensitive information and humanitarian dignity.

Practical Measure

The organisation should retain sufficient evidence demonstrating that assistance or services reached the intended purpose or beneficiary category, without collecting unnecessary or excessive personal information.

8.12 Financial Management and Disbursement Policy

Purpose of the Policy

This policy regulates how the organisation manages revenues, expenses, bank accounts, payments, approvals, supporting documents, financial records, and reconciliation.

Core Elements

The policy should address:

- Approved bank accounts.
- Signature authorities.
- Payment approval procedures.
- Supporting documentation.
- egregation of duties.
- Bank reconciliations.
- Cash controls.
- Payments to partners, suppliers, and beneficiaries.
- Treatment of financial discrepancies.
- Reporting to the Board and competent authority where required.

Practical Measure

No expenditure should be made without an approved purpose, appropriate authority, and supporting documents. Personal accounts and informal financial channels should not be used

8.13 Cash and Donation Boxes Policy

Purpose of the Policy

This policy regulates the handling of cash and donation boxes, where applicable, in a manner that protects funds and ensures traceability.

Core Elements

The policy should address:

- When cash may be accepted.
- Approved locations and methods for donation boxes.
- Authorisation to open or manage boxes.
- Dual control requirements.
- Counting and reconciliation.
- Deposit into the official bank account.
- Recording and reporting.
- Handling shortages, discrepancies, or suspected misuse.

Practical Measure

Donation boxes and cash collections should be subject to documented controls and should not be managed by one person alone.

8.14 Conflict of Interest Policy

Purpose of the Policy

This policy regulates how conflicts of interest are identified, disclosed, recorded, managed, and mitigated in the organisation's decisions and activities.

Core Elements

The policy should include:

- Definition of conflicts of interest.
- Practical examples.
- Duty to disclose.
- Conflict of interest register.
- Preventing the interested person from participating in the relevant decision.
- Documenting the decision in the minutes.
- Annual review of disclosures by Board members and executive management.

Practical Measure

Donation boxes and cash collections should be subject to documented controls and should not be managed by one person alone.

8.15 Voluntary Work Policy

Purpose of the Policy

This policy regulates the acceptance, registration, task assignment, training, follow-up, and management of volunteers, and protects the organisation from misuse of volunteer status.

Core Elements

The policy should include:

- Conditions for accepting volunteers.
- Registration through approved channels.
- Acceptance of the Volunteer Charter.
- Written assignment of tasks.
- Training before the task is performed.
- Confidentiality and data protection.
- Professional conduct.
- Prohibition on fundraising without approval.
- Use of the organisation's name or logo.
- Return of entrusted items and badges.
- Handling breaches.

This policy is based on the legal framework governing voluntary work, which regulates volunteers, volunteer teams, and entities organising voluntary work, and

requires the organisation of voluntary work, its licensing, and the registration of volunteers and volunteering opportunities in accordance with the approved controls.

Practical Measure

The volunteer acceptance form should include an explicit undertaking not to collect donations, advertise donations, or use the organisation's name for this purpose except based on prior official approval and in accordance with approved procedures.

8.16 Data Protection and Confidentiality Policy

Purpose of the Policy

This policy aims to protect the data of donors, beneficiaries, volunteers, employees, partners, and any sensitive financial, administrative, or operational data. It is a complementary policy and may be integrated within the professional code of conduct or the relevant internal procedures.

Core Elements

- The policy should address:
- Types of data processed by the organisation.
- Persons authorised to access data.
- Purpose of data use.
- Confidentiality obligations.
- Protection of beneficiary dignity.
- Data sharing with partners.
- Retention and disposal of records.
- Handling data breaches or unauthorised access.

Practical Measure

Staff and volunteers who access sensitive data should sign a confidentiality undertaking and receive clear instructions on the permitted use and disclosure of such data.

8.17 Internal Reporting and Escalation Policy

Purpose of the Policy

This policy defines how to report breaches, risk indicators, suspicions, misuse of funds, misuse of the organisation's name, or any irregular conduct.

Core Elements

The policy should include:

- Who may report.
- What cases must be reported.
- To whom reports should be made.
- Protection of good-faith reporters.
- Documentation.
- Initial assessment.
- Escalation to senior management or the Board of Directors.
- Referral to the Ministry or competent authority where necessary.
- Corrective actions.

Practical Measure

An internal incident and breach register should be established. The register should include the incident, date, parties involved, action taken, final decision, and any internal or external escalation.

8.18 Record Retention Policy

Purpose of the Policy

This policy regulates the records the organisation must retain, where they are stored, the retention period, and who may access them.

Core Elements

The policy should address:

- Administrative records.
- Financial and accounting records.
- Donation records.
- Partner and beneficiary records.
- Volunteer records.
- Risk and incident records.
- Training records.
- Supervisory correspondence.
- Retention periods.
- Access rights.
- Secure storage and disposal.

Practical Measure

Retention periods vary according to the type of record and the applicable legislation or instructions. As a general rule, administrative records should be retained for no less than five years, while financial and accounting records should be retained for no less than ten years, unless the relevant legislation or instructions require a longer period. Donation-related accounting records should also be retained for no less than ten years in accordance with the Executive Regulation of the Donation Regulation Law.

8.19 Training and Awareness Policy

Purpose of the Policy

This policy regulates how the organisation trains Board members, employees, volunteers, and relevant partners on legal obligations, internal procedures, risk indicators, donation controls, volunteer obligations, and reporting mechanisms.

Core Elements

- The policy should include:
- Who should be trained.
- Training topics.
- Training frequency.

- Training records.
- Role-based training.
- Awareness messages.
- Review of training effectiveness.

Practical Measure

The organisation should maintain a training register that includes the topic, date, participants, trainer, materials used, and any evaluation or follow-up action.

8.20 Use of the Organisation's Name and Logo Policy

Purpose of the Policy

This policy regulates the use of the organisation's name, logo, identity, official channels, digital platforms, and public communications.

Core Elements

The policy should address:

- Who may use the organisation's name or logo.
- Approval of media or public content.
- Use of the name or logo by volunteers.
- Use of the name or logo by partners.
- Use in donation campaigns.
- Digital links and social media posts.
- Response to impersonation or unauthorised use.

Practical Measure

No person, volunteer, partner, or employee should use the organisation's name, logo, donation links, or public messages for fundraising or external communication unless this is approved through the official procedures.

8.21 Breaches and Corrective Actions Policy

Purpose of the Policy

This policy regulates how the organisation deals with breaches, supervisory observations, internal weaknesses, complaints, or risk indicators, and how corrective actions are planned, implemented, and documented.

Core Elements

The policy should include:

- Types of breaches or weaknesses.
- Initial review.
- Risk assessment.
- Corrective action plan.
- Responsible person.
- Timeline.
- Follow-up.
- Closure and documentation.
- Reporting to the Board or competent authority where required.

Practical Measure

Corrective actions should address the root cause of the issue, not merely the visible symptom. For example, if a document is missing, the corrective action should not only add the missing document, but also review why the documentation process failed.

8.22 Approval and Review of Policies

Recommended Good Practice

Policies should be approved by the Board of Directors or relevant governing body, or by the authority designated within the organisation's governance framework.

Policies should be reviewed periodically, and in particular when:

- The legal or regulatory framework changes.
- The organisation's activities change.
- A new fundraising channel is used.
- A new type of partner or beneficiary relationship is introduced.
- An incident, breach, or risk indicator arises.
- Supervisory observations are received.
- There are changes in the organisation's structure or risk profile.

The organisation should retain evidence of policy approval, review, and communication to relevant staff or volunteers.

8.23 Common Mistakes in Internal Policies

Common mistakes include:

- Having policies that are copied from other organisations and not adapted to the organisation's actual activities.
- Keeping policies that are not communicated to staff or volunteers.
- Writing policies that are too complex to implement.
- Not linking policies to legal or supervisory requirements.
- Not assigning responsibility for implementation.
- Not documenting decisions made under the policy.
- Not updating policies when circumstances change.
- Treating policies as formal documents rather than operational tools.

8.24 Chapter Summary

Internal policies and procedures are practical tools that help the organisation translate laws, regulations, supervisory expectations, and good practices into day-to-day action.

A strong internal policy framework should be clear, proportionate, documented, and applied in practice. It should help the organisation manage governance, donations, donors, partners, beneficiaries, volunteers, records, training, reporting, and risk indicators in a consistent and accountable manner.

The key message of this chapter is that policies are not valuable because they exist on paper, but because they guide decisions, prevent abuse, support transparency, and help the organisation demonstrate compliance and effectiveness.

Regulation of Donations: Collection, Receipt, and Provision

09

Regulation of Donations: Collection, Receipt, and Provision

9.1 Purpose of this Chapter

This chapter aims to explain the practical framework that Non-Profit Organisations and relevant entities should follow when collecting, receiving, providing, or advertising donations, in a manner that ensures compliance with the law, protects donors' funds, strengthens transparency, and prevents the misuse of donation channels or the organisation's status or name.

The chapter does not aim to restrict legitimate charitable, humanitarian, social, or public benefit activities. Rather, it aims to clarify the controls that help ensure that donations are collected, received, provided, and used through approved channels and for their intended purposes.

This chapter should be read together with the Donation Regulation Law, its Executive Regulation, and any decisions, circulars, or instructions issued by the Ministry or the competent authority.

9.2 Importance of Regulating Donations

Donations are one of the most sensitive areas in the work of Non-Profit Organisations because they involve funds or resources collected from the public, donors, or supporters for a charitable, humanitarian, social, or public benefit purpose.

Regulating donations helps achieve several objectives:

- Protecting donors' funds.
- Ensuring that donations are used for the purposes for which they were collected.
- Preventing misleading or unauthorised fundraising.
- Ensuring transparency in collection, receipt, disbursement, and reporting.
- Protecting the organisation's reputation and public trust.
- Reducing risks of abuse, including terrorist financing abuse.
- Enabling competent authorities to supervise donation-related activities effectively.

Accordingly, any activity involving donations should be managed through clear procedures, approved channels, documented records, and appropriate reporting.

9.3 What is Meant by Donations?

Legal Obligation

For the purposes of this Manual, donations include funds or assets collected, received, or provided for charitable, humanitarian, social, or public benefit purposes, whether in cash, in kind, movable or immovable, or through electronic or digital means, in accordance with the applicable legal definition under the Donation Regulation Law.

The legal definition of donations is broad and covers multiple forms of funds and assets of financial value. However, the acceptance, handling, use, or disposal of any form of donation must comply with the applicable restrictions, prohibitions, and requirements governing Non-Profit Organisations and donation-related activities, and must observe any approvals required from the competent authority where applicable.

The practical rule is that the organisation should not focus only on the form of the donation. It should also consider its purpose, source, channel, value, any conditions attached to it, the intended beneficiary, and whether the donation is consistent with the organisation's approved objectives and the applicable legal and regulatory requirements.

9.4 Who is Covered by Donation Regulation?

Legal Obligation

The Donation Regulation Law applies to any entity that wishes to collect or provide donations in the State, including in free zones.

Accordingly, donation regulation may apply to:



Licensed entities permitted by their establishing legislation, decrees, or decisions to collect, receive, or provide donations.



Authorised entities that receive a permit from the competent authority to collect, organise, or provide donations.



Public Benefit Organisations, associations, civil foundations, charitable or humanitarian entities, and other legal persons where they collect, receive, provide, or advertise donations.



Beneficiary entities that receive donations or assistance, to the extent relevant to verification, documentation, and reporting.



Any party involved in a donation campaign, donation channel, fundraising event, digital link, in-kind donation, or provision of assistance.

The mere fact that an organisation is non-profit or has a public benefit purpose does not automatically give it the authority to collect or advertise donations. The legal basis, permit, approval, or licence must always be verified before carrying out any donation-related activity.

9.5 Licensed Entities and Authorised Entities

Legal Obligation

The Donation Regulation Law distinguishes between licensed entities and authorised entities.

A licensed entity is an entity whose establishing law, decree, or decision permits it to collect, receive, or provide donations. Such entities may include charitable associations and certain federal, local, or civil institutions whose establishing instruments or applicable legislation grant them such authority.

An authorised entity is a legal person that does not have the authority to collect, receive, or provide donations by default, but obtains a specific permit from the competent authority to collect, organise, or provide donations in accordance with the law.

This distinction is important because not every Non-Profit Organisation is automatically a licensed entity for fundraising purposes. The organisation must verify whether it is legally authorised to collect or provide donations, or whether it must obtain a prior permit before carrying out any donation-related activity.

Where it is unclear whether the organisation is a licensed entity or requires a permit, the matter should be verified through the approved channels and procedures of the competent authority before collecting, receiving, advertising, or providing donations.

9.6 Prohibition on Fundraising by Natural Persons

Legal Obligation

The Donation Regulation Law prohibits natural persons from collecting donations, organising fundraising, or advertising donations outside the channels and entities licensed or authorised in accordance with the applicable legislation.

Accordingly, no individual may use personal accounts, personal social media pages, private links, cash collection methods, or any other individual channel to collect donations in the name of an organisation, campaign, beneficiary, humanitarian case, or charitable purpose, unless this is carried out through an approved legal framework and by an entity authorised to do so.

The organisation should ensure that its employees, members, volunteers, representatives, and supporters understand that personal initiatives to collect donations may create legal, financial, reputational, and supervisory risks.

9.7 Prohibition on Fundraising by Volunteers Without Approval

Legal Obligation

Volunteers and volunteer teams may not collect donations, allow donations to be collected, or advertise donations by any means except with prior approval from the Ministry and in accordance with the approved procedures.

This means that volunteering and fundraising must be clearly distinguished. A volunteer's participation in a humanitarian, social, awareness, or organisational activity does not automatically give the volunteer the authority to collect funds, receive donations, publish donation links, or use the organisation's name or logo for fundraising purposes.

The organisation should reflect this prohibition in volunteer instructions, volunteer undertakings, training materials, and any agreements with volunteer teams or partners involved in implementing activities.

9.8 When is an Activity Considered Fundraising?

Legal Obligation / Practical Guidance

An activity may be considered fundraising where it involves inviting the public, donors, supporters, members, companies, or any other persons to provide funds, in-kind resources, services, or other forms of support for a charitable, humanitarian, social, or public benefit purpose.

Fundraising may take many forms, including:

- Direct requests for donations.
- Public appeals through social media or websites.
- Donation links or electronic payment pages.
- Donation boxes.
- Charity events, exhibitions, markets, auctions, or charitable activities.
- Collection of in-kind donations.
- Corporate or institutional donation campaigns.
- Public messages that may reasonably be understood as requesting donations.
- Use of the organisation's name or logo to invite support.

The organisation should not assess fundraising only by the wording used. Even where the word "donation" is not used, a message or activity may still be considered fundraising if its practical purpose is to invite people to provide funds or resources.

9.9 Conditions for Granting a Permit

Legal Obligation

Where a permit is required, the organisation or authorised entity must comply with the conditions and requirements specified by the competent authority, the Donation Regulation Law, its Executive Regulation, and any approved procedures or forms.

Such conditions may relate to:

- The legal status of the applicant.
- The purpose of the fundraising.
- The target amount.
- The period of collection.
- The methods and locations of collection.
- The persons responsible for the collection process.
- The beneficiary entities or purposes.
- The advertising materials and public messages.
- The method of receiving and disbursing the funds.
- Reporting and closing requirements.

The organisation should not begin fundraising, advertising, publishing donation links, or collecting funds before ensuring that all required approvals or permits have been obtained.

9.10 Permit Application Procedures

Legal Obligation

Where a fundraising permit is required, the application should be submitted to the competent authority in accordance with the approved procedures and within the required timeframes.

The application should include complete and accurate information, including the purpose of the fundraising, the target amount, the collection period, the persons responsible for the process, the collection methods, the proposed beneficiary entities, the advertising materials, and any other information required by the competent authority.

The organisation should retain a complete file for each permit application, including:

- The application submitted.
- Supporting documents.
- Correspondence with the competent authority.
- The permit or approval issued.
- Any conditions attached to the permit.
- Approved advertising materials.
- Records of collection and expenditure.
- Reports submitted after completion of the campaign.The organisation should not begin fundraising, advertising, publishing donation links, or collecting funds before ensuring that all required approvals or permits have been obtained.

9.11 Duration and Extension of the Permit

Legal Obligation

A fundraising permit is linked to a specific period, purpose, and approved scope. Donations should not be collected outside the approved period or beyond the approved scope unless an extension, amendment, or additional approval has been obtained in accordance with the applicable procedures.

Where the organisation needs to extend the campaign, change the purpose, change the collection channel, increase the target amount, add a new beneficiary entity, or modify any material element of the campaign, it should verify whether prior approval or amendment of the permit is required.

The organisation should monitor the permit period and ensure that collection, advertising, reporting, and closure activities are carried out within the approved timeframe.

9.12 Advertising and Publicity for Fundraising

Legal Obligation

Advertising and publicity for fundraising are subject to the requirements of the Donation Regulation Law, its Executive Regulation, and the approvals issued by the competent authority.

Any public message that invites the public to donate or support a campaign may fall within the scope of donation advertising, whether it is published through traditional media, websites, social media, messaging applications, printed materials, public events, or any other channel.

The organisation should ensure that all donation-related advertising is:

- Approved before publication.
- Consistent with the permit or approval issued.
- Clear and not misleading.
- Linked to a specific and lawful purpose.
- Published through official and approved channels.
- Free from exaggerated, misleading, or emotionally exploitative language.
- Protective of the dignity and privacy of beneficiaries.
- Supported by accurate information on how donations will be used.

No employee, volunteer, partner, or third party should publish donation-related content in the name of the organisation unless this is approved through the organisation's official procedures.

9.13 Means of Collecting Donations

Donations must be collected through means and channels approved by the competent authority and consistent with the permit, approval, or legal status of the entity.

Approved means may include bank transfers, authorised electronic platforms, approved digital payment links, authorised donation boxes, charitable events, in-kind collection methods, or other methods permitted under the applicable procedures.

The organisation should ensure that every collection channel is:

01 Official and approved.

02 Linked to the organisation or the authorised campaign.

03 Capable of being traced and reconciled.

04 Supported by records from the bank, platform, or authorised collection mechanism.

05 Protected from misuse, impersonation, or unauthorised access.

The use of personal accounts, informal collection methods, unapproved digital links, or channels that cannot be reconciled with the organisation's records should be avoided.

9.14 In-Kind Donations

Legal Obligation / Recommended Good Practice

In-kind donations may include goods, equipment, supplies, food items, clothing, medical materials, or any other non-cash resources donated for charitable, humanitarian, social, or public benefit purposes.

The organisation should record in-kind donations in a manner that allows them to be traced from receipt to use or distribution.

The in-kind donation record should include, where applicable:

- Description of the donated items.
- Estimated value, where appropriate.
- Date of receipt.
- Donor details, where available.
- Purpose or intended use.
- Storage location.
- Distribution or use records.
- Beneficiary entity or beneficiary category.
- Any restrictions, conditions, or special handling requirements.

The organisation should apply additional review to high-value, unusual, conditional, or sensitive in-kind donations, or where the donor, source, purpose, or intended beneficiary is unclear.

9.15 Electronic and Digital Donations

Legal Obligation / Recommended Good Practice

Electronic and digital donation channels may provide efficiency, speed, and accessibility, but they also require clear controls because of the risks of impersonation, unauthorised links, unclear donors, rapid dissemination, and difficulty of control.

The organisation should ensure that electronic and digital donations are collected only through approved and official channels, and that any digital campaign, payment link, platform, webpage, or online message is approved before publication.

Controls over electronic and digital donations should include:

01 Use of approved platforms or official payment channels.

02 Linking each digital campaign to the relevant permit or approval where applicable.

03 Reviewing digital messages before publication.

04 Matching platform reports with the organisation's bank account and internal records.

05 Monitoring fake pages, unauthorised links, or impersonation attempts.

06 Recording digital donation data in a manner proportionate to the level of risk.

07 Escalating any unusual activity, suspicious link, or unauthorised campaign.

Where the use of a new digital channel, crowdfunding platform, or non-traditional mechanism is unclear, the organisation should verify the applicable requirements through the competent authority before use.

9.16 Cash Donations

Legal Obligation / Recommended Good Practice

Cash donations may present higher risks due to the possibility of loss, difficulty of traceability, challenges in verifying the source, and the risk of unauthorised use or incomplete records.

The organisation should only accept or handle cash donations where this is permitted and through approved procedures.

Controls over cash donations should include:

- Prior approval for cash collection where required.
- Use of authorised persons only.
- Dual control when receiving, counting, or transferring cash.
- Issuance of receipts where applicable.
- Recording the cash donation in the relevant register.
- Prompt deposit into the organisation's official bank account.
- Reconciliation between receipts, cash counted, bank deposits, and accounting records.
- Investigation and documentation of any shortage, discrepancy, or delay.
- Prohibition on using personal accounts or retaining cash outside approved arrangements.

The organisation should not treat cash as a routine or informal method of collection. Where alternative official banking or electronic channels are available, these should be preferred because they provide better transparency and traceability.

9.17 Administrative and Operational Expenses

Legal Obligation

The Executive Regulation of the Donation Regulation Law permits licensed non-governmental entities, subject to the prior approval of the competent authority, to deduct a percentage from donations to cover the administrative and operational expenses necessary for the fundraising process, in accordance with the percentages, conditions, and controls specified in the Regulation.

The organisation should not deduct any amount from donations for administrative or operational expenses unless this is permitted under the applicable legal and regulatory framework, and unless the required approval has been obtained from the competent authority where applicable.

Administrative and operational expenses should be clearly linked to the fundraising activity, recorded accurately, supported by documents, and included in the reports submitted to the competent authority where required.

9.18 Efficiency Measurement and Assessment System

Regulatory / Supervisory Requirement

The Executive Regulation provides for measuring the efficiency and assessing the performance of licensed entities and authorised entities that collect and provide donations, based on indicators that may include the percentage of fundraising costs compared to total donations, the degree of compliance with fundraising controls and procedures, the percentage of donations spent on the purposes for which they were collected, the comparison between the targeted amount and the amount actually collected, the percentage of beneficiary entities from which approval was obtained for information-sharing authorisations, and any other indicators agreed in coordination with local authorities.

This requirement is primarily a regulatory and supervisory tool used by the competent authority to measure the efficiency and compliance of entities that collect or provide donations. Its practical impact on licensed or authorised entities is that they should maintain the data, records, and reports necessary to demonstrate compliance with such indicators, including data on donation proceeds, fundraising costs, expenditure, beneficiary entities, relevant approvals, and supporting documentation.

9.19 Use of Donations for the Specified Purpose

Legal Obligation

Donations must be used for the purpose for which they were collected or approved. The organisation should not change the purpose of a donation, redirect it to another activity, use it for unrelated expenditure, or allocate it to a different beneficiary entity unless this is permitted under the applicable legal and regulatory framework and approved by the competent authority where required.

This principle is central to protecting donors' funds and maintaining public trust. A donor, member of the public, or competent authority should be able to understand why the donation was collected, how much was collected, where it was deposited, how it was spent, and how the organisation can demonstrate that the donation reached its intended purpose.

The organisation should maintain records linking each campaign or restricted donation to its approved purpose, collection channel, expenditure, beneficiary entity or beneficiary category, and final reporting.

9.20 Prohibitions Relating to Donations

Legal Obligation

The organisation should ensure that donation-related activities do not involve prohibited or unauthorised practices. In particular, the organisation should avoid:



Collecting, advertising, or calling for donations by natural persons outside the channels and entities licensed or authorised in accordance with the applicable legislation.



Collecting, receiving, or providing donations without a permit or approval where such permit or approval is required.



Using personal accounts, private links, unauthorised platforms, or unofficial channels to collect donations.



Launching fundraising campaigns or public appeals before obtaining the required approvals.



Using the organisation's name, logo, or public trust to collect donations for unauthorised purposes.



Allowing volunteers or volunteer teams to collect donations, allow donations to be collected, or advertise donations without prior approval.



Changing the purpose of donations or redirecting them to another activity or beneficiary without the required approval.



Accepting donations that are clearly linked to unlawful, misleading, unclear, or unauthorised purposes.



Failing to maintain donation records, reports, and supporting documentation.



Using donations in a manner that conflicts with the organisation's approved objectives, the permit issued, or the applicable legal and regulatory requirements.

9.21 Donation Records

Legal Obligation

The organisation should maintain accurate and organised donation records that allow the competent authority, the Board, auditors, and relevant internal functions to trace donations from receipt to use or distribution.

Donation records should include, as applicable:

- Date of receipt.
- Donation amount or description of in-kind donation.
- Collection channel.
- Donor information, where available and appropriate.
- Campaign or purpose linked to the donation.
- Permit or approval reference, where applicable.
- Bank deposit or platform report.
- Expenditure or distribution details.
- Beneficiary entity or beneficiary category.
- Supporting documents.
- Any conditions attached to the donation.
- Any review, suspension, rejection, or escalation decision.

Donation records should be retained for the period required under the applicable legislation and instructions. Donation-related accounting records should be retained for no less than ten years, unless a longer period is required.

9.22 Financial and Closing Reports for Campaigns

Legal Obligation

At the end of a fundraising campaign or donation-related activity, the organisation should prepare the required financial and closing reports in accordance with the applicable permit, approval, legal requirement, or instruction issued by the competent authority.

Such reports should include, where applicable:

- The approved purpose of the campaign.
- The target amount and the amount actually collected.
- Collection channels used.
- Administrative and operational expenses, where permitted.
- Amounts spent and remaining balances.
- Beneficiary entities or beneficiary categories.
- Evidence of disbursement or delivery.
- Any deviations from the original plan and their justification.
- Supporting documents and records.
- Any required approvals or correspondence with the competent authority.

Campaign closure should not be treated as a purely internal matter. Where the law, permit, or competent authority requires reporting, the organisation must comply with the reporting requirements within the prescribed timeframe.

9.23 Due Diligence on Donations and Donors

Recommended Good Practice / Legal Obligation where applicable

Due diligence on donations and donors should be applied in a risk-based and proportionate manner. This means that the organisation should not impose the same level of information requirements on all donors or all donations. Instead, the level of review should correspond to the value, nature, purpose, channel, conditions, and risk profile of the donation.

Low-risk small donations received through official and approved channels may require basic information and ordinary recording. Higher-risk donations, such as large, unusual, anonymous, repeated, conditional, or unclear donations, may require additional review before acceptance.

The organisation should consider the following:

- Is the donation consistent with the organisation's approved objectives?
- Is the donation received through an official and approved channel?
- Is the donation linked to a clear purpose?
- Is the donor known or reasonably identifiable where required?
- Are there any unusual conditions attached to the donation?

- Is there any third party connected to the donation?
- Is the proposed beneficiary or purpose clear?
- Are there any risk indicators requiring escalation?

The organisation should document the basis for accepting, suspending, reviewing, or rejecting higher-risk donations.

9.24 Handling Anonymous or Unclear Donations

Recommended Good Practice / Legal Obligation where applicable

Anonymous or unclear donations should be handled with caution, particularly where they are large, repeated, conditional, or received through unusual channels.

The organisation may accept small low-risk donations where they are received through official and approved channels, provided that they are recorded using the available information in a manner proportionate to their nature and value.

However, large anonymous donations, repeated anonymous donations, or donations with unclear source, purpose, condition, or channel should be subject to additional review before acceptance. The organisation should not accept large anonymous donations without appropriate verification, nor should it accept conditional donations from an unknown or unclear source where the condition may affect the independence of the organisation or direct funds outside the approved purpose.

Where uncertainty remains, the organisation should document the case, suspend acceptance where appropriate, and refer to the competent authority if the appropriate course of action is unclear.

9.25 Conditional Donations

Recommended Good Practice / Legal Obligation where applicable

A conditional donation is a donation where the donor attaches a condition to its use, such as directing it to a specific purpose, beneficiary, activity, partner, geographic area, or implementation method.

Conditional donations are not prohibited in all cases. However, they require careful review to ensure that the condition is lawful, clear, consistent with the organisation's approved objectives and classification, and compliant with the applicable permit, approval, and legal requirements.

The organisation may accept a conditional donation where:



The condition is lawful and clear.



The condition is consistent with the organisation's approved objectives and classification.



The condition does not conflict with the permit, approval, or applicable legal and regulatory requirements.



The condition does not direct funds or resources to an unclear person or entity.



The condition can be implemented, documented, and monitored.



The condition does not give the donor inappropriate control over the organisation's decisions, priorities, or implementation methods.



The condition does not result in unjustified discrimination or exclusion among beneficiaries.



The condition does not require the use of an untrusted or unauthorised channel, partner, or implementer.



The condition does not change the purpose of the donation or the beneficiary outside the approved or authorised scope.

The organisation should not accept conditional donations where the condition is unlawful, unclear, directs funds or resources to an untrusted or unclear person or entity, conflicts with the permit or approved purpose, undermines the organisation's independence, is difficult to implement or document, or includes a request to subsequently transfer funds or resources to an unspecified or unauthorised third party.

Where there is uncertainty or serious risk indicators, the organisation should document the case and refer to the competent authority before taking a final decision to accept or reject the donation.

9.26 Relationship Between Donations and Beneficiaries

Recommended Good Practice / Legal Obligation where applicable

Where donations are collected or allocated for the benefit of specific beneficiaries, beneficiary categories, or beneficiary entities, the organisation should ensure that the beneficiaries are consistent with the purpose of the donation and the relevant permit or approval.

The organisation should maintain adequate information to demonstrate that donations reached the intended purpose or beneficiary category. However, it should also protect the dignity and personal data of beneficiaries and should avoid collecting or disclosing unnecessary information.

Where the beneficiary is a legal person or beneficiary entity, the organisation should verify its legal status and the basis for providing support to it, in a manner proportionate to risk.

9.27 Relationship Between Donations and Partners

Recommended Good Practice / Legal Obligation where applicable

Where a partner, intermediary, service provider, or implementing entity is involved in collecting, managing, transferring, or distributing donations, the organisation should clearly define the role of that party and apply due diligence proportionate to the level of risk.

9.28 Risk Indicators in Donations

Recommended Good Practice

Donation-related risk indicators may include:

- A donation that is large or unusual compared to the organisation's normal activity.
- A donation received through an unofficial or unclear channel.
- A donor refusing to provide basic information where such information is required.
- A donation linked to an unclear or unrelated purpose.
- A condition requiring funds to be directed to an unclear person or entity.
- A request to transfer funds to a third party not included in the approved arrangement.
- Use of personal accounts, private links, or unauthorised platforms.
- Repeated anonymous donations that appear connected.
- Negative information relating to the donor, beneficiary, or partner.
- Pressure to accept or transfer the donation quickly without review.
- Inconsistency between the donor, purpose, channel, and proposed beneficiary.
- Donation records that cannot be reconciled with bank or platform records.

The presence of one indicator does not automatically mean that the donation is suspicious or prohibited, but it requires review, documentation, and, where necessary, escalation.

9.29 What Should the Organisation Do When a Risk Indicator Appears?

Recommended Good Practice

Where a risk indicator arises in relation to a donation, the organisation should take proportionate steps based on the nature and seriousness of the indicator.

Such steps may include:

- Requesting additional information about the donor or donation.
- Reviewing the purpose and any conditions attached to the donation.
- Verifying the legal status of a legal person donor, where relevant.
- Reviewing the channel used to provide the donation.
- Assessing whether the proposed beneficiary or partner is clear and appropriate.
- Referring the case to senior management or the relevant committee.
- Suspending acceptance of the donation until the review is complete.
- Rejecting the donation where uncertainty remains or serious indicators arise.
- Referring to the Ministry or competent authority where the appropriate action is unclear.
- Documenting the decision and the reasons for it.

The organisation should avoid accepting a higher-risk donation merely because it supports a good purpose if the surrounding circumstances remain unclear or inconsistent with the applicable requirements.

9.30 Fundraising Campaign File

Recommended Good Practice / Legal Obligation where applicable

The organisation should maintain a complete file for each fundraising campaign or donation-related activity.

The file should include, as applicable:

- Purpose of the campaign.
- Permit or approval issued.
- Target amount.
- Campaign period.
- Approved collection channels.
- Approved advertising materials.
- Persons responsible for the campaign.
- Records of amounts collected.
- Bank or platform reports.
- Administrative and operational expenses, where permitted.
- Expenditure and distribution records.
- Beneficiary entities or beneficiary categories.
- Reports submitted to the competent authority.
- Any risk indicators, incidents, or corrective actions.
- Closing report and supporting documents.

Maintaining a complete campaign file helps the organisation demonstrate transparency, traceability, and proper use of donations.

9.31 Self-Assessment Questions Before Launching a Fundraising Campaign

Before launching a fundraising campaign, the organisation should consider the following questions:

- Are we legally permitted to collect or advertise donations for this purpose?
- Do we require a permit or approval?
- Has the purpose of the campaign been clearly defined?
- Is the target amount realistic and justified?
- Are the collection channels official and approved?
- Have the advertising materials been reviewed and approved?
- Are the beneficiary entities or beneficiary categories clear?
- Are administrative or operational expenses permitted and approved?
- Do we have a system to record donations and reconcile them with bank or platform records?
- Do we have a plan for expenditure, reporting, and closing the campaign?
- Have responsibilities been assigned internally?
- Have volunteers, partners, or third parties been instructed not to collect or advertise donations unless authorised?
- Do we know when to refer to the competent authority if a matter is unclear?

9.32 Chapter Summary

The regulation of donations is one of the most important areas of compliance and risk management for Non-Profit Organisations.

The key practical messages of this chapter are as follows:

- Not every Non-Profit Organisation is automatically authorised to collect or advertise donations.
- The legal basis, permit, approval, and authorised channels must be verified before any fundraising activity.
- Donations must be collected, received, recorded, used, and reported in accordance with the applicable legal and regulatory requirements.
- Personal accounts, informal channels, unauthorised links, and misleading public appeals should not be used.
- Donations should be used for the purposes for which they were collected.
- Anonymous, large, unusual, conditional, or unclear donations should be reviewed in a risk-based and proportionate manner.
- Volunteers and third parties should not collect or advertise donations without prior approval.
- Each campaign should have a complete file containing approvals, records, reports, and supporting documents.
- Where requirements are unclear, the organisation should refer to the competent authority before proceeding.

By applying these principles, the organisation protects donors' funds, strengthens public trust, reduces risks of abuse, and demonstrates effective compliance with the donation regulatory framework.

Management of Funds, Accounts, Records, and Financial Reports

10

Management of Funds, Accounts, Records, and Financial Reports

10.1 Purpose of this Chapter

This chapter aims to explain the practical controls for managing the funds of Non-Profit Organisations, including bank accounts, cash, donations, disbursements, investment, accounting records, financial reports, final accounts, and oversight of the use of funds.

Sound financial management is one of the most important elements in protecting Non-Profit Organisations from abuse, as it ensures that financial and in-kind resources are used for the purposes for which the organisation was established, and that donors' and beneficiaries' funds are safeguarded, documented, and traceable.

10.2 Special Nature of the Organisation's Funds

Legal Obligation

The funds of an association are the property of the association itself. Its members have no personal right to such funds, and a member who withdraws or is dismissed has no right to claim any part of those funds, taking into account the special nature of the funds of social solidarity funds.

Practical Impact

This means that the organisation's funds:



Are not the personal funds of members, founders, or Board members.



May not be used for private benefit.



May not be distributed as returns or profits.



Must be used only to achieve the purposes for which the organisation was established.



Must be clearly separated from the funds of individuals or related parties.

10.3 Bank Accounts

Legal Obligation

The legal framework governing Public Benefit Organisations requires each association to have one or more bank accounts with national banks operating in the State. The organisation's cash funds must be deposited in its name in its bank accounts, and funds may not be spent before they are deposited into those accounts.

The organisation should ensure that its bank accounts are opened, managed, and updated through the approved procedures, and that any required certificates, approvals, or notifications are obtained from the competent authority.

Practical Requirements

The organisation should ensure that:

- All bank accounts are opened in the official name of the organisation.
- Bank accounts are not opened in the personal name of any member, employee, volunteer, founder, or Board member.
- Authorised signatories are approved and updated.
- The competent authority is notified of accounts and changes where required.
- Cash received by the organisation is deposited into its official bank accounts.
- Bank transactions are supported by appropriate documents.
- Bank statements are reviewed and reconciled periodically.

10.4 Use of Personal Accounts

Legal Obligation / Recommended Good Practice

The organisation should not use personal bank accounts to receive, hold, transfer, or disburse the organisation's funds, donations, or resources.

The use of personal accounts creates serious risks, including:

01 Loss of traceability.

02 Mixing personal funds with organisational funds.

03 Difficulty in demonstrating proper use of funds.

04 Risk of misuse or unauthorised control.

05 Weakness in audit and supervision.

06 Reputational and regulatory concerns.

Any funds belonging to the organisation, or collected in its name or for its purposes, should be processed only through official and approved accounts and channels.

10.5 Cash Funds

Legal Obligation / Recommended Good Practice

Cash presents higher risks because it may be lost, miscounted, misused, or difficult to trace. Therefore, cash should be managed through clear and documented controls.

Where cash is received, the organisation should ensure that:

- Receipt of cash is permitted under the applicable rules.
- Cash is received only by authorised persons.
- Receipts are issued where applicable.
- Cash is recorded immediately in the relevant register.
- Cash is counted under dual control where possible.
- Cash is deposited into the organisation's official bank account without undue delay.
- Cash is not spent before being deposited into the bank account.
- Any discrepancy, shortage, or delay is documented and reviewed.

Cash should not be treated as an informal or routine substitute for official banking channels.

10.6 Donation Boxes

Legal Obligation / Recommended Good Practice

Donation boxes, where used, should be subject to specific controls and should only be used where permitted and approved in accordance with the applicable legal and regulatory requirements.

Controls over donation boxes should include:

- Approval for placing the donation box.
- Identification of the location of the box.
- Numbering or labelling of boxes.
- Restricting access to authorised persons.
- Opening the box under dual control.
- Counting and recording the amounts collected.
- Depositing funds into the organisation's official bank account.
- Reconciling amounts collected with internal records.
- Documenting any shortage, discrepancy, or irregularity.

Donation boxes should not be managed informally or by one person alone.

10.7 Financial Disbursement

Legal Obligation / Recommended Good Practice

Financial disbursement should be carried out only for approved purposes, through approved channels, and based on proper documentation and authority.

Before any disbursement is made, the organisation should verify:

- The purpose of the payment.
- Whether the payment is consistent with the organisation's approved objectives and budget.
- The identity of the recipient.
- The supporting documents.
- The approval authority.
- The method of payment.

- Whether the payment is linked to donations, a campaign, project, contract, or beneficiary.
- Whether any additional approval is required.

No payment should be made without sufficient supporting documentation, clear approval, and proper recording in the accounts.

10.8 Use of Funds for the Organisation's Purposes

Legal Obligation

The organisation's funds must be used for the purposes for which the organisation was established, and in accordance with its articles of association, licence, declaration, classification, and applicable approvals.

The organisation should avoid any use of funds that may be interpreted as:

01 A private benefit.

02 Distribution of profits or returns.

03 Expenditure outside the approved purpose.

04 Support for an unauthorised activity.

05 Payment to an unclear or unrelated party.

06 Use of donations for a purpose other than the purpose for which they were collected.

Each disbursement should be linked to a clear purpose, supported by documents, and capable of being reviewed.

10.9 Investment

Legal Obligation

The association may, after obtaining the approval of the competent authority, invest funds that exceed its needs in a manner that generates financial returns to help it achieve its purposes, in accordance with the controls, procedures, and requirements specified in the Executive Regulation of Federal Decree-Law No. (50) of 2023 on the Regulation of Public Benefit Organisations and any decisions or instructions issued by the competent authority.

The organisation may not treat investment as an unrestricted authority or as an independent commercial activity. Investment must be linked to achieving the organisation's purposes, limited to funds that exceed operational needs and existing obligations, and carried out in accordance with approved procedures and approvals.

Proposed Practical Measure

Before entering into any investment, the organisation should:



Verify that the funds to be invested exceed operational needs and existing financial obligations.



Prepare a clear justification explaining the purpose of the investment, the source of the funds, and how the expected return supports the organisation's objectives.



Refer to the Executive Regulation and relevant decisions or instructions to identify the applicable controls and procedures.



Obtain the approval of the competent authority before implementing the investment, where required.



Submit the investment decision to the Board of Directors or the relevant internal authority, and document the decision, justification, and related approvals.



Assess investment risks, including loss, liquidity, reputational risk, and inconsistency with the organisation's purposes or non-profit nature.



Avoid financial speculation, high-risk investments, or any investment that is inconsistent with the organisation's purposes or approved controls.



Retain records and documents relating to the investment, returns, expenses, and related decisions.



Provide the competent authority with the necessary reports on a periodic basis, in accordance with the approved requirements and procedures.



Review the investment periodically to ensure that it continues to serve the organisation's purposes and complies with the controls and approvals issued.

10.10 Accounting Records for Donations

Legal Obligation

The organisation should maintain clear and organised accounting records for donations, in accordance with the Donation Regulation Law, its Executive Regulation, and any relevant instructions issued by the competent authority.

Donation accounting records should allow donations to be traced from receipt to use or distribution.

These records should include, where applicable:

- Donation amount or description of in-kind donation.
- Date of receipt.
- Collection channel.
- Campaign or purpose linked to the donation.
- Permit or approval reference.
- Bank deposit or platform report.
- Administrative and operational expenses, where permitted.
- Expenditure or distribution details.
- Beneficiary entity or beneficiary category.
- Remaining balance, where applicable.
- Supporting documents and reports.

Donation-related accounting records should be retained for no less than ten years, unless a longer period is required by applicable legislation or instructions.

10.11 General Financial Records of the Organisation

Legal Obligation / Recommended Good Practice

In addition to donation-related records, the organisation should maintain general financial records that reflect its overall financial position and operations.

These may include:

- General ledger.
- Revenue and expenditure records.
- Bank statements.
- Bank reconciliation records.
- Invoices and receipts.
- Contracts and purchase orders.
- Payroll records, where applicable.
- Asset registers.
- Budget records.
- Financial reports submitted to the Board or competent authority.
- Audit reports and management letters.

Financial records should be accurate, complete, organised, and capable of being reviewed by the Board, auditor, Ministry, competent authority, or any other authorised body.

10.12 Final Accounts and Annual Budget

Legal Obligation

The organisation should prepare its final accounts and annual budget in accordance with the applicable legal and regulatory requirements, and submit them to the competent authority where required.

The final accounts should reflect the organisation's revenues, expenses, assets, liabilities, and financial position. The annual budget should reflect the planned activities, expected revenues, expected expenditure, and financial priorities of the organisation.

The Board of Directors should review and approve the final accounts and budget in accordance with the organisation's governance framework. Any audit observations or financial weaknesses should be followed up through corrective actions.

10.13 Reports Related to Permits and Fundraising Campaigns

Legal Obligation

Where the organisation obtains a permit or approval for a fundraising campaign or donation-related activity, it should comply with the reporting requirements associated with that permit or approval.

Reports may include:

- Amounts collected.
- Collection channels used.
- Administrative and operational expenses deducted, where permitted.
- Amounts spent.
- Beneficiary entities or beneficiary categories.
- Remaining balances.
- Evidence of disbursement or delivery.
- Any deviations or issues encountered.
- Supporting documents and closing reports.

The organisation should retain a complete file for each fundraising campaign, including the permit, approved materials, records, reports, and correspondence with the competent authority.

10.14 Administrative and Operational Expenses

Legal Obligation

Where the applicable legal and regulatory framework permits the deduction of administrative and operational expenses from donations, such deduction must be made only within the approved limits and conditions, and after obtaining the required approval from the competent authority where applicable.

Administrative and operational expenses should be:

- Necessary for the fundraising process.
- Permitted under the applicable rules.
- Approved where required.
- Calculated within the authorised percentages.
- Supported by documents.
- Recorded separately.
- Included in the reports submitted to the competent authority where required.

The organisation should avoid deducting or using donation funds for administrative or operational purposes unless the legal basis and approval are clear.

10.15 Separation Between the Organisation's Funds and Restricted Donation Funds

Recommended Good Practice / Legal Obligation where applicable

The organisation should distinguish between its general funds and restricted donations collected or received for a specific purpose, campaign, beneficiary, or activity.

Restricted donations should not be used for general organisational expenses unless this is permitted by the applicable legal framework, the terms of the permit or approval, and the conditions attached to the donation.

The organisation should maintain records that allow each restricted donation to be linked to its purpose, expenditure, balance, and related reports.

10.16 Payments to Partners and Suppliers

Recommended Good Practice / Legal Obligation where applicable

Payments to partners, suppliers, service providers, or implementing entities should be made only where there is a clear legal or contractual basis, an approved purpose, supporting documents, and appropriate internal approval.

Before making a payment, the organisation should verify:

- The identity and legal status of the partner or supplier.
- The purpose of the payment.
- The contract, purchase order, memorandum of understanding, or approved arrangement.
- Evidence of services, goods, or implementation.
- The approved bank account of the recipient.
- Whether the payment is linked to a donation, campaign, project, or restricted fund.
- Any reporting or documentation obligations.

Payments should not be made to unclear third parties, personal accounts, or parties not included in the approved arrangement.

10.17 Payments to Beneficiaries

Recommended Good Practice / Legal Obligation where applicable

Where the organisation provides financial or in-kind assistance to beneficiaries or beneficiary entities, it should maintain sufficient records showing the purpose of the assistance, the basis of eligibility, the method of delivery, and evidence of receipt or use.

Payments or support to beneficiaries should be made in a manner that respects dignity, protects personal data, and avoids unnecessary disclosure of sensitive information.

Where assistance is provided through a partner or intermediary, the organisation should ensure that the partner maintains appropriate records and provides evidence of delivery, in accordance with the agreement and applicable requirements.

10.18 Bank Reconciliations and Periodic Review

Recommended Good Practice

Bank reconciliations are an important control to ensure that bank statements match the organisation's accounting records and that all receipts and payments are properly recorded.

The organisation should conduct periodic bank reconciliations to identify:

- Unrecorded deposits.
- Unrecorded payments.
- Duplicate entries.
- Delayed deposits.
- Unauthorised transactions.
- Bank charges or fees.
- Discrepancies between bank records and internal records.
- Transactions requiring further review.

Bank reconciliations should be reviewed by a person who is not solely responsible for initiating or executing payments, where possible. In smaller organisations, compensating controls such as Board review or external accountant review may be used.

10.19 Assets and Entrusted Items

Recommended Good Practice

The organisation should maintain a register of assets and entrusted items, including equipment, devices, vehicles, donation boxes, identification cards, official stamps, access tools, and any items provided to employees, volunteers, partners, or project teams.

The asset and entrusted items register should include:

- Description of the item.
- Identification or serial number, where applicable.
- Date of receipt or assignment.
- Person responsible.

- Location.
- Condition.
- Return date.
- Loss, damage, or disposal records.
- Approval for disposal or write-off.

Entrusted items should be returned when the task, employment, volunteering assignment, or partnership ends.

10.20 Handling Discrepancies, Shortages, or Losses

Recommended Good Practice

Any financial discrepancy, shortage, loss, or unexplained difference should be recorded, reviewed, and addressed promptly.

Examples include:

- Difference between cash counted and receipts issued.
- Difference between platform reports and bank deposits.
- Missing supporting documents.
- Unexplained bank transactions.
- Lost donation boxes or entrusted items.
- Delayed deposits.
- Missing invoices or receipts.
- Unclear payments to partners or beneficiaries.

The organisation should document the issue, assign responsibility for review, identify the cause, take corrective action, and escalate the matter to senior management, the Board, or the competent authority where required.

10.21 Financial Risk Indicators

Recommended Good Practice

Financial risk indicators may include:

- Use of personal accounts.
- Cash retained without clear justification.
- Payments without supporting documents.
- Repeated delays in depositing cash.
- Bank transactions that cannot be matched with records.
- Donations collected through unauthorised links or channels.
- Payments to unclear third parties.
- Payments to partners or suppliers without contracts or evidence of delivery.
- Unexplained discrepancies between campaign records and bank statements.
- Repeated audit observations.
- Unusual withdrawals or transfers.
- Pressure to make urgent payments without normal review.
- Missing records for donations or expenditure.
- Use of donation funds for purposes other than those approved.

The appearance of a financial risk indicator does not automatically mean that misuse has occurred, but it requires review, documentation, and, where necessary, escalation.

10.22 Role of the Board of Directors in Financial Oversight

Recommended Good Practice / Legal Obligation where applicable

The Board of Directors plays a central role in financial oversight. It should ensure that the organisation has appropriate financial controls, accurate records, approved budgets, and clear reporting mechanisms.

The Board should review:

- Budgets.
- Final accounts.
- Financial reports.
- Audit reports.
- Major donations and restricted funds.
- Material expenditure.
- Investment decisions.
- Bank account arrangements.
- Financial risk indicators.
- Corrective actions relating to financial observations.

The Board does not need to manage every financial transaction, but it should ensure that the financial management system is reliable, transparent, and subject to review.

10.23 Role of the External Auditor

Recommended Good Practice / Legal Obligation where applicable

The external auditor provides an independent review of the organisation's financial statements and may identify weaknesses in accounting records, internal controls, documentation, or compliance with financial requirements.

The organisation should cooperate with the external auditor, provide requested records and documents, review audit findings, and take corrective action in response to audit observations.

Audit findings should not be treated as a formality. They should be used to improve financial governance, strengthen controls, and reduce the risk of repeated weaknesses.

10.24 Retention of Supporting Documents

Legal Obligation / Recommended Good Practice

The organisation should retain financial and accounting supporting documents for the periods required by applicable legislation and instructions.

Supporting documents may include:

- Invoices.
- Receipts.
- Bank statements.
- Bank transfer confirmations.
- Contracts.
- Purchase orders.
- Donation records.
- Campaign reports.
- Partner reports.

- Beneficiary delivery evidence.
- Board approvals.
- Audit reports.
- Correspondence with the competent authority.

Administrative records should generally be retained for no less than five years, while financial and accounting records should generally be retained for no less than ten years, unless a longer period is required under applicable legislation or instructions. Donation-related accounting records should be retained for no less than ten years.

10.25 Financial Management Self-Assessment Questions

The organisation may use the following questions to assess the strength of its financial management:

- Are all bank accounts opened in the official name of the organisation?
- Are personal accounts prohibited for organisational funds or donations?
- Are authorised signatories approved and updated?
- Are cash receipts deposited into official bank accounts without delay?
- Are payments supported by documents and approvals?
- Are bank reconciliations carried out periodically?
- Are donation funds separated from general funds where required?
- Are campaign records complete and linked to bank or platform reports?
- Are administrative and operational expenses deducted only where permitted and approved?
- Are partner and supplier payments supported by contracts and evidence of delivery?
- Are beneficiary payments documented appropriately?
- Are investment decisions approved and reported as required?
- Are financial records retained for the required period?
- Are audit observations followed up through corrective actions?
- Can the organisation demonstrate how its funds were received, used, and monitored?

10.26 Chapter Summary

Sound financial management is a core element of protecting Non-Profit Organisations from abuse and demonstrating transparency and effectiveness.

The practical messages of this chapter are as follows:

- The organisation's funds belong to the organisation and may not be treated as personal funds.
- Funds must be used only for approved purposes.
- Bank accounts should be official, transparent, and subject to periodic review.
- Personal accounts and informal channels should not be used.
- Cash should be tightly controlled and deposited into official accounts.
- Disbursements should be approved, documented, and linked to clear purposes.
- Donations and restricted funds should be traceable from receipt to use.
- Investment should only be undertaken within the approved legal and regulatory framework and with the required approvals.
- Financial records and supporting documents should be retained for the required period.
- Financial risk indicators should be reviewed, documented, and escalated where necessary.
- The Board of Directors should exercise effective oversight over budgets, accounts, reports, audit findings, and corrective actions.

By applying these controls, the organisation can protect its resources, safeguard donors' funds, demonstrate accountability, and support confidence in the integrity and effectiveness of its work.

Partners, Beneficiary Entities, and Final Beneficiaries

11

Partners, Beneficiary Entities, and Final Beneficiaries

11.1 Purpose of this Chapter

This chapter aims to explain how Non-Profit Organisations should deal with partners, beneficiary entities, and final beneficiaries in an organised, transparent, and risk-based manner, to ensure that funds, resources, or services reach the intended purposes, and to prevent the misuse of the organisation, its resources, name, or programmes.

The management of partners and beneficiaries is particularly important where the organisation collects donations, provides assistance, implements programmes through other parties, distributes in-kind or financial resources, or carries out charitable, humanitarian, or social activities inside or outside the State.

This chapter also takes into account the terrorist financing risk indicators and typologies highlighted in the UAE Financial Intelligence Unit report on terrorist financing typologies and facilitators, particularly those relating to the use of intermediaries, local accounts, foreign non-profit organisations, corporate networks, unlicensed hawala, and dealing with higher-risk countries or parties. The report is used as a national source for understanding risks and indicators, and not as a standalone legislative text.

11.2 Who is a Partner?

Recommended Good Practice

For the purposes of this Manual, a partner means any entity, legal person, or implementing party with which the organisation deals in order to achieve one of its purposes, whether through:

- Implementing a programme or project.
- Distributing assistance.
- Providing services to beneficiaries.
- Managing a field activity.
- Providing a support platform or channel.
- Cooperating in a campaign or event.
- Providing technical or operational support.
- Representing the organisation before a third party.
- Receiving funds, resources, or in-kind materials to implement a specific purpose.
- Reaching beneficiary groups on behalf of the organisation.

A partner may be a government entity, a Public Benefit Organisation, an association, a civil foundation, a charitable entity, a company, a service provider, or an entity outside the State, depending on the nature of the activity and the approvals required.

11.3 Who is a Beneficiary Entity?

Legal Obligation

The Donation Regulation Law defines a beneficiary entity as any natural or legal person to whom donations and assistance are provided inside or outside the State.

Accordingly, a beneficiary entity may include:

- An individual or family.
- A Public Benefit Organisation.
- An association or civil foundation.

- A charitable or humanitarian entity.
- An institution providing services to an eligible group.
- An entity outside the State, where permitted and in accordance with the required approvals.
- Any party to whom donations or assistance are provided for a lawful purpose.

The fact that an entity is a "beneficiary" does not exempt the organisation from the duty to verify or document the relationship. The organisation must be able to demonstrate the reason for providing support, the method of providing it, its purpose, and its consistency with the permit or approved activity.

11.4 Who is the Final Beneficiary?

Recommended Good Practice

The final beneficiary is the person, group, community, or entity that ultimately receives the benefit or impact of the assistance, service, or programme.

The final beneficiary may include:

- A person in need.
- A family.
- A social group.
- Patients, students, or persons of determination.
- Volunteers or trainees.
- A local community.
- An entity providing a public service.
- A group benefiting from a cultural, educational, humanitarian, or social activity.

The practical distinction is that the beneficiary entity may be an intermediary or institution receiving support, while the final beneficiary is the person or group that should actually receive the benefit.

11.5 Why Do Partnerships and Beneficiaries Present Risk Exposure?

Recommended Good Practice / FATF Recommendations

Risks increase when the organisation does not implement the activity itself, when it relies on external parties, or when it is difficult to verify that resources have reached the specified purpose.

Key risks may include:

- Use of an unlicensed or untrusted partner.
- Transfer of funds to an entity unrelated to the purpose.
- Assistance not reaching eligible beneficiaries.
- Use of assistance for unauthorised purposes.
- Weak documentation or reporting.
- Intervention by unauthorised parties in beneficiary selection.
- Conflicts of interest in selecting partners or beneficiaries.
- Difficulty in verifying activities outside the State.
- Misuse of the organisation's name by the partner.

- Use of a partner or beneficiary entity as a front for another party.
- Existence of a third party directing the relationship without appearing in the agreement.
- Transfer of funds through informal channels or accounts not belonging to the partner.

The FATF Best Practices Paper emphasises that Non-Profit Organisations differ in their exposure to terrorist financing risks depending on their type, activities, and characteristics, and that measures should be focused, proportionate, and risk-based, rather than applied to all organisations or all relationships in the same way.

11.6 Partners and Intermediaries as Potential Facilitators

Risk Indicator / Based on National Analysis

When dealing with a partner, implementer, or beneficiary entity, the organisation should not look only at the licence or legal name. It should also understand whether that party operates as an intermediary, pass-through channel, or front for another party.

The UAE Financial Intelligence Unit report highlighted a number of terrorist financing typologies and facilitators, including the role of listed persons, foreign political extremists, family members, money movers or intermediary accounts, nominees in corporate structures, and certain professionals or corporate service providers abroad. The report also referred to typologies involving the movement and concealment of funds through financial institutions, unlicensed hawala, corporate networks, trade, virtual assets, and loan settlements.

Accordingly, partner due diligence should include a practical understanding of the following questions:

01 Who effectively controls the partner or the relationship?

02 Who requested the support or partnership?

03 Who will receive the funds or resources?

04 Is the bank account in the name of the partner itself?

05 Is there a third party directing the relationship?

06 Is the partner actually capable of implementing the activity?

07 Are there higher-risk parties, jurisdictions, or payment channels?

08 Can the delivery of support to the final beneficiary be evidenced?

11.7 Principle of Partner Due Diligence

Recommended Good Practice

Partner due diligence means that the organisation does not enter into a partnership or implementation relationship without sufficient knowledge of the other party, the nature of its work, its legal status, reputation, and ability to implement the agreed purpose.

Due diligence does not mean applying the same procedures to all partners. A low-risk partner may require simple verification, while a new, foreign, or higher-risk partner, or one dealing with funds, beneficiaries, or sensitive activities, may require deeper verification.

The purpose of due diligence is not to obstruct legitimate partnerships, but to protect the organisation from having its funds, resources, name, or programmes used for purposes other than those for which it was established.

11.8 Levels of Partner Due Diligence

11.8.1 Simplified Due Diligence

Simplified due diligence applies where the partner is known, local, licensed, and does not deal with sensitive funds or resources.

Proposed measures include:

- Verifying the legal name.
- Obtaining a copy of the licence or evidence of legal status.
- Identifying the purpose of the cooperation.
- Documenting the scope of cooperation.
- Identifying a point of contact.
- Retaining basic correspondence.

11.8.2 Standard Due Diligence

Standard due diligence applies where the partner implements part of an activity or programme, or deals with beneficiaries, resources, or data.

Proposed measures include:

- Verifying the licence or establishment instrument.
- Identifying authorised signatories.
- Reviewing previous experience.
- Signing a written agreement.
- Defining the budget or resources.
- Defining reporting requirements.
- Retaining implementation documents.
- Reviewing any potential conflict of interest.
- Ensuring that accounts or receipt channels are in the name of the partner or beneficiary entity.

11.8.3 Enhanced Due Diligence

Enhanced due diligence applies where risks are higher, such as:

- A new or unknown partner.
- A partner outside the State.
- A partner dealing directly with funds or assistance.
- A partner operating in a higher-risk environment or activity.
- A partner requesting the use of cash or unusual channels.
- The presence of unclear third parties or intermediaries.
- Negative indicators or unclear information.
- Multiple or rapid transfers that are inconsistent with the nature of the activity.

- The relationship being linked to foreign non-profit organisations of unclear status.
- Use of digital platforms, virtual assets, or payment channels that are difficult to trace.

Proposed measures include:

- Deeper review of the licence and governance.
- Verification of authorised persons and effective controllers where appropriate.
- Review of previous reports or activities.
- Requesting references or evidence of implementation.
- Including clear oversight conditions in the agreement.
- Milestone-based payments linked to implementation.
- Detailed financial and implementation reports.
- The organisation's right to review, visit, or request documents.
- Prohibiting the transfer of funds or resources to a third party without prior approval.
- Periodic review of the relationship.
- Referring to the Ministry or competent authority where matters are unclear.

11.9 Testing Partner or Beneficiary Entity Risk from a Terrorist Financing Perspective

Recommended Good Practice / Based on National and International Analysis

The organisation, particularly when dealing with partners or beneficiary entities in charitable, humanitarian, or donation-related activities, should apply a practical test that goes beyond the question: "Is the partner licensed?" It should also ask: "Could this partner or relationship be used to raise, move, conceal, or use funds unlawfully?"

This test is based on international practice, which recognises that the risk of abuse of Non-Profit Organisations varies according to activity, characteristics, and operating environment, and that measures should be focused, proportionate, and risk-based, rather than applied to everyone in the same way.

11.10 Minimum Partner File

The organisation should maintain a file for each important partner. The file should include:

- Full legal name.
- Licence or establishment instrument.
- Address and contact details.
- Names of authorised signatories or representatives.
- Names of key points of contact.
- Purpose of the partnership.
- Scope of work.
- Duration of the relationship.
- Value of funding or resources, if any.

- Approved bank account or receipt method.
- Contract or memorandum of understanding.
- Implementation plan.
- Reporting requirements.
- Evidence of disbursement, distribution, or completion.
- Due diligence results.
- Risk level.
- Any risk indicators or observations.
- Decisions on approval, renewal, or termination.
- Any correspondence with the Ministry or competent authority regarding the relationship.

11.11 Agreements and Memoranda of Understanding

Recommended Good Practice

The organisation should not rely on verbal understandings in important partnerships. The relationship should be documented in writing, especially where it involves funds, resources, beneficiaries, data, or use of the organisation's name.

The agreement or memorandum of understanding should include:

- Names of the parties.
- Purpose of the cooperation.
- Scope of work.
- Roles and responsibilities.
- Duration of the agreement.
- Funds or resources.
- Payment or delivery channels.
- Reporting requirements.
- Document retention requirements.
- Data protection and confidentiality.
- Use of the organisation's name and logo.
- Prohibition on fundraising in the organisation's name without approval.
- Prohibition on transferring funds or resources to a third party without approval.
- Prohibition on using personal accounts.
- Mechanism for dealing with breaches.
- Right to review or request documents.
- Right of termination.
- Requirements for compliance with laws and instructions.

11.12 Selection of Beneficiaries

Recommended Good Practice

Beneficiaries should be selected based on clear criteria that are internally defined, and not based on personal relationships, external pressure, or individual discretion.

Depending on the type of programme, possible criteria may include:

- Financial or social need.
- Belonging to the target group.
- Eligibility under the purpose of the programme.
- Priority based on the severity of need.

- Avoidance of unjustified duplication of benefits.
- Availability of required documents.
- Consistency of the assistance with the authorised purpose.
- Absence of unmanaged conflicts of interest

The organisation should avoid:

01 Selecting beneficiaries without criteria.

02 Unjustified intervention by members, employees, or partners.

03 Expenditure outside the approved purpose.

04 Providing assistance to relatives or related parties without disclosure and assessment.

05 Providing assistance outside the approved purpose.

06 Failing to document the reason for selection.

07 Accepting beneficiary lists from an external party without review.

11.13 Verification of Beneficiaries

Recommended Good Practice

Beneficiary verification does not need to be complex in all cases, but it should be appropriate to the nature of the assistance and the level of risk.

Simplified Verification

This is suitable for low-risk activities or general services, such as:

- Attending an awareness activity.
- Participating in a cultural programme.
- Receiving general educational materials.
- Standard Verification This is suitable for individual assistance or social programmes, such as:
- Verifying identity.
- Requesting supporting documents.
- Conducting a brief case assessment.
- Approval by the programme officer.
- Appropriate proof of receipt.

Enhanced Verification

This is suitable for high-value financial or in-kind assistance or higher-risk cases, such as:

- Deeper review of documents.
- Approval by an internal committee.
- Visit or field verification where needed.
- Periodic review.
- More detailed proof of receipt.
- Ensuring that there is no unjustified third party directing receipt or use.

11.14 Protecting the Dignity and Data of Beneficiaries

Recommended Good Practice

The organisation should recognise that beneficiaries are not merely "cases" or "numbers", but persons or groups with rights, dignity, and privacy.

Practical rules include:

- Collecting only the minimum necessary data.
- Using data only for the specified purpose.
- Storing files securely.
- Not publishing beneficiaries' images or stories without appropriate consent.
- Avoiding degrading or exploitative images in fundraising campaigns.
- Masking sensitive data in public reports.
- Restricting access to beneficiary files.
- Not sharing beneficiary lists with partners or third parties except for a legitimate purpose and under clear controls.

11.15 Evidence that Assistance or Services Have Reached the Intended Beneficiaries

Recommended Good Practice

The organisation should be able to demonstrate that assistance or services have reached the intended entity or target group.

Examples of appropriate evidence include:

- Receipts.
- Distribution lists.
- Implementation reports.
- Photographic evidence, with due regard to privacy.
- Reports from implementing partners.
- Beneficiary lists.
- Bank transfer evidence.
- Completion certificates.
- Visit reports.
- Impact assessment reports.
- Correspondence approving or closing the project.

The level of evidence should be proportionate to the value of the assistance, the sensitivity of the programme, the level of risk, and the nature of the beneficiaries.

11.16 Partners and Beneficiary Entities Outside the State

Recommended Good Practice / Requires Confirmation When Applied

Activities, assistance, or partnerships outside the State may involve higher risks due to differences in the legal environment, difficulty of verification, multiple intermediaries, and the possible presence of more sensitive geographic, political, or security factors.

The UAE Financial Intelligence Unit report also noted that certain typologies involving the movement and concealment of funds may involve external jurisdictions or entities, higher-risk neighbours, foreign non-profit organisations, crowdfunding channels, or transfers through different networks.

- When dealing outside the State, the organisation should:
- Ensure that the necessary approvals are in place.
- Verify the legal status of the partner or beneficiary entity.
- Use official financial channels.
- Clearly define the purpose and beneficiaries.
- Avoid informal transfers.
- Avoid the use of cash or personal accounts.
- Require implementation and financial reports.
- Retain evidence of distribution or use.
- Review any restrictions or instructions issued by the competent authorities.
- Ensure that there are no unclear third parties in the relationship.

Any activity, transfer, partnership, or provision of assistance outside the State should be subject to a review of official requirements and the necessary approvals from the Ministry, the competent authority, and any relevant government entities.

11.17 Partners in Voluntary Work

Legal Obligation / Recommended Good Practice

Where the organisation cooperates with partners to organise voluntary work or volunteering opportunities, it must observe the provisions of the Voluntary Work Law and its Executive Regulation, including the registration of volunteers and volunteering opportunities, licensing of voluntary work, and the obligations of entities organising voluntary work.

Important elements in volunteering partnerships include:

- Who is the organising entity?
- Who registers the volunteering opportunity?
- Who verifies the registration of volunteers?
- Who defines the tasks of volunteers?
- Who provides health and safety requirements and orientation?
- Who protects volunteer data?
- Who deals with breaches?
- Is there any fundraising?
- If fundraising exists, has prior approval from the Ministry been obtained?
- It should be emphasised that volunteers or volunteer teams may not collect donations, allow donations to be collected, or advertise donations by any means except with prior approval from the Ministry.

11.18 Conflicts of Interest in the Selection of Partners and Beneficiaries

Recommended Good Practice

Conflicts of interest may arise when selecting a partner, beneficiary, supplier, or implementer.

Examples include:

- A partner owned by a Board member.
- A supplier related to an employee.
- A beneficiary who is a relative of the programme officer.
- A volunteer directing assistance to persons connected to them.
- A Board member pressuring the organisation to select a specific entity.
- A partner proposing beneficiaries connected to it without disclosure.
- A beneficiary entity requesting that support be directed to parties connected to its management.

Proposed controls include:



Disclosure of the relationship.



Excluding the conflicted person from the decision.



Recording the case in the conflict of interest register.



Assessing the partner or beneficiary according to the ordinary criteria.



Obtaining approval from a higher authority where the relationship continues.



Independent review of sensitive cases.

11.19 Risk Indicators Related to Partners

The organisation should pay attention to the following indicators:

- The partner refuses to provide a licence or documents.
- The identity of those responsible for the partner is unclear.
- The partner requests transfers to a personal account.
- The partner requests transfers to an account that does not belong to it.
- The partner requests cash payment without justification.
- Multiple parties are involved in the relationship without clear justification.
- Implementation reports are not provided.
- Beneficiaries are unclear.

- Bank accounts or authorised persons change frequently.
- Visits or review are refused.
- Negative information exists about the partner.
- Pressure is applied for rapid implementation without verification.
- The partner's capacity is inconsistent with the size of the project.
- The partner requests use of the organisation's name or logo without controls.
- Multiple companies or entities are used without an apparent operational need.
- Funds or resources are quickly transferred to another party.
- There is a link to a higher-risk jurisdiction, region, or funding channel.
- Foreign non-profit organisations of unclear status are used as part of the relationship.
- Digital platforms, virtual assets, or unusual payment methods are requested without justification.

The existence of one indicator does not necessarily mean that abuse has occurred, but it requires verification, raising the level of due diligence, and documenting the decision.

11.20 Risk Indicators Related to Beneficiaries

Indicators may include:

- Inconsistent information in the assistance request.
- Repeated requests from the same person or family without justification.
- External interference in beneficiary selection.
- Refusal to provide basic information.
- Use of unclear or incomplete documents.
- Request to transfer assistance to a third party.
- Absence of evidence of receipt.
- Repeated complaints about distribution.
- Manipulation of beneficiary lists.
- Undisclosed relationship with an employee or volunteer.
- A party imposing names of beneficiaries without a clear basis.
- The beneficiary category does not match the authorised purpose.
- Distribution patterns are inconsistent with the objectives of the programme.

11.21 Dealing with Risk Indicators

Proposed Practical Measure

When a risk indicator arises in relation to a partner, beneficiary entity, or final beneficiary, the organisation should:

- Temporarily stop the procedure if continuing may increase the risk.
- Request additional information or documents.
- Review the file internally.
- Increase the level of due diligence where needed.
- Escalate the matter to management or the relevant committee.
- Document the indicator and the decision.
- Adjust the risk level.
- Take corrective action.
- Refer to the Ministry or competent authority where the matter is unclear or where there is a legal or regulatory issue.
- Update the risk register and the partner or beneficiary register.

11.22 Follow-Up of Partners After Contracting

Recommended Good Practice

Due diligence does not end when the agreement is signed. The partner should be followed up during and after implementation.

Follow-up tools may include:

- Periodic reports.
- Follow-up meetings.
- Disbursement documents.
- Evidence of distribution or implementation.
- Field visits where needed.
- Review of a sample of cases.
- Evaluation of the partner's performance after project completion.
- Documentation of lessons learned.
- Review of any complaints or risk indicators.
- Review of the partner's compliance with the prohibition on transferring resources to a third party without approval.

Follow-up questions include:

- Did the partner implement what was agreed?
- Were funds or resources used for the specified purpose?
- Did the partner provide the required reports?
- Did any risk indicators arise?
- Were there any complaints?
- Can delivery of support to the final beneficiary be evidenced?
- Should the relationship continue, be amended, or be terminated?

11.23 Termination of the Relationship with the Partner

Recommended Good Practice

The organisation should be able to terminate its relationship with a partner where there are serious reasons to do so.

Possible reasons for termination include:

- Use of funds for a purpose other than that agreed.
- Failure to provide reports.
- Refusal to permit review or verification.
- Provision of misleading information.
- Undisclosed conflict of interest.
- Serious legal or reputational risks.
- Breach of the agreement.
- Use of the organisation's name without approval.
- Fundraising without a permit or authorisation.
- Transfer of funds or resources to a third party without approval.
- Inability to evidence delivery of support to beneficiaries.
- Unclear relationship with higher-risk parties.

Upon termination, the organisation should document:

- Reason for termination.
- Remaining funds or resources.
- Required documents.
- Corrective actions.
- Whether the competent authority should be notified.
- Any restrictions on future dealings.
- Lessons learned to update due diligence procedures.

11.24 Register of Partners, Beneficiary Entities, and Final Beneficiaries

Recommended Good Practice

The organisation should maintain organised registers of partners, beneficiary entities, and final beneficiaries, according to the nature of the activity.

The partner register should include:

- Partner name.
- Type of partner.
- Licence or establishment instrument.
- Purpose of the relationship.
- Risk level.
- Agreement.
- Duration.
- Reports.
- Status of the relationship.
- Any risk indicators.
- Approval or termination decision.
- Risk level.
- Any observations or complaints.

The final beneficiary register may include, as needed:

- Case code or number.
- Beneficiary category.
- Eligibility criteria.
- Type of assistance.
- Date of provision.

- Evidence of receipt.
- Observations or complaints.
- Any conflict of interest or risk indicator.

Data protection should be observed and no more information than necessary should be collected.

11.25 Relationship of this Chapter to Recommendation 8 and the FATF Methodology

FATF Recommendations / Recommended Good Practice

This chapter helps the organisation apply one of the most important principles of Recommendation 8: protecting Non-Profit Organisations from abuse is not achieved by imposing general controls on everyone in the same way, but by understanding where risks actually exist.

The FATF Best Practices Paper emphasises that Recommendation 8 does not apply to the entire universe of non-profit entities in an absolute manner, and that countries and organisations should distinguish between risk levels and avoid treating all organisations as high risk without assessment. It also explains that disproportionate measures may lead to adverse consequences, such as disrupting legitimate activities or affecting access by organisations to financial services.

Accordingly, the organisation should apply stronger controls to higher-risk partnerships or beneficiary entities, while keeping procedures simpler and more proportionate in low-risk cases.

11.26 Self-Assessment Questions for Partners and Beneficiaries

The organisation may use the following questions:

- Do we know the legal status of the partner?
- Do we have a contract or memorandum of understanding?
- Have we defined the purpose and responsibilities?
- Do we know who is authorised to sign on behalf of the partner?
- Is the bank account in the name of the partner or beneficiary entity?
- Is there an unclear third party in the relationship?
- Have we conducted appropriate due diligence?
- Are we using official payment channels?
- Does the partner provide sufficient reports?
- Can we evidence the delivery of assistance?
- Are there clear criteria for selecting beneficiaries?
- Do we protect beneficiary data?
- Is there a complaints mechanism?
- Has any risk indicator appeared?
- Have decisions been documented?
- Do we need to refer to the competent authority?
- Is the relationship low, medium, or high risk?
- Should the risk assessment be updated based on this relationship?

11.27 Chapter Summary

Partnerships, beneficiary entities, and final beneficiaries are a central part of the work of Non-Profit Organisations. The more the organisation relies on external parties, the greater the need for due diligence, documentation, and follow-up.

The rules of this chapter may be summarised as follows:



No important partnership should be entered into without sufficient knowledge of the other party.



No funds or resources should be transferred without a clear purpose and documented agreement.



No transfers should be made to personal accounts or accounts that do not belong to the partner without a clear legal justification and appropriate approval.



Beneficiaries should not be selected without criteria.



Beneficiary data or images should not be used without controls.



The organisation should not rely fully on a partner without reports or evidence of implementation.



Risk indicators should not be ignored.



The organisation should understand who effectively controls the relationship and who benefits from it.



The relationship should be documented from the beginning through to closure.



The Ministry or competent authority should be consulted where matters are unclear, particularly in activities, partnerships, or assistance outside the State.

In this way, partnerships become a tool to enhance the organisation's impact, rather than a vulnerability that may be abused.

Donors, Contributors, and Due Diligence on Sources of Funding

12

Donors, Contributors, and Due Diligence on Sources of Funding

12.1 Purpose of this Chapter

This chapter aims to explain how Non-Profit Organisations should deal with donors, contributors, and sources of funding in a risk-based and proportionate manner, in order to protect the organisation, donors' funds, beneficiaries, and public trust.

The purpose of donor due diligence is not to create unnecessary barriers to legitimate donations, nor to treat all donors as high risk. Rather, it is to help the organisation understand the nature of the donation, its purpose, the channel through which it is received, any conditions attached to it, and whether there are indicators that require additional review before acceptance.

This chapter should be read together with the chapter on the regulation of donations, as well as the chapters on risk management, financial management, partners, beneficiaries, and risk indicators.

12.2 Importance of Donor Due Diligence

Donor due diligence is important because donations and funding sources may be misused if they are received from unclear sources, through unofficial channels, for unclear purposes, or with conditions that may affect the organisation's independence or direct funds outside the approved purpose.

01 Understand who is providing support, where this is required and proportionate.

02 Confirm that the donation is consistent with the organisation's approved objectives.

03 Ensure that donations are received through official and approved channels.

04 Identify large, unusual, anonymous, repeated, conditional, or unclear donations.

05 Prevent the misuse of the organisation's name, accounts, or donation channels.

06 Protect donors' funds and ensure their use for the intended purposes.

07 Document the reasons for accepting, suspending, reviewing, or rejecting donations.

08 Demonstrate transparency and effective risk management to the Ministry or competent authority.

Donor due diligence should be applied in a manner that is proportionate to the nature, value, purpose, channel, and risk profile of the donation.

12.3 Who is a Donor or Contributor?

For the purposes of this Manual, a donor or contributor means any natural or legal person who provides funds, in-kind resources, services, or any other form of support to the organisation, whether for a general purpose, a specific campaign, a programme, a beneficiary group, or a particular activity.

A donor or contributor may include:

- An individual.
- A company or private sector entity.
- A charitable or humanitarian entity.
- A Public Benefit Organisation.
- A foreign non-profit organisation, where permitted and subject to the applicable requirements.
- A partner providing funds or resources.
- A person providing in-kind donations or services.
- A person contributing through a crowdfunding or public campaign, where such channels are permitted and approved.

The level of information and review required for each donor should depend on the level of risk associated with the donation and the relationship.

12.4 What is Considered a Source of Funding?

A source of funding refers to the origin or channel through which the organisation receives financial or in-kind support. It may include:

- The organisation's own resources.
- Membership fees or subscriptions.
- Donations.
- Grants.
- Contributions from partners.
- Returns on approved investments.
- In-kind support.
- Approved fundraising campaigns.
- Support received through authorised digital or electronic channels.
- Any other source permitted under the applicable legal and regulatory framework.

Understanding the source of funding does not mean asking every donor intrusive questions about their personal wealth or financial affairs. Rather, it means that the organisation should understand, to a reasonable and proportionate extent, the nature of the support, the donor or contributing entity where relevant, the channel used, the purpose of the funds, and whether there are any indicators that require further review.

12.5 Risk-Based Donor Due Diligence Principle

Donor due diligence should be risk-based. This means that the organisation should not apply the same level of information and verification to every donor or donation.

Small, low-risk donations received through official and approved channels may require only basic recording of the available information. Medium-risk donations may require additional information such as the donor's name, contact details, purpose of the donation, payment method, and any conditions. Higher-risk donations may require additional review of the nature and purpose of the donation, the legal status of a legal person donor, the authorised signatory where applicable, the reason for the donation or relationship with the organisation, the proposed beneficiary, the channel used, and any third party connected to the donation.

The organisation should avoid two extremes: accepting all donations without review, and imposing excessive requirements on every donor regardless of the size and risk of the donation.

12.6 Levels of Donor Due Diligence

12.6.1 Simplified Due Diligence

Simplified due diligence may be appropriate for small, low-risk donations received through official and approved channels, especially where the donation is not conditional, not unusual, and not linked to a higher-risk activity or jurisdiction.

In such cases, the organisation may rely on the available information, including the amount, channel, campaign or purpose, and donor name where available.

12.6.2 Standard Due Diligence

Standard due diligence may be appropriate where the donation is of moderate value, linked to a specific purpose, made by a legal person, or includes conditions that require review.

In such cases, the organisation may collect and retain information such as the donor's name, contact details, capacity, purpose of the donation, payment method, and any conditions attached to the donation.

12.6.3 Enhanced Due Diligence

Enhanced due diligence may be appropriate where the donation is large, unusual, repeated, anonymous, conditional, received through an unusual channel, linked to a higher-risk jurisdiction or environment, made by a legal person of unclear status, or connected to a third party or beneficiary that is not sufficiently clear.

Enhanced due diligence may include:

- Requesting additional information on the nature and purpose of the donation.
- Reviewing the legal status of a legal person donor.
- Identifying the authorised signatory where applicable.
- Understanding the reason for the donation or the relationship with the organisation.
- Reviewing the proposed beneficiary or purpose.
- Reviewing the payment or collection channel.
- Identifying any third party connected to the donation.
- Referring the donation to senior management or the relevant committee.
- Suspending acceptance pending completion of review.
- Referring to the competent authority where the appropriate action is unclear.

12.7 Donor Information Required According to Risk

The organisation may apply the following indicative approach:

Risk Level	Suggested Information
Low	Name where available, donation value, channel used, purpose or campaign linked to the donation.
Medium	Name, contact details, capacity, purpose of the donation, payment method, and any conditions attached to the donation.
High	Additional information on the nature and purpose of the donation, legal status of the legal person where the donor is a legal entity, authorised signatory where applicable, reason for the donation or relationship with the organisation, proposed beneficiary, channel used, and any third party connected to the donation or its implementation.

Classifying a donation as higher risk does not mean that the donor must always be asked for broad information about the source of their personal funds. Rather, it means applying a higher level of review and documentation based on the nature, value, channel, and purpose of the donation, in a manner proportionate to the applicable legal and regulatory requirements and the organisation's approved procedures.

12.8 Large or Unusual Donations

Large or unusual donations should be reviewed before acceptance, particularly where they are inconsistent with the organisation's normal donation patterns, activities, donor profile, or expected funding sources.

A donation may be considered large or unusual due to:

- Its value compared to the organisation's usual donations.
- Its timing.
- Its channel.
- Conditions attached to it.
- The donor's profile or legal status.
- The proposed beneficiary.
- The request for rapid acceptance or transfer.
- The absence of sufficient information.
- The use of cash or an unofficial channel.
- Repetition of similar donations in a short period.

Possible actions include requesting additional information, reviewing the purpose, verifying the channel, referring the donation to senior management, suspending acceptance pending review, rejecting the donation where uncertainty remains, and documenting the decision.

12.9 Conditional Donations

Conditional donations are donations where the donor requires the funds or resources to be used in a specific way, for a specific purpose, by a specific partner, or for a specific beneficiary or beneficiary category.

Conditional donations may be accepted where the condition is lawful, clear, consistent with the organisation's approved objectives and classification, does not conflict with the permit or legal requirements, does not direct funds to an unclear or untrusted person or entity, can be implemented and documented, and does not give the donor inappropriate control over the organisation's decisions.

The organisation should not accept conditional donations where the condition is unlawful, unclear, inconsistent with the approved purpose, harmful to the organisation's independence, difficult to verify or document, or includes a request to transfer funds or resources to an unspecified or unauthorised third party.

Where uncertainty remains, the organisation should document the case and refer to the competent authority where the appropriate course of action is unclear.

12.10 Anonymous or Incomplete Donations

The organisation may receive donations for which limited information is available, particularly in public campaigns or electronic channels.

Small low-risk donations received through official and approved channels may be accepted and recorded using the available information, provided that this is proportionate to the nature and value of the donation.

However, large anonymous donations, repeated anonymous donations, or donations with incomplete or unclear information should be subject to additional review. The organisation should not accept large anonymous donations without appropriate verification, nor should it accept conditional donations from an anonymous or unclear source where the condition may affect the organisation's independence or direct funds outside the approved purpose.

The organisation should document the reasons for accepting, suspending, or rejecting anonymous or incomplete donations.

12.11 Crowdfunding and Public Campaigns

Crowdfunding and public campaigns can help mobilise support, but they also create additional risks because they may involve multiple donors, rapid dissemination, digital channels, and difficulty in identifying every contributor.

The organisation should ensure that crowdfunding and public campaigns are carried out only through authorised channels and in accordance with the applicable permit or approval requirements.

The organisation should maintain records of:

- The campaign purpose.
- The approved platform or channel.
- The permit or approval, where required.
- Amounts collected.
- Platform or payment reports.
- Donor information where available.
- Expenditure and distribution records.
- Beneficiary entities or beneficiary categories.
- Any unusual patterns or risk indicators.
- Closing reports.

Unauthorised crowdfunding, personal campaigns, or public appeals made in the organisation's name should not be permitted.

12.12 Donations Through Personal Accounts

Donations should not be collected, received, held, or transferred through personal bank accounts or personal digital accounts.

The use of personal accounts creates serious risks, including loss of traceability, mixing of personal and organisational funds, difficulty in demonstrating proper use of funds, risk of misuse, and regulatory concerns.

Any donation collected in the name of the organisation, or for one of its campaigns or purposes, should be received only through official and approved accounts and channels.

12.13 High-Value In-Kind Donations

High-value in-kind donations may include vehicles, equipment, devices, medical supplies, real estate, valuable goods, or other assets of significant value.

- The donation is consistent with the organisation's objectives.
- The donor and purpose are clear.
- The asset or item can be lawfully accepted and used.
- There are no unclear conditions attached to it.
- The organisation has the capacity to store, use, maintain, or distribute the item.
- The value is recorded where appropriate.
- The receipt, use, or distribution of the item can be documented.
- Any required approvals are obtained.

High-value in-kind donations should be recorded in a dedicated register and should be subject to appropriate oversight.

12.14 Donations Linked to Foreign Entities or Foreign Non-Profit Organisations

Donations linked to foreign entities or foreign Non-Profit Organisations may require additional review, particularly where the foreign entity is not well known, its legal status is unclear, it operates in a higher-risk environment, or the donation is linked to cross-border assistance, foreign partners, or external beneficiaries.

Before accepting such donations, the organisation should consider:

01 The legal status of the foreign entity.

02 The purpose of the donation.

03 The channel through which the donation is received.

04 Whether the donation is linked to a foreign partner or beneficiary.

05 Whether any approvals, permits, or coordination are required.

06 Whether the donation is consistent with the organisation's approved objectives and scope.

07 Whether there are any risk indicators or negative information.

Where the requirements are unclear, the organisation should refer to the Ministry or competent authority before accepting or using the donation.

12.15 Donations Through Virtual Assets or Crypto-Assets

Donations through virtual assets or crypto-assets may present higher risks due to volatility, anonymity or pseudonymity, difficulty of tracing, platform risks, and regulatory considerations.

The organisation should not accept donations through virtual assets, crypto-assets, or non-traditional digital mechanisms unless this is permitted under the applicable legal and regulatory framework and after obtaining the necessary guidance, approval, or confirmation from the competent authority.

Where such a donation is offered, the organisation should not proceed on an informal basis. It should document the case, suspend acceptance, and verify the applicable requirements through the approved channels.

12.16 Donations from Higher-Risk Jurisdictions or Areas

Donations from jurisdictions, areas, or environments that may be considered higher risk should be reviewed carefully, particularly where the donor, purpose, channel, or proposed beneficiary is unclear.

Higher risk may arise due to:

- Weak transparency.
- Conflict or instability.
- Sanctions exposure.
- Higher terrorist financing risk.
- Complex cross-border arrangements.
- Use of informal channels.
- Connection to unclear partners or beneficiary entities.

The organisation should not reject all donations from higher-risk areas automatically. Rather, it should apply a risk-based approach, conduct additional review where appropriate, document its decision, and refer to the competent authority where requirements are unclear.

12.17 Risk Indicators Related to Donors and Donations

Risk indicators related to donors and donations may include:

- A donor refusing to provide basic information where such information is required.
- A donation inconsistent with the donor's apparent profile or relationship with the organisation.
- A large or unusual donation with no clear purpose.
- A donor requesting anonymity despite the size or nature of the donation.
- A donor imposing conditions that direct funds to an unclear person or entity.
- A donation received through an unofficial or personal account.
- A request to transfer funds to a third party.
- A donation linked to a foreign entity of unclear status.
- Multiple donations that appear structured or connected.
- Negative information relating to the donor, beneficiary, partner, or intermediary.
- Pressure to accept or transfer the donation quickly.
- Repeated incomplete or inconsistent information.
- The use of cash where official channels are available.
- Donations linked to virtual assets or non-traditional channels without clarity.

The presence of one indicator does not automatically mean that the donation is suspicious or prohibited. It means that the organisation should review the case, document the facts, and take proportionate action.

12.18 Dealing with a Risk Indicator in a Donation

Where a risk indicator appears in relation to a donation, the organisation should respond in a structured and proportionate manner.

Possible actions include:

- Requesting additional information about the donation.
- Verifying the legal status of a legal person donor.
- Reviewing the purpose and any conditions attached to the donation.
- Reviewing the channel through which the donation is received.
- Assessing the proposed beneficiary or any third party involved.
- Referring the matter to senior management or the relevant internal committee.
- Suspending acceptance of the donation until the review is complete.
- Rejecting the donation where uncertainty remains or serious indicators arise.
- Referring to the Ministry or competent authority where the appropriate action is unclear.
- Documenting the decision and the reasons for it.

The organisation should not accept a donation where material uncertainty remains regarding its purpose, channel, conditions, or connected parties.

12.19 Rejection of Donations

The organisation should reject a donation where accepting it would conflict with the law, the organisation's approved objectives, the permit or approval issued, donor funds protection requirements, or the organisation's integrity and independence.

Grounds for rejection may include:

- The donation is linked to an unlawful purpose.
- The donor or purpose is unclear in a manner that cannot be resolved.
- The donation is conditional in a way that undermines the organisation's independence.
- The donation directs funds to an unclear person or entity.
- The donation requires use of an unauthorised channel or partner.
- The donation is received through a personal or unofficial account.
- The donation cannot be documented or monitored.
- There is serious negative information or risk indicators.
- Accepting the donation would expose the organisation to legal, supervisory, reputational, or operational risks.

The rejection decision should be documented, including the reasons, the persons involved in the review, and whether any referral to the competent authority was made.

12.20 Return of Donations

Where a donation has been received and is later found to be unacceptable, the organisation should consider whether the donation should be returned, suspended, transferred, or dealt with in accordance with instructions from the competent authority.

The organisation should not return or transfer funds in a way that creates additional risk, conceals the issue, or violates applicable legal or regulatory requirements.

Before returning a donation, the organisation should consider:

01 The reason for return.

02 Whether the donor is identifiable.

03 Whether the original channel can be used.

04 Whether the donation is linked to a legal or regulatory issue.

05 Whether the competent authority should be consulted.

06 How the return will be documented.

07 Whether the incident should be recorded in the risk or incident register.

Where the appropriate treatment is unclear, the organisation should refer to the Ministry or competent authority before taking action.

12.21 Donor and Donation Register

The organisation should maintain a donor and donation register proportionate to the nature of its activities and donation channels.

The register may include:

- Donor name, where available.
- Donor type.
- Contact details, where appropriate.
- Donation value or description.
- Date of receipt.
- Channel used.
- Campaign or purpose.
- Permit or approval reference, where applicable.
- Conditions attached to the donation.
- Proposed beneficiary or beneficiary category.
- Risk level, where relevant.
- Due diligence conducted.
- Decision to accept, suspend, reject, or return the donation.
- Supporting documents.
- Reports or evidence of use.

The register should be maintained in a manner that protects donor data and allows the organisation to demonstrate transparency and traceability.

12.22 Protection of Donor Data

The organisation should protect donor data and use it only for legitimate and authorised purposes.

Donor data should not be shared with third parties except where there is a lawful basis, donor consent where required, a regulatory requirement, or a legitimate operational need supported by appropriate controls.

Practical controls include:

01 Limiting access to donor data to authorised persons.

02 Storing records securely.

03 Avoiding unnecessary disclosure of personal information.

04 Protecting electronic records and donation platforms.

05 Ensuring that partners or service providers protect donor data.

06 Retaining donor data only for the required period.

07 Responding appropriately to unauthorised access or data breaches.

12.23 Role of the Board of Directors and Executive Management

The Board of Directors or governing body should ensure that the organisation has clear policies and procedures for accepting, reviewing, rejecting, and recording donations.

The Board or senior management should be involved in decisions relating to high-risk donations, large or unusual donations, conditional donations, donations linked to higher-risk jurisdictions, or donations where there are serious risk indicators.

Executive management should ensure that the procedures are applied, records are maintained, staff are trained, and risk indicators are escalated.

The organisation should not leave sensitive donation decisions to one person acting alone.

12.24 Self-Assessment Questions for Donors and Sources of Funding

The organisation may use the following questions:

- Do we know which donations are low, medium, or high risk?
- Are donations received through official and approved channels?
- Do we have procedures for large or unusual donations?
- Do we have procedures for anonymous or incomplete donations?
- Are conditional donations reviewed before acceptance?

- Do we document the reasons for accepting or rejecting higher-risk donations?
- Do we prevent the use of personal accounts?
- Do we review donations linked to foreign entities or higher-risk areas?
- Do we have a clear position on virtual assets or crypto-assets?
- Do we maintain a donor and donation register?
- Do we protect donor data?
- Are high-risk donations escalated to senior management or the Board?
- Do we know when to refer to the Ministry or competent authority?
- Can we demonstrate how donations were received, reviewed, accepted, rejected, or used?

12.25 Chapter Summary

Donors, contributors, and sources of funding are central to the work of many Non-Profit Organisations. Managing them properly helps protect the organisation, donors, beneficiaries, and public trust.

The key practical messages of this chapter are as follows:

- Donor due diligence should be risk-based and proportionate.
- Not all donors require the same level of review.
- Small low-risk donations through official channels may require simplified recording.
- Large, unusual, conditional, anonymous, repeated, or unclear donations require additional review.
- Donations should not be collected or received through personal accounts or unauthorised channels.
- Donations linked to foreign entities, higher-risk jurisdictions, virtual assets, or unclear third parties require particular caution.
- Conditional donations should be accepted only where the condition is lawful, clear, implementable, documented, and consistent with the organisation's approved objectives and applicable approvals.
- Donor data should be protected and used only for legitimate purposes.
- Sensitive donation decisions should be documented and escalated where appropriate.
- Where the correct course of action is unclear, the organisation should refer to the Ministry or competent authority before proceeding.

By applying these principles, the organisation strengthens transparency, protects donors' funds, reduces risks of abuse, and demonstrates that it manages funding sources in a responsible, proportionate, and effective manner.

Voluntary Work, Volunteers, and Volunteer Teams

13

Voluntary Work, Volunteers, and Volunteer Teams

13.1 Purpose of this Chapter

This chapter aims to explain how voluntary work should be organised within Non-Profit Organisations and relevant entities, in a manner that ensures that volunteering is organised, licensed, safe, documented, and consistent with the laws and regulations applicable in the United Arab Emirates.

The chapter also aims to protect the organisation, volunteers, and beneficiaries from risks associated with the misuse of volunteer status, the misuse of the organisation's name, uncontrolled access to beneficiaries, data, or resources, or the collection of donations without official approval.

This chapter is based on Federal Law No. (13) of 2018 on Voluntary Work, Cabinet Decision No. (70) of 2020 on the Executive Regulation of the Law, and the relevant provisions governing donations and Non-Profit Organisations.

13.2 Importance of Organising Voluntary Work

Legal Obligation / Recommended Good Practice

Voluntary work is one of the key elements of community work and the Non-Profit Organisation sector, as it enables individuals, teams, and entities to participate in serving society without financial or employment-related consideration.

However, voluntary work may also create operational, legal, reputational, and financial risks if it is not properly organised, particularly where volunteers interact with beneficiaries, donors, partners, funds, data, communication channels, or the organisation's name and logo.

Organising voluntary work helps the organisation to:

01 Ensure that volunteering opportunities are consistent with its approved objectives.

02 Confirm that volunteers and volunteer teams meet the applicable requirements.

03 Define the tasks and limits of authority of volunteers.

04 Protect beneficiaries, data, and resources.

05 Prevent unauthorised fundraising.

06 Document volunteer participation and volunteering hours.

07 Respond to breaches or risk indicators.

08 Demonstrate compliance with the Voluntary Work Law and its Executive Regulation.

13.3 Definition of Voluntary Work

Legal Obligation

The Voluntary Work Law defines voluntary work as any individual or collective activity, without financial or employment-related consideration, which aims to achieve a benefit for others.

Accordingly, voluntary work is characterised by the following elements:

01 It may be carried out individually or collectively.

02 It is performed without financial or employment-related consideration.

03 Its purpose is to achieve a benefit for others.

04 It must be carried out in accordance with the applicable legal and regulatory controls and conditions.

05 It must be licensed or registered in accordance with the approved requirements.

The organisation should not treat any unpaid participation as voluntary work automatically. The nature of the task, the organising entity, the platform or approval requirements, the beneficiaries, and the legal framework governing the activity should be considered.

13.4 Entities Organising Voluntary Work

Legal Obligation

Under the Voluntary Work Law, entities organising voluntary work include federal and local government entities, associations and civil foundations, and the private sector.

Accordingly, a Public Benefit Organisation, association, or civil foundation that organises a volunteering opportunity, uses volunteers, or establishes a volunteer team is considered an entity organising voluntary work and must comply with the applicable legal and regulatory controls.

The organisation should therefore identify, before launching any volunteering opportunity, whether it is acting as the organising entity, whether another party is organising the opportunity, and which party is responsible for registration, licensing, volunteer instructions, supervision, records, and reporting.

13.5 Scope of Application of Voluntary Work Provisions

Legal Obligation

The provisions of the Voluntary Work Law apply to:

- Voluntary work.
- Volunteers.
- Volunteer teams.
- Entities organising voluntary work.

This does not apply only to voluntary work inside the State. The organisation should also consider the controls applicable to any voluntary work outside the State, virtual volunteering, or volunteering organised through platforms or partners, as determined by the Executive Regulation and the instructions issued by the competent authority.

13.6 Registration and Licensing of Voluntary Work

Legal Obligation

The Voluntary Work Law provides for the establishment of a register at the Ministry for registering volunteers and volunteer teams, and prohibits the organisation of any voluntary work inside or outside the State unless it is licensed.

The Executive Regulation determines the controls, conditions, and procedures for registration and licensing. It also provides that registering and displaying a volunteering opportunity through the National Volunteering Platform, or any other platform affiliated with the competent authority, constitutes licensing of that opportunity.

Accordingly, before launching or announcing a volunteering opportunity, the organisation should verify:

01 Whether the opportunity must be registered or licensed.

02 Whether the opportunity is being displayed through the approved platform.

03 Whether the organisation has completed the required data and documents.

04 Whether volunteers are registered in accordance with the approved procedures.

05 Whether the opportunity is consistent with the organisation's approved objectives and classification.

06 Whether additional approvals are required due to the nature, location, beneficiaries, or risks of the activity.

13.7 Conditions for Natural Person Volunteers

Legal Obligation

Under the Voluntary Work Law, a natural person volunteer must be a citizen of the State or a resident, must not be less than eighteen Gregorian years of age, while allowing those below that age to volunteer with the approval of their guardian, must be of good conduct and behaviour, medically fit for the voluntary work assigned, licensed to practise the profession where volunteering is in the field of their profession, and registered to practise voluntary work.

The Executive Regulation also adds requirements such as accepting the Volunteer Charter, and having a professional licence, academic certificate, or experience certificate where the volunteering is specialised.

Practical Measure

Depending on the nature of the opportunity, the organisation should verify:

- Volunteer information.
- Registration through the approved channel.
- Age or guardian approval where needed.
- Fitness or suitability for the task.
- Qualifications or professional licence where the volunteering is specialised.
- Acceptance of the Volunteer Charter.
- Absence of an apparent conflict of interest.
- The volunteer's understanding of the tasks and limits of authority.

13.8 Legal Person Volunteers and Visiting Volunteers

Legal Obligation

The Executive Regulation determines the conditions and controls for volunteering by legal persons, as well as the conditions and controls for volunteering by persons visiting the State.

Where the organisation works with a legal person volunteer, a corporate volunteer programme, a visiting volunteer, or a volunteer group linked to an external entity, it should verify the applicable requirements before assigning tasks or allowing participation.

The organisation should not allow any person or entity to act in its name as a volunteer unless the relevant legal and procedural requirements have been verified.

13.9 Controls for Practising Voluntary Work

Legal Obligation

Voluntary work should be practised in accordance with the controls set out in the law, its Executive Regulation, and the instructions of the competent authority.

Practical controls include ensuring that the volunteering activity:

- Is consistent with the organisation's approved objectives and classification.
- Does not prejudice the security or safety of society.
- Does not cause harm to others, the environment, property, or privacy.
- Does not conflict with the laws, customs, or public order of the State.

- Is licensed by the Ministry or the competent authority where required.
- Avoids conflicts of interest or personal benefit.
- Does not involve the promotion of goods or services for personal gain.
- Respects the policies, systems, and regulations of the organising entity.
- Protects confidential information and data accessed during volunteering.
- Is implemented within the tasks and objectives defined for the volunteering opportunity.

13.10 Volunteer Charter

Legal Obligation

Acceptance of the Volunteer Charter is one of the key requirements for practising voluntary work under the Executive Regulation.

The Volunteer Charter helps clarify the expected conduct of volunteers and volunteer teams, including discipline, teamwork, compliance with instructions, respect for applicable legislation, confidentiality, and protection of the property and reputation of the organising entity.

The organisation should ensure that volunteers accept the Volunteer Charter before starting the task and should retain evidence of such acceptance as part of the volunteer file.

13.11 Defining Volunteer Tasks

Legal Obligation / Recommended Good Practice

The organising entity is required to define the tasks to be performed by the volunteer or volunteer team. This is an essential control because unclear tasks may lead to misuse of the organisation's name, unauthorised communication with beneficiaries or donors, access to data beyond the need for the task, or engagement in activities outside the approved opportunity.

For each volunteering opportunity, the organisation should define:

- The purpose of the opportunity.
- The tasks assigned to volunteers.
- The location and duration.
- The responsible supervisor.
- The persons or groups with whom volunteers may interact.
- Whether volunteers may access data, beneficiaries, resources, or systems.
- What volunteers are prohibited from doing.
- Reporting and escalation requirements.
- Health, safety, and confidentiality requirements.
- Return of entrusted items at the end of the task.

13.12 Prohibition on Fundraising by Volunteers Without Approval

Legal Obligation

Volunteers and volunteer teams are prohibited from collecting donations, allowing donations to be collected, or advertising donations by any means, except with prior approval from the Ministry and in accordance with the approved procedures.

This means that volunteer status does not grant authority to:

- Collect cash or in-kind donations.
- Publish donation links.
- Advertise fundraising campaigns.
- Request donations from the public.
- Receive funds on behalf of the organisation.
- Use personal accounts for donations.
- Use the organisation's name or logo to solicit support.
- Encourage third parties to collect donations.

The organisation should reflect this prohibition in volunteer instructions, training, undertakings, and any volunteer-related agreements or communications.

13.13 Use of the Organisation's Name and Logo by Volunteers

Recommended Good Practice / Legal Obligation where applicable

Volunteers may only use the organisation's name, logo, identity, badges, uniforms, cards, platforms, or official messages within the limits of the task assigned to them and in accordance with the organisation's approved procedures.

Volunteers should not:

01 Use the organisation's name outside the approved task.

02 Publish content in the organisation's name without approval.

03 Create pages, groups, links, or messages using the organisation's identity.

04 Communicate with donors or beneficiaries in a manner not authorised by the organisation.

05 Use the organisation's logo to collect or advertise donations.

06 Retain badges, IDs, or entrusted items after the volunteering task ends.

The organisation should issue clear instructions on the use of its name and logo and should recover any entrusted items after the completion of the volunteering opportunity.

13.14 Volunteers and Access to Beneficiaries

Recommended Good Practice

Where volunteers interact with beneficiaries, the organisation should ensure that such interaction is controlled, respectful, and limited to the purpose of the volunteering opportunity.

Controls may include:

- Defining the categories of beneficiaries with whom volunteers may interact.
- Providing instructions on appropriate conduct.
- Prohibiting unauthorised collection of personal information.
- Prohibiting unauthorised photography, recording, or publication of beneficiary stories.
- Ensuring that communication with beneficiaries is carried out through approved channels.
- Ensuring that volunteers do not select beneficiaries or distribute assistance without supervision.
- Establishing a mechanism for complaints or incident reporting.

Beneficiary dignity, privacy, and safety should be protected at all times.

13.15 Volunteers and Access to Data

Recommended Good Practice / Legal Obligation where applicable

Volunteers may, in some cases, have access to personal, operational, financial, beneficiary, donor, or partner data. Such access should be limited to what is necessary for the assigned task.

The organisation should ensure that:

- Volunteers access only the data needed for the task.
- Volunteers sign or accept confidentiality obligations.
- Data is not copied, transferred, photographed, or shared without approval.
- Personal devices are not used to store sensitive data unless permitted under approved controls.
- Access is withdrawn when the task ends.
- Any data breach or unauthorised access is reported and documented.

13.16 Volunteers and Access to Funds or In-Kind Resources

Recommended Good Practice / Legal Obligation where applicable

Volunteers should not have uncontrolled access to funds, donations, donation boxes, financial records, or valuable in-kind resources.

Where volunteers support activities involving in-kind resources, distribution, logistics, or storage, the organisation should define the role of volunteers and apply suitable controls, such as:

- Assigning a responsible staff member or supervisor.
- Recording items handed to volunteers.
- Using distribution lists or delivery records.
- Prohibiting volunteers from receiving cash donations.
- Prohibiting volunteers from using personal accounts or personal channels.
- Requiring return of entrusted items.
- Recording any shortage, loss, damage, or discrepancy.
- Escalating any risk indicator or breach.

13.17 Volunteers in Activities Outside the State

Legal Obligation / Requires Confirmation When Applied

Voluntary work outside the State may require additional controls and approvals, as determined by the Voluntary Work Law, its Executive Regulation, and the instructions issued by the Ministry or the competent authority.

Before allowing volunteers to participate in activities outside the State, the organisation should verify:



Whether the activity is permitted.



Whether the volunteering opportunity has been registered or licensed.



Whether approvals or coordination with the competent authority are required.



Whether the volunteers meet the applicable conditions.



Whether the partner or beneficiary entity outside the State has been verified.



Whether travel, safety, insurance, data, reporting, and supervision arrangements are clear.



Whether the activity involves donations, resources, or assistance.



Whether any higher-risk geographic, operational, or partner-related factors are present.

The organisation should not treat external voluntary work as an informal extension of local volunteering. It should be subject to additional review and documentation.

13.18 Virtual Voluntary Work

Recommended Good Practice / Legal Obligation where applicable

Virtual voluntary work may include activities performed through digital platforms, online meetings, remote support, communication channels, design, translation, mentoring, awareness activities, or technical assistance.

Although virtual volunteering may not involve physical presence, it may still create risks where volunteers access data, communicate with beneficiaries, publish content, manage digital channels, or use the organisation's name.

Controls over virtual volunteering should include:

- Defining the digital task clearly.
- Using approved communication channels.
- Limiting access to data and systems.
- Prohibiting the creation of unauthorised pages, links, or accounts.
- Prohibiting fundraising or donation advertising without approval.
- Protecting confidentiality and personal data.
- Retaining evidence of outputs, attendance, or hours.
- Recording any digital incident or misuse.

13.19 Volunteers as a Potential Risk Indicator

Recommended Good Practice

The use of volunteers may become a risk indicator where volunteering is not properly organised, where volunteers operate outside defined tasks, or where volunteer status is used to access funds, data, beneficiaries, or public trust without adequate controls.

Risk indicators may include:

- A volunteer collecting donations without approval.
- A volunteer publishing donation links or fundraising messages.
- Use of the organisation's logo or name outside the assigned task.
- A volunteer contacting beneficiaries outside approved channels.
- A volunteer requesting personal information from beneficiaries without authorisation.
- A volunteer refusing to follow instructions.
- A volunteer retaining entrusted items after the task ends.
- A volunteer attempting to influence beneficiary selection.
- A volunteer requesting payments, gifts, or personal benefits.
- A volunteer sharing confidential information or beneficiary images.
- A volunteer acting on behalf of an unclear third party.
- Repeated complaints about a volunteer or volunteer team.
- Participation of unregistered volunteers where registration is required.

The presence of one indicator does not automatically establish abuse, but it requires review, documentation, and proportionate action.

13.20 Obligations of the Entity Organising Voluntary Work

Legal Obligation

Entities organising voluntary work are required to comply with obligations under the Voluntary Work Law and its Executive Regulation.

These obligations include, in particular:

01 Providing health and safety requirements for volunteers and volunteer teams.

02 Insuring volunteers and volunteer teams during voluntary work where necessary.

03 Qualifying volunteers and volunteer teams through specialised introductory courses on voluntary work.

04 Defining the tasks required from the volunteer or volunteer team.

05 Providing the needs necessary for the volunteer or volunteer team to perform the task.

06 Maintaining the confidentiality of personal information relating to the volunteer or volunteer team.

07 Ensuring that volunteers and volunteer teams satisfy the registration requirements under the law.

The organisation should translate these obligations into practical steps in each volunteering opportunity file.

13.21 Obligations of Volunteers and Volunteer Teams

Legal Obligation

Volunteers and volunteer teams are required to comply with their obligations under the Voluntary Work Law and its Executive Regulation.

These obligations include, in particular:

- Discipline and working in a team spirit according to the requirements of voluntary work.
- Complying with all instructions issued to them and performing the assigned tasks.
- Complying with the Volunteer Charter.
- Complying with the laws in force in the State.
- Maintaining the confidentiality of information and data accessed during voluntary work.
- Updating personal data.
- Complying with the task and its objectives, respecting the policies, systems, and regulations of the organising entity, and safeguarding its property.
- Notifying the organising entity if they stop performing the voluntary work.
- Not displaying, providing, promoting, or advertising any goods or services during voluntary work for material benefit or personal gain.

- Returning all tools, equipment, devices, or entrusted items upon ompletion of the voluntary work.
- Complying with health and safety instructions.

The organisation should ensure that volunteers understand these obligations before starting the task.

13.22 Dealing with Volunteer Breaches

Recommended Good Practice

The organisation should have clear procedures for dealing with volunteer breaches, complaints, incidents, or risk indicators.

Such procedures should include:

- Recording the breach or incident.
- Temporarily suspending the volunteer's access to beneficiaries, data, funds, systems, or entrusted items where needed.
- Reviewing the facts.
- Obtaining the volunteer's explanation where appropriate.
- Escalating serious matters to management or the relevant committee.
- Taking corrective action.
- Recovering any entrusted items.
- Notifying the Ministry or competent authority where required or where the matter is unclear.
- Updating the volunteer record and risk register.
- Reviewing controls to prevent recurrence.

Examples of breaches may include collecting donations without approval, using the organisation's name without authorisation, disclosing confidential information, acting outside the assigned task, failing to return entrusted items, or violating beneficiary protection requirements.

13.23 Register of Volunteers and Volunteering Opportunities

Recommended Good Practice / Regulatory Requirement where applicable

The organisation should maintain a register of volunteers and volunteering opportunities.

The volunteer register should include:

- Name.
- Contact details.
- Registration number or evidence of registration.
- Opportunities in which the volunteer participated.
- Tasks assigned.
- Training or orientation provided.
- Acceptance of the Volunteer Charter.
- Any entrusted items or tools provided.
- Any observations or breaches.
- End date of the task.
- Training or orientation provided.
- Acceptance of the Volunteer Charter.
- Any entrusted items or tools provided.
- Any observations or breaches.
- End date of the task.

The volunteering opportunities register should include:

- Name of the opportunity.
- Purpose.
- Licence or registration.
- Date and location.
- Responsible person.
- Number of volunteers.
- Tasks.
- Risks and controls.
- Implementation report.
- Incidents or observations.

The register should be maintained in a manner that protects personal data and allows the organisation to demonstrate proper organisation and oversight of voluntary work.

13.24 Voluntary Work and Fundraising: Separating the Two Roles

Core Guidance Message

The organisation must clearly distinguish between:



A volunteer participating in a community, humanitarian, social, or organisational activity; and



A person or entity authorised to collect donations.

Volunteer status does not grant the right to collect funds, request donations, advertise donations, receive money, or use the organisation's name for fundraising purposes. Any confusion between the two roles may result in legal breaches and financial and reputational risks.

Practical Rule

Every volunteer should understand the following message:

> ***I am participating in a specific voluntary task. I do not have authority to collect donations, advertise donations, receive funds, or use the organisation's name for this purpose unless prior official approval has been obtained.***

13.25 Self-Assessment Questions for Voluntary Work

The organisation may use the following questions to assess the strength of its voluntary work controls:

- Is the volunteering opportunity registered or licensed?
- Does the opportunity fall within the organisation's approved objectives and classification?
- Are the volunteers registered?
- Have the volunteers accepted the Volunteer Charter?

- Have the tasks been clearly defined?
- Have volunteers been trained or briefed on the relevant instructions?
- Are volunteers aware that they may not collect or advertise donations without approval?
- Are volunteers' access to beneficiaries, data, systems, funds, or resources controlled?
- Is there a supervisor responsible for the opportunity?
- Are volunteer hours, attendance, and activities documented?
- Are entrusted items recorded and returned after the task?
- Are breaches, complaints, or risk indicators recorded?
- Are virtual or external volunteering activities subject to additional controls?
- Is there a clear distinction between volunteering and fundraising?
- Does the organisation know when to refer to the Ministry or competent authority?

13.26 Chapter Summary

Voluntary work is a valuable part of the work of Non-Profit Organisations, but it must be organised through clear legal, operational, and risk-based controls.

The key practical messages of this chapter are as follows:

- Voluntary work should be registered or licensed where required.
- Volunteers and volunteer teams should meet the applicable legal and procedural requirements.
- The organisation should define the tasks, limits of authority, and responsibilities of volunteers.
- Volunteers should accept the Volunteer Charter and receive appropriate orientation.
- Volunteers should not collect, allow the collection of, or advertise donations except with prior approval from the Ministry and in accordance with approved procedures.
- Volunteers' use of the organisation's name, logo, data, beneficiaries, funds, or resources should be controlled.
- The organisation should maintain records of volunteers and volunteering opportunities.
- Volunteer breaches and risk indicators should be recorded, reviewed, and escalated where necessary.
- External, virtual, specialised, or higher-risk volunteering should be subject to additional controls.
- The distinction between voluntary work and fundraising should be made clear to every volunteer.
- By applying these controls, the organisation can benefit from voluntary work while protecting volunteers, beneficiaries, donors, the organisation's reputation, and the wider sector from misuse or abuse.

Transparency, Records, Reports, and Disclosure to the Competent Authority

14

Transparency, Records, Reports, and Disclosure to the Competent Authority

14.1 Purpose of this Chapter

This chapter aims to explain the practical requirements and recommended practices relating to record-keeping, reporting, documentation of decisions, and disclosure to the Ministry or the competent authority upon request, or where there is a legal or regulatory requirement.

Transparency does not only mean publishing information to the public. It also means that the organisation is able to demonstrate that its activities, donations, partnerships, resources, volunteers, and decisions are managed in an organised, documented, and reviewable manner.

Records and reports are among the most important evidence of effectiveness, because they show that the organisation does not merely maintain written policies, but applies them in practice and can provide evidence when required.

14.2 Concept of Transparency in Non-Profit Organisations

Transparency means that the organisation maintains clear and reliable information about its legal status, activities, funds, decisions, beneficiaries, partners, volunteers, and reports.

In practice, transparency requires the organisation to be able to answer the following questions:

- What is the organisation authorised to do?
- What activities were implemented?
- What donations or resources were received?
- How were funds used?
- Who approved key decisions?
- Who were the partners or beneficiary entities?
- How were volunteers involved?
- What records support the organisation's decisions?
- What information was submitted to the Ministry or competent authority?
- Were risk indicators, breaches, complaints, or observations documented and followed up?

Transparency should be balanced with confidentiality, data protection, and beneficiary dignity. The organisation should maintain sufficient records for review and supervision without disclosing unnecessary personal or sensitive information.

14.3 Core Records of the Organisation

The organisation should maintain core records that demonstrate its legal status, governance, operations, financial management, and compliance.

These may include:

- Licence, declaration, classification, and founding documents.
- Articles of association or founding instrument.
- Board and committee meeting minutes.
- Authority matrix and delegation of authorities.
- Internal regulations, policies, and procedures.

- Financial records and accounting documents.
- Bank account records and authorised signatory documents.
- Donation and fundraising records.
- Partner and beneficiary entity records.
- Volunteer and volunteering opportunity records.
- Risk assessment and risk register.
- Incident, breach, and risk indicator records.
- Conflict of interest register.
- Training and awareness records.
- Supervisory correspondence and inspection reports.
- Corrective action plans and evidence of closure.
- Reports submitted to the Ministry or competent authority.

The purpose is not to create unnecessary paperwork, but to ensure that the organisation can demonstrate what it did, why it did it, who approved it, and what evidence supports it.

14.4 National Register of Non-Profit Organisations

The national register, or any register maintained by the Ministry or competent authority, is an important tool for documenting the legal status, classification, and key information of organisations.

The organisation should ensure that its registered information is accurate and up to date, including information relating to its name, address, legal status, classification, Board or authorised persons, branches, activities, and any other information required by the Ministry or competent authority.

Where there is any material change in the organisation's information, the organisation should verify whether notification, approval, or update of the register is required.

14.5 Governance Records

Governance records help demonstrate that the organisation is managed through clear decisions and documented oversight.

These records may include:

- Board meeting minutes.
- General assembly records, where applicable.
- Committee records.
- Decisions approving budgets, accounts, policies, and activities.
- Decisions approving partners, major donations, or higher-risk activities.
- Decisions relating to conflicts of interest.
- Decisions relating to breaches, observations, and corrective actions.
- Attendance records and voting records where applicable.
- Evidence of review of financial and operational reports.

Governance records should be sufficiently clear to show the decision taken, the date of the decision, the persons involved, the basis of approval, and any follow-up required.

14.6 Financial and Accounting Records

The organisation should maintain financial and accounting records that allow its funds, revenues, expenses, donations, assets, obligations, and financial position to be reviewed.

These records may include:

- Accounting books and ledgers.
- Revenue and expenditure records.
- Bank statements.
- Bank reconciliation records.
- Donation records.
- Invoices and receipts.
- Payment approvals.
- Contracts and purchase orders.
- Payroll records, where applicable.
- Asset registers.
- Audit reports.
- Final accounts and annual budgets.
- Reports submitted to the Board, auditor, Ministry, or competent authority.

Financial records should be complete, accurate, organised, and linked to supporting documents.

14.7 Final Accounts and Annual Budget

The final accounts and annual budget are key records that demonstrate the organisation's financial position, planned activities, and use of resources.

The organisation should prepare, approve, and submit final accounts and annual budgets in accordance with the applicable legal and regulatory requirements.

The Board of Directors or governing body should review these documents, follow up on audit observations, and ensure that the organisation's financial position is consistent with its approved objectives and activities.

14.8 Fundraising Campaign Reports

Where the organisation collects or receives donations through a campaign, permit, or approved activity, it should maintain complete campaign records and prepare the required reports.

Campaign reports may include:

- Purpose of the campaign.
- Permit or approval issued.
- Target amount.
- Amount actually collected.
- Collection channels.
- Administrative and operational expenses, where permitted.
- Amounts spent.
- Remaining balances.
- Beneficiary entities or beneficiary categories.
- Evidence of disbursement or delivery.
- Supporting documents.
- Any deviations, risk indicators, or corrective actions.

14.9 Activity and Programme Reports

The organisation should maintain reports on its key activities, programmes, and projects.

Activity and programme reports may include:

- Name of the activity or programme.
- Approved objective.
- Date and location.
- Responsible team.
- Partners involved.
- Beneficiary category.
- Resources used.
- Volunteers involved.
- Outputs or results.
- Evidence of implementation.
- Challenges, incidents, or observations.
- Lessons learned.
- Follow-up actions.

The level of reporting should be proportionate to the size, value, complexity, and risk level of the activity.

14.10 Volunteer and Volunteering Opportunity Records

The organisation should maintain records relating to volunteers and volunteering opportunities.

These may include:

- Volunteer registration information.
- Evidence of registration through approved channels where required.
- Volunteer Charter acceptance.
- Assigned tasks.
- Training or orientation records.
- Attendance and volunteering hours.
- Entrusted items or tools.
- Supervisor responsible for the opportunity.
- Incidents, complaints, or breaches.
- Evidence of closure of the volunteering opportunity.

Volunteer records help demonstrate that voluntary work is organised, documented, and subject to appropriate oversight.

14.11 Partner and Beneficiary Entity Records

The organisation should maintain records relating to partners, implementing entities, beneficiary entities, and final beneficiaries, as appropriate to the nature of the activity.

Partner records may include:

- Legal name and status.
- Licence or establishment document.
- Contact details.
- Authorised signatories or representatives.
- Purpose of the relationship.
- Agreement or memorandum of understanding.

- Due diligence results.
- Risk level.
- Reports and evidence of implementation.
- Payments or resources provided.
- Risk indicators, complaints, or observations.
- Renewal, suspension, or termination decisions.
- Beneficiary entity records may include:
- Name and legal status of the entity.
- Purpose of support.
- Amount or resources provided.
- Evidence of receipt or use.
- Reports or feedback.
- Risk indicators or complaints.

Final beneficiary records should be proportionate and should protect dignity and personal data.

14.12 Risk and Incident Register

The organisation should maintain a risk and incident register to record material risks, incidents, breaches, complaints, risk indicators, and actions taken.

The register may include:

- Date of the incident or indicator.
- Description of the issue.
- Area affected, such as donations, partners, volunteers, beneficiaries, finance, or data.
- Risk level.
- Person responsible for review.
- Immediate action taken.
- Escalation decision.
- Corrective action.
- Closure date.
- Evidence of closure.
- Whether the Ministry or competent authority was notified or consulted.

The risk and incident register helps the organisation demonstrate that it does not ignore risk indicators and that it takes proportionate action.

14.13 Conflict of Interest Register

The organisation should maintain a conflict of interest register to record disclosures made by Board members, management, employees, volunteers, partners, or other relevant persons.

The register may include:

01 Name of the person.

02 Nature of the interest.

03 Related decision or transaction.

04 Date of disclosure.

05 Action taken to manage the conflict.

06 Whether the person was excluded from the decision.

07 Approval or review by the Board or relevant authority.

08 Closure or follow-up action.

Maintaining a conflict of interest register helps protect the integrity of decisions and reduces the risk of private benefit, favouritism, or misuse of authority.

14.14 Complaints and Observations

Complaints, feedback, and observations may provide important information about weaknesses, risks, or potential misuse.

The organisation should maintain a mechanism for receiving, recording, reviewing, and responding to complaints and observations.

Records should include:

- Date of complaint or observation.
- Source of complaint, where appropriate.
- Subject matter.
- Person responsible for review.
- Action taken.
- Response provided, where applicable.
- Corrective action.
- Closure date.
- Any escalation to management, the Board, the Ministry, or the competent authority.

Complaints should not be dismissed merely because they are informal. Where they contain risk indicators or allegations of misuse, they should be reviewed and documented.

14.15 Disclosure to the Ministry or Competent Authority

The organisation should disclose information, reports, records, or documents to the Ministry or competent authority where required by law, regulation, permit, approval, circular, request, or supervisory procedure.

Disclosure may relate to:

- Licensing or registration information.
- Changes in governance, Board, or authorised persons.
- Financial statements and budgets.
- Donation and fundraising reports.
- Campaign closure reports.
- Records of activities or programmes.
- Partner or beneficiary information.
- Volunteer records.
- Risk indicators or breaches.
- Corrective action plans.
- Responses to inspection or supervisory observations.

Disclosure should be accurate, timely, complete, and supported by records.

14.16 When Should the Organisation Refer to the Ministry or Competent Authority?

The organisation should refer to the Ministry or competent authority where there is uncertainty, a legal or regulatory requirement, or a higher-risk issue requiring official guidance, approval, or notification.

- Unclear licensing or classification status.
- Launching a fundraising campaign where approval may be required.
- Accepting a large, unusual, conditional, or unclear donation.
- Using a new digital fundraising channel.
- Working with a foreign partner or beneficiary entity.
- Implementing activities outside the State.
- Receiving donations from outside the State where applicable.
- Dealing with virtual assets or non-traditional donation channels.
- Identifying serious risk indicators.
- Discovering unauthorised use of the organisation's name or logo.
- Receiving inspection observations or corrective action requirements.
- Uncertainty regarding what information may be disclosed or shared.

Referral should be documented, including the question raised, the response received, and any action taken.

14.17 Record Retention and Retention Periods

The organisation should retain records for the periods required by applicable legislation, regulations, instructions, permits, or supervisory requirements.

As a general rule, administrative records should be retained for no less than five years, while financial and accounting records should be retained for no less than ten years, unless the applicable legislation or instructions require a longer period.

Donation-related accounting records should be retained for no less than ten years in accordance with the requirements applicable to donation records.

Records should not be destroyed, deleted, or altered while they are subject to review, audit, inspection, investigation, dispute, or corrective action.

14.18 Quality of Records

Record quality is as important as the existence of records. A record that is incomplete, inconsistent, or difficult to retrieve may not be sufficient to demonstrate compliance or effectiveness.

Good records should be:

- Accurate.
- Complete.
- Dated.
- Linked to the relevant activity, donation, partner, beneficiary, or decision.
- Supported by documents.
- Organised and retrievable.
- Protected from unauthorised alteration.
- Consistent with reports submitted to the Ministry or competent authority.
- Retained for the required period.

The organisation should periodically review the quality of its records and correct weaknesses where identified.

14.19 Digital Transformation and Electronic Records

The organisation may maintain electronic records, digital files, and automated systems, provided that they are reliable, secure, accessible, and capable of being reviewed.

Electronic records should be protected through appropriate controls, such as:

- Access rights.
- Password protection.
- Backup.
- Audit trails where available.
- Protection against unauthorised modification.
- Secure storage.
- Clear file naming and indexing.
- Retention in accordance with required periods.
- Ability to retrieve and provide records upon request.

Digital transformation should improve transparency and record quality, not create fragmented or uncontrolled records across personal devices, informal messaging applications, or unmanaged storage systems.

14.20 Public Disclosure and Transparency with the Public

Public transparency may help strengthen trust in the organisation and the wider sector. However, public disclosure should be balanced with confidentiality, beneficiary dignity, donor privacy, data protection, and legal requirements.

Public disclosure may include:

- General information about the organisation.
- Approved objectives and areas of work.
- Summary of activities and programmes.
- Public annual reports.
- General financial information where appropriate.
- Information on major campaigns or initiatives.
- Impact stories presented in a respectful and lawful manner.

The organisation should avoid publishing sensitive beneficiary information, personal data, donor information, internal risk assessments, or confidential supervisory correspondence unless disclosure is lawful, appropriate, and approved.

14.21 Common Record-Keeping Mistakes

Common mistakes include:

- Maintaining records in scattered files without a clear structure.
- Keeping records only with one employee or volunteer.
- Using personal email accounts or personal devices for official records.
- Not linking donations to the relevant campaign or purpose.
- Not keeping evidence that assistance reached beneficiaries.

- Not retaining partner reports.
- Not documenting decisions or approvals.
- Not keeping Board or committee minutes.
- Not recording risk indicators or corrective actions.
- Submitting reports that are inconsistent with internal records.
- Destroying or deleting records before the end of the retention period.
- Not protecting electronic records or access rights.

These weaknesses may not always indicate misuse, but they reduce the organisation's ability to demonstrate compliance, transparency, and effectiveness.

14.22 Self-Assessment Questions for Records and Reports

The organisation may use the following questions:

- Do we know which records we are required to keep?
- Can we retrieve key records quickly?
- Are our records consistent with the reports submitted to the competent authority?
- Do we maintain an updated donation register?
- Do we maintain complete partner files?
- Can we prove that assistance or services reached the intended purpose?
- Do we maintain records of volunteers and volunteering opportunities?
- Do we know how to respond to a data request from the competent authority?
- Do we maintain a register of observations and corrective actions?
- Do we review the root cause of observations?
- Do we verify whether corrective actions are effective?
- Does the Board review material observations?
- Do we use national risk indicators in our internal reviews?
- Do we classify observations by seriousness?
- Do we know when immediate escalation is required?
- Do we refer to the Ministry or competent authority where matters are unclear?

14.23 Chapter Summary

Transparency, records, reports, and disclosure are essential to demonstrating that the organisation is operating properly, lawfully, and effectively.

The key practical messages of this chapter are as follows:

01 Transparency means having reliable, organised, and reviewable records.

02 Records should cover legal status, governance, finance, donations, partners, beneficiaries, volunteers, risks, complaints, and corrective actions.

03 Records should be accurate, complete, and retrievable.

04 Financial and accounting records should generally be retained for no less than ten years, and administrative records for no less than five years, unless longer periods apply.

05 Donation-related accounting records should be retained for no less than ten years.

06 Reports submitted to the Ministry or competent authority should be consistent with internal records

07 Electronic records should be secure, backed up, and protected from unauthorised alteration.

08 Public transparency should be balanced with confidentiality, data protection, and beneficiary dignity.

09 Risk indicators, complaints, and supervisory observations should be recorded and followed up.

10 Where matters are unclear, the organisation should refer to the Ministry or competent authority.

By maintaining strong records and transparent reporting, the organisation strengthens public trust, facilitates supervision, protects itself from misuse, and demonstrates that its policies and controls are applied in practice.

Risk-Based Supervision, Inspection, Follow-Up, and Corrective Actions

15

Risk-Based Supervision, Inspection, Follow-Up, and Corrective Actions

15.1 Purpose of this Chapter

This chapter aims to explain how Non-Profit Organisations should prepare for supervision, inspection, and follow-up by the Ministry or the competent authority, and how they should deal with data requests, supervisory observations, potential violations, risk indicators, and corrective actions in an organised, transparent, and risk-based manner.

Supervision is not merely an external procedure carried out by the competent authority, nor is it a purely formal review of files. It is part of the broader governance, compliance, and effectiveness framework. A well-managed organisation should be able at any time to demonstrate that its activities, resources, donations, partnerships, volunteers, and records are managed in accordance with the law, clear internal policies, and controls that are proportionate to the level of risk.

This chapter also links internal oversight and external supervision with the effectiveness requirements under the FATF Methodology, particularly those relating to protecting Non-Profit Organisations from terrorist financing abuse.

15.2 Legal Basis for Supervision and Inspection

Legal Obligation

The legal and regulatory framework governing Public Benefit Organisations gives the Ministry and the competent authority the power to supervise, inspect, follow up, request information, review records, and take appropriate measures where weaknesses, breaches, or violations are identified.

Supervision and inspection may relate to the organisation's legal status, governance, activities, financial records, donations, fundraising campaigns, partners, beneficiaries, volunteers, internal controls, corrective actions, or compliance with decisions, permits, circulars, and instructions issued by the Ministry or the competent authority.

Accordingly, the organisation should treat supervision and inspection as part of its normal operating environment, and should maintain its records, policies, and evidence in a manner that allows it to respond effectively and in a timely manner.

15.3 Supervision as Evidence of Effectiveness, Not Merely Compliance

Supervision and inspection are not limited to checking whether documents exist. They also assess whether the organisation applies its policies and controls in practice.

For example, it is not sufficient for the organisation to have a donations policy if it cannot demonstrate how donations were recorded, reviewed, accepted, rejected, used, and reported. It is not sufficient to have a volunteer policy if volunteers were not registered, trained, assigned clear tasks, or prevented from collecting donations without approval.

Effective supervision therefore looks at both form and substance:

- Does the policy exist?
- Is the policy approved?
- Is the policy understood by staff and volunteers?
- Is the policy applied in practice?
- Are decisions documented?
- Are risk indicators identified and escalated?
- Are corrective actions implemented and closed?
- Can the organisation provide evidence when requested?

This approach helps demonstrate effectiveness, which is a key element under the FATF assessment methodology.

15.4 What Does Practical Supervision Mean?

Practical supervision means that the organisation is able to demonstrate, through records and evidence, that it manages its legal obligations and risk exposure in a structured and proportionate manner.

This may include demonstrating that:

The organisation's licence, declaration, classification, and key information are up to date.

- Activities are consistent with the approved objectives and classification.
- Donations are collected, received, recorded, and used through approved channels.
- Financial records and bank accounts are properly maintained.
- Partners and beneficiary entities are subject to appropriate due diligence.
- Volunteers are registered, assigned clear tasks, and prevented from unauthorised fundraising.
- Records are retained for the required periods.
- Risk indicators are recorded and followed up.
- Supervisory observations are addressed through corrective actions.
- The Board of Directors or governing body exercises appropriate oversight.

15.5 Risk-Based Supervision

Risk-based supervision means that supervisory attention and the intensity of inspection or follow-up may vary according to the level of risk associated with the organisation, its activities, resources, donations, partners, beneficiaries, volunteers, and operating environment.

An organisation that carries out limited local activities, does not collect donations, does not deal with higher-risk partners, and maintains strong records may require a different level of follow-up from an organisation that collects public donations, implements cross-border activities, deals with foreign partners, or has repeated supervisory observations.

The organisation should understand that risk-based supervision does not mean that low-risk organisations are not supervised. Rather, it means that the nature, frequency, scope, and depth of supervision may be proportionate to the risk profile.

15.6 Levels of Follow-Up According to Risk

The intensity of follow-up may vary depending on the risk level.

Low-Risk	Medium-Risk	High-Risk
Follow-Up This may include periodic desk review, submission of basic records, review of annual reports, verification of updated information, and simple follow-up on any minor observations.	Follow-Up This may include more detailed review of selected areas, such as donations, financial records, volunteer records, partner files, or implementation reports, as well as follow-up on corrective actions.	Follow-Up This may include more frequent or deeper review, on-site inspection, targeted examination of high-risk activities or campaigns, review of cross-border partnerships, review of risk indicators, verification of corrective actions, and escalation where required.

The organisation should be ready to explain its risk profile and to provide evidence supporting its internal assessment and controls.

15.7 Possible Types of Supervision and Follow-Up

Supervision and follow-up may take different forms, depending on the applicable legal and regulatory framework and the decision of the Ministry or competent authority.

Possible types include:

- Desk review.
- Data and document requests.
- Review of annual reports, budgets, or final accounts.
- Review of donation and fundraising campaign files.
- Review of partner, beneficiary, or volunteer records.
- Thematic review of a specific risk area.
- Follow-up on previous observations.
- On-site inspection or field visit.
- Meetings with the Board, management, employees, volunteers, or relevant persons.
- Review of corrective action plans.
- Verification of closure of observations.
- Referral or escalation where serious concerns arise.

The organisation should ensure that the relevant records are available, organised, and capable of being retrieved within the required timeframe.

15.8 Prior Preparation for Supervision and Inspection

The organisation should not wait until it receives an inspection notice or data request to organise its records. Inspection readiness should be part of daily governance and compliance.

Prior preparation includes:

- Maintaining an updated governance and compliance file.
- Ensuring that licensing, declaration, and classification records are available.
- Keeping Board decisions and internal policies organised.
- Maintaining financial records, bank statements, and reconciliations.
- Maintaining donation and fundraising campaign files.
- Maintaining partner and beneficiary records.
- Maintaining volunteer records and volunteering opportunity files.
- Keeping risk assessment and risk registers up to date.
- Recording incidents, breaches, and corrective actions.
- Assigning a focal point for supervisory communication.
- Ensuring that staff know how to respond to official requests.

The objective is not to prepare documents only for inspection, but to ensure that the organisation's daily work is already documented and reviewable.

15.9 Dealing with Data Requests

When the Ministry or competent authority requests data, records, or information, the organisation should respond in an accurate, timely, complete, and professional manner.

The organisation should:

01 Confirm receipt of the request.

02 Identify the scope and deadline.

03 Assign responsibility for preparing the response.

04 Collect information from the relevant departments or persons.

05 Ensure that the response is accurate and consistent with internal records.

06 Avoid providing estimates where exact records are required.

07 Clarify where information is not available or requires additional time.

08 Submit the response through the approved channel.

08 Retain a copy of the request, response, and supporting documents.

If the request is unclear, the organisation should seek clarification through the approved channel rather than guessing or submitting incomplete information.

15.10 Inspection Visit or Field Review

An inspection visit or field review may involve meetings, review of documents, walkthrough of procedures, testing of samples, verification of records, and discussion of observations.

The organisation should manage the visit professionally by:

- Assigning a responsible contact person.
- Ensuring that relevant staff are available.
- Providing a suitable place for document review or meetings.
- Making records available in an organised manner.
- Responding honestly and accurately.
- Avoiding unsupported statements.
- Providing evidence where available.
- Recording documents provided to inspectors.
- Taking note of requests or observations raised during the visit.
- Following up after the visit on any outstanding matters.

The organisation should not conceal information, alter records, or provide inconsistent explanations. Where an error or weakness exists, it is better to explain it clearly and demonstrate the corrective action being taken.

15.11 How Should the Organisation Respond During Supervision?

During supervision or inspection, the organisation should answer questions based on facts, records, and approved procedures.

A good response should:

- Be direct and accurate.
- Refer to the relevant policy, decision, register, or file.
- Explain what happened in practice, not only what should happen in theory.
- Distinguish between routine procedures and exceptional cases.
- Acknowledge weaknesses where they exist.
- Explain corrective actions taken or planned.
- Avoid giving assurances that cannot be supported by documents.
- Avoid contradicting records previously submitted to the Ministry or competent authority.

The organisation should remember that effectiveness is demonstrated through evidence. A clear record is often more convincing than a general verbal explanation.

15.12 Distinguishing Between an Administrative Observation, a Violation, and a Risk Indicator

The organisation should understand the difference between an administrative observation, a potential violation, and a risk indicator.

Administrative Observation

This may involve a minor weakness, incomplete file, delay in updating a record, or procedural gap that does not necessarily indicate misuse or a legal breach.

Potential Violation

This may involve conduct that may be inconsistent with a legal, regulatory, licensing, donation, financial, or supervisory requirement, such as collecting donations without a permit where one is required, using personal accounts, or failing to maintain required records.

Risk Indicator

This is a circumstance that may indicate exposure to misuse or abuse and requires review, documentation, and possibly escalation. Examples include unclear donations, unusual transfers, unauthorised donation links, unclear partners, or volunteers collecting donations without approval.

The same issue may sometimes fall into more than one category. For example, missing donation records may be an administrative weakness in one case, but may become a serious concern if linked to large donations, unclear channels, or failure to account for funds.

15.13 Cases Requiring Immediate Escalation

Some situations require immediate internal escalation and, where appropriate, referral to the Ministry or competent authority.

Examples include:

- Fundraising without a required permit or approval.
- Use of personal accounts to collect or hold donations.
- Unauthorised donation links or public fundraising appeals.
- Significant unexplained financial discrepancy.
- Refusal by a partner to provide implementation reports or evidence.
- Transfer of funds to an unclear third party.
- Serious negative information relating to a donor, partner, beneficiary entity, or intermediary.
- Misuse of the organisation's name, logo, or legal status.
- Volunteers collecting donations without approval.
- Loss or misuse of donation funds or valuable in-kind resources.
- Suspicion that funds, resources, or activities may have been diverted.
- Failure to implement a corrective action required by the competent authority.
- Any issue that may affect the organisation's legal status, reputation, or ability to operate.

Immediate escalation should be documented, including the facts, persons involved, initial action taken, and any referral made.

15.14 Supervisory Observations

Supervisory observations are findings or comments issued by the Ministry or competent authority following review, inspection, data analysis, or follow-up.

Observations may relate to:

- Missing or incomplete records.
- Weaknesses in policies or procedures.
- Delay in submitting reports.
- Weak financial documentation.
- Incomplete donation records.
- Weak partner or beneficiary due diligence.
- Unregistered or poorly documented volunteers.
- Use of unclear channels.
- Weak Board oversight.
- Failure to update risk assessment.
- Failure to close previous observations.

The organisation should treat supervisory observations seriously, even where they are not classified as violations. Repeated observations may indicate a systemic weakness that requires corrective action.

15.15 Classification of Observations by Seriousness

The organisation may internally classify observations according to their seriousness to determine the appropriate response.

Low-Severity Observation

A minor documentation or procedural issue that can be corrected quickly and does not indicate material risk.

Medium-Severity Observation

A recurring weakness, incomplete control, or gap affecting an important area such as donations, records, volunteers, or partners.

High-Severity Observation

A serious weakness or potential breach that may affect funds, beneficiaries, legal compliance, public trust, or exposure to terrorist financing abuse or other misuse.

Classifying observations helps the organisation prioritise corrective actions and allocate resources effectively.

15.16 Corrective Actions

Corrective actions are the steps taken by the organisation to address observations, weaknesses, breaches, or risk indicators.

A corrective action plan should include:

- Description of the observation or issue.
- Root cause.
- Required action.
- Person responsible.
- Deadline.
- Evidence required for closure.

- Review or approval authority.
- Status of implementation.
- Date of closure.
- Any additional measures to prevent recurrence.

Corrective action should be realistic, measurable, and linked to the actual weakness identified. It should not be limited to a general statement that the issue will not happen again.

15.17 Root Cause, Not Only Formal Treatment

The organisation should address the root cause of a weakness, not only the visible symptom.



If a document is missing, the root cause may be that the process does not clearly assign responsibility for documentation.



If a report was submitted late, the root cause may be the absence of a compliance calendar.



If a volunteer collected donations without approval, the root cause may be weak volunteer training or unclear instructions.



If a partner failed to provide reports, the root cause may be that the agreement did not include reporting obligations.



If bank records do not match internal records, the root cause may be weak reconciliation procedures.

Addressing the root cause helps prevent recurrence and demonstrates that the organisation is improving its internal controls.

15.18 Dealing with Potential Violations

Where a potential violation is identified, the organisation should respond promptly, carefully, and transparently.

The organisation should:

- Record the facts.
- Preserve relevant documents and records.
- Stop or suspend the relevant activity where necessary.
- Identify the legal or regulatory requirement that may have been breached.
- Escalate internally to senior management or the Board.
- Take immediate containment measures.
- Prepare corrective actions.
- Refer to the Ministry or competent authority where required or where the matter is unclear.
- Cooperate with any supervisory review or follow-up.
- Document the final decision and lessons learned.

The organisation should avoid informal treatment of potential violations, particularly where they involve donations, funds, beneficiaries, partners, volunteers, data, or public communications.

15.19 Continuous Internal Oversight

Internal oversight should be continuous and not limited to external inspections.

The organisation should periodically review:

- Licensing and classification records.
- Board and governance records.
- Financial records and bank reconciliations.
- Donation and fundraising campaign files.
- Partner and beneficiary records.
- Volunteer records.
- Risk assessment and risk indicators.
- Complaints and incidents.
- Corrective action plans.
- Compliance with reporting requirements.

Continuous oversight helps the organisation identify issues early and reduce the likelihood of serious findings during inspection.

15.20 Use of National Risk Indicators in Internal Inspection Plans

The organisation should consider national risk indicators, sectoral guidance, supervisory observations, and relevant typologies when preparing its internal review or inspection plans.

For example, internal reviews may focus on:

- Donation channels.
- Use of personal accounts.
- Conditional or anonymous donations.
- Digital fundraising links.
- Partners or beneficiary entities outside the State.
- Volunteers and fundraising risks.
- Financial discrepancies.
- Records retained for donation campaigns.
- Risk indicators identified by national authorities or supervisory bodies.

Using national risk indicators helps align the organisation's internal controls with the broader national understanding of risk.

15.21 Role of the Board of Directors in Supervision and Follow-Up

The Board of Directors or governing body should exercise oversight over supervision, inspection, and corrective actions.

The Board should review:

- Significant supervisory observations.
- High-risk findings.
- Corrective action plans.
- Delays in implementing corrective actions.
- Repeated weaknesses.
- Material financial or donation-related issues.

- Risk indicators requiring escalation.
- Reports submitted to the Ministry or competent authority.
- Lessons learned from inspections and internal reviews.

The Board should ensure that corrective actions are not treated as administrative tasks only, but as part of the organisation's governance and risk management framework.

15.22 Supervision Over Donations

The organisation should maintain specific oversight over donations and fundraising activities.

This includes reviewing:

01 Whether the required permits or approvals were obtained.

02 Whether donation channels were approved.

03 Whether campaign files are complete.

04 Whether donations are recorded and reconciled.

05 Whether administrative and operational expenses were deducted only where permitted and approved.

06 Whether donations were used for the approved purpose.

07 Whether large, unusual, anonymous, or conditional donations were reviewed.

08 Whether closing reports were submitted where required.

Donation supervision should focus on traceability, legality, transparency, and proper use of funds.

15.23 Supervision Over Voluntary Work

The organisation should maintain oversight over voluntary work, volunteers, and volunteer teams.

This includes reviewing:

- Whether volunteering opportunities were registered or licensed where required.
- Whether volunteers were registered.
- Whether volunteers accepted the Volunteer Charter.
- Whether tasks were clearly defined.
- Whether volunteers received instructions or training.
- Whether volunteers were prohibited from unauthorised fundraising.
- Whether entrusted items were returned.
- Whether volunteer breaches, complaints, or incidents were recorded and followed up.

Volunteer supervision should ensure that volunteer status is not misused to collect donations, access data, or use the organisation's name beyond the approved task.

15.24 Supervision Over Partners and Beneficiaries

The organisation should review whether partners, implementers, beneficiary entities, and final beneficiaries are managed in accordance with approved procedures.

This includes reviewing:

- Partner due diligence files.
- Agreements or memoranda of understanding.
- Approved bank accounts and payment channels.
- Implementation reports.
- Evidence that assistance or services reached the intended purpose.
- Beneficiary selection criteria.
- Complaints or risk indicators.
- Any third-party involvement.
- Use of funds or resources by partners.
- Termination or suspension decisions.

This review helps ensure that the organisation does not lose control of its resources after transferring them to a partner or beneficiary entity.

15.25 Supervision Over Records and Document Retention

The organisation should periodically review the quality, completeness, and retention of records.

This includes reviewing:

- Whether records are organised and retrievable.
- Whether donation records are retained for the required period.
- Whether financial and accounting records are retained for the required period.
- Whether partner, beneficiary, and volunteer records are complete.
- Whether reports submitted to the Ministry or competent authority are consistent with internal records.
- Whether electronic records are secure and backed up.
- Whether records are protected from unauthorised alteration or deletion.

Strong record-keeping is one of the main tools for demonstrating compliance and effectiveness.

15.26 Indicators of Weak Inspection Readiness

Indicators of weak inspection readiness may include:

- Records scattered across personal devices or informal channels.
- Lack of a clear focal point for supervisory communication.
- Inability to retrieve donation or campaign files.
- Incomplete Board minutes or governance records.
- Financial reports inconsistent with bank statements.
- Missing partner agreements or implementation reports.

- Lack of volunteer records.
- No register of risk indicators or incidents.
- Corrective actions not documented or not closed.
- Repeated supervisory observations.
- Staff unable to explain procedures.
- Policies that exist on paper but are not applied in practice.
- Delayed or incomplete responses to official requests.

These indicators do not always mean that a violation has occurred, but they show that the organisation needs to strengthen its governance and compliance systems.

15.27 Inspection Readiness Checklist

The organisation may use the following checklist before an inspection or supervisory review:

- Licence, declaration, classification, and founding documents are available and up to date.
- Board and committee records are organised.
- Internal policies and authority matrix are approved and accessible.
- Financial records and bank reconciliations are complete.
- Donation and fundraising campaign files are complete.
- Donation records are reconciled with bank or platform records.
- Partner files and agreements are available.
- Beneficiary records and evidence of delivery are available.
- Volunteer records and volunteering opportunity files are complete.
- Risk assessment and risk register are updated.
- Incident and breach register is updated.
- Conflict of interest register is maintained.
- Training records are available.
- Corrective action plans are tracked and supported by evidence.
- Reports submitted to the Ministry or competent authority are retained.
- Staff responsible for key areas are prepared to explain procedures.
- Any unclear matters have been referred to the Ministry or competent authority.

15.28 Self-Assessment Questions for Supervision and Follow-Up

The organisation may use the following questions:

- Are we ready to respond to a data request from the Ministry or competent authority?
- Do we know where our key records are stored?
- Are our records consistent with the reports we submitted?
- Can we demonstrate that donations were used for their approved purposes?

- Can we demonstrate that partners were reviewed and followed up?
- Can we demonstrate that volunteers were registered and assigned clear tasks?
- Do we maintain a register of observations and corrective actions?
- Do we review the root cause of observations?
- Do we verify whether corrective actions are effective?
- Does the Board review material observations?
- Do we use national risk indicators in our internal reviews?
- Do we classify observations by seriousness?
- Do we know when immediate escalation is required?
- Do we refer to the Ministry or competent authority where matters are unclear?

15.29 Chapter Summary

Risk-based supervision, inspection, follow-up, and corrective actions are essential parts of protecting the organisation and demonstrating effectiveness.

The key practical messages of this chapter are as follows:

- Supervision is not only an external process; it should be supported by continuous internal oversight.
- Inspection readiness should be part of daily governance, not an activity carried out only when inspection is announced.
- Data requests should be answered accurately, completely, and within the required timeframe.
- Supervisory observations should be recorded, classified, and addressed.
- Corrective actions should address the root cause of weaknesses, not only the visible symptom.
- Serious risk indicators or potential violations should be escalated promptly.
- The Board of Directors should oversee material observations and corrective actions.
- Donations, partners, beneficiaries, volunteers, financial records, and documents should be subject to regular internal review.
- Records and reports are essential evidence of compliance and effectiveness.
- Where matters are unclear, the organisation should refer to the Ministry or competent authority.

By applying these principles, the organisation can deal with supervision and inspection in a professional manner, strengthen its internal controls, reduce the risk of repeated weaknesses, and demonstrate that it is taking practical and proportionate measures to protect itself and the sector from abuse.

Awareness, Training, and Capacity-Building

16

Awareness, Training, and Capacity-Building

16.1 Purpose of this Chapter

This chapter aims to explain the importance of awareness, training, and capacity-building within Non-Profit Organisations, and how training can help Board members, management, employees, volunteers, and relevant partners understand their legal obligations, internal procedures, risk indicators, and practical responsibilities.

Training is not a formal activity carried out only to record attendance. It is a practical tool to strengthen governance, protect the organisation from abuse, improve compliance, and support the effectiveness of the organisation's controls.

The chapter also explains how organisations can develop a proportionate training plan that reflects the nature of their activities, size, risk profile, and the roles of the persons involved in their work.

16.2 Importance of Awareness and Training

Awareness and training are essential because many weaknesses in Non-Profit Organisations do not arise from bad intent, but from lack of understanding, unclear roles, or failure to recognise risk indicators.

Training helps the organisation to ensure that:

01 Board members understand their oversight role.

02 Executive management understands its responsibility for implementation.

03 Employees understand policies and procedures relevant to their work.

04 Volunteers understand the limits of their role.

05 Donation and fundraising teams understand approval and documentation requirements.

06 Programme teams understand partner and beneficiary due diligence.

07 Staff and volunteers know how to report risk indicators or breaches.

A person who does not understand the applicable procedure may unintentionally expose the organisation to risk. Training therefore helps prevent mistakes before they occur.

16.3 National Basis for Awareness in the Area of Financial Crime Prevention

The national framework places importance on awareness and education in relation to protecting Non-Profit Organisations from abuse, particularly in the context of anti-money laundering, countering the financing of terrorism, and protecting the sector from terrorist financing abuse.

The Ministry, in coordination with relevant authorities, plays an important role in awareness, guidance, supervision, and ensuring that organisations understand their risks and obligations.

Non-Profit Organisations should treat national guidance, supervisory observations, risk indicators, and relevant typology reports as practical sources for updating their internal awareness and training materials.

16.4 Who Should Be Trained?

Training should be provided to persons according to their role and level of responsibility.

This may include:

- Board members or trustees.
- Executive management.
- Finance and accounting staff.
- Fundraising and donations staff.
- Programme and project teams.
- Staff dealing with partners, beneficiary entities, or final beneficiaries.
- Volunteer coordinators.
- Volunteers and volunteer teams.
- Persons responsible for communication, media, or social media.
- Persons responsible for records, reports, or responding to supervisory requests.
- Relevant partners or implementers, where appropriate.

Not everyone needs the same level of training. Training should be role-based and proportionate.

16.5 Core Training Topics

Core training topics may include:

- Legal status and classification of the organisation.
- Approved objectives and scope of activities.
- Donation and fundraising rules.
- Financial controls and use of official bank accounts.
- Prohibition on personal accounts and informal channels.
- Donor due diligence and handling unusual donations.
- Partner and beneficiary due diligence.
- Voluntary work rules and prohibition on unauthorised fundraising by volunteers.
- Records, reporting, and retention requirements.
- Risk indicators and internal escalation.
- Conflicts of interest.
- Data protection and confidentiality.
- Use of the organisation's name and logo.
- Dealing with supervisory requests and inspection.
- Corrective actions and lessons learned.

Training should explain not only what the rules are, but also why they matter and how they are applied in practice.

16.6 Training on National Risk Indicators

Training should include national risk indicators and typologies relevant to Non-Profit Organisations, including those relating to donations, partners, beneficiaries, volunteers, financial channels, digital fundraising, foreign entities, and activities outside the State.

Training on risk indicators should help staff and volunteers understand that a risk indicator is not proof of wrongdoing, but a sign that requires review, documentation, and, where necessary, escalation.

Examples of risk indicator training may include:

- Large or unusual donations.
- Conditional or anonymous donations.
- Use of personal accounts.
- Unauthorised donation links.
- Partners refusing to provide documents.
- Unclear beneficiary entities.
- Volunteers collecting donations without approval.
- Requests to transfer funds to third parties.
- Negative information relating to a donor, partner, or intermediary.
- Missing or inconsistent records.
- Pressure to implement quickly without review.

The organisation should update training materials when new risk indicators, supervisory observations, or national guidance are issued.

16.7 Training on Voluntary Work

Training on voluntary work is important because volunteers may interact with beneficiaries, donors, data, resources, or the organisation's name and reputation.

Volunteer training should cover:

- The purpose of the volunteering opportunity.
- Tasks assigned to volunteers.
- Limits of authority.
- Volunteer Charter requirements.
- Confidentiality and data protection.
- Beneficiary dignity and appropriate conduct.
- Health and safety requirements.
- Use of the organisation's name, logo, badges, or materials.
- Prohibition on collecting or advertising donations without approval.
- Reporting incidents, complaints, or risk indicators.
- Returning entrusted items after completion of the task.

Volunteers should receive practical and simple instructions before starting the task, and the organisation should retain evidence of the training or briefing provided.

16.8 Training on Donations

Persons involved in donations or fundraising should receive training on the legal and procedural requirements governing donation-related activities.

Training should cover:

- Difference between licensed and authorised entities.
- When a permit or approval is required.
- Approved donation channels.
- Advertising and public fundraising messages.
- Donation records.
- Handling cash and in-kind donations.
- Digital donation links and online campaigns.
- Anonymous, conditional, large, or unusual donations.
- Administrative and operational expenses.
- Campaign closure reports.
- Risk indicators in donations.
- Escalation and referral to the competent authority where necessary.

Training should emphasise that fundraising must not be carried out informally or through personal accounts, private links, or unauthorised public appeals.

16.9 Training on Partners and Beneficiaries

Persons responsible for programmes, projects, partnerships, or assistance should receive training on partner and beneficiary controls.

Training should cover:

- Partner due diligence.
- Minimum partner file.
- Agreements and memoranda of understanding.
- Payment and delivery channels.
- Beneficiary eligibility criteria.
- Evidence that assistance reached the intended purpose.
- Protection of beneficiary dignity and data.
- Conflicts of interest in partner or beneficiary selection.
- Risk indicators relating to partners, beneficiary entities, and final beneficiaries.
- Follow-up of partners after contracting.
- Termination or suspension of relationships where serious concerns arise.

Training should make clear that a partnership is not only a programme issue; it is also a governance, financial, reputational, and risk management issue.

16.10 Training on Records and Reports

Records and reports are essential evidence of compliance and effectiveness. Therefore, persons responsible for documentation, finance, programmes, volunteers, donations, or supervisory responses should be trained on record-keeping requirements.

Training should cover:

- What records must be retained.
- Retention periods.
- Donation records and campaign files.
- Financial and accounting records.
- Partner and beneficiary records.
- Volunteer records.
- Risk and incident registers.
- Conflict of interest records.
- Training records.
- Supervisory correspondence.
- Corrective action evidence.
- Consistency between internal records and reports submitted to the competent authority.
- Protection of electronic records and access rights.

Training should emphasise that records should be accurate, complete, dated, organised, and retrievable.

16.11 Training Methodology: Not One Training for Everyone

Training should be tailored to the role of the trainee. A Board member does not need the same training as a volunteer, and a finance officer does not need the same training as a communications officer.

The organisation may use a role-based approach as follows:

Board members: oversight, governance, risk, financial control, corrective actions, and accountability.	**Executive management:** implementation, supervision, escalation, reporting, and staff responsibilities.	**Finance staff:** bank accounts, payments, cash, donations, reconciliations, records, and financial risk indicators.
Fundraising staff: permits, channels, donor due diligence, campaign reporting, and donation risk indicators.	**Programme staff:** partners, beneficiaries, implementation evidence, and activity risks.	**Volunteer coordinators:** registration, tasks, Volunteer Charter, supervision, and breaches.

Volunteers: assigned tasks, conduct, confidentiality, prohibition on fundraising, and reporting of incidents.

Communications staff: use of the organisation's name and logo, public messages, beneficiary images, and avoiding unauthorised fundraising language.

This approach ensures that training is practical and relevant.

16.12 Annual Training Plan

The organisation should prepare an annual training plan proportionate to its size, activities, and risks.

The plan may include:

- Training objectives.
- Target groups.
- Topics.
- Frequency.
- Delivery method.
- Person or unit responsible.
- Training materials.
- Expected outcomes.
- Evaluation method.
- Follow-up actions.

The annual plan should take into account supervisory observations, internal incidents, new activities, changes in legal requirements, and risk indicators identified during the year.

16.13 Training Register

The organisation should maintain a training register to document training and awareness activities.

The training register may include:

- Training title.
- Date.
- Duration.
- Target audience.
- Participants.
- Trainer or facilitator.
- Training materials used.
- Attendance record.
- Key topics covered.
- Evaluation results, where applicable.
- Follow-up actions.
- Link to relevant policies or procedures.

The training register helps demonstrate that awareness and training are implemented in practice and are not merely planned.

16.14 Measuring Training Effectiveness

The organisation should not measure training only by the number of sessions or participants. It should also consider whether the training improved understanding and behaviour.

Training effectiveness may be measured through:

- Short tests or knowledge checks.
- Practical case discussions.
- Participant feedback.
- Review of errors or incidents after training.
- Improvement in record quality.
- Reduction in repeated observations.
- Better identification and reporting of risk indicators.
- Improved response to supervisory requests.
- Evidence that staff and volunteers apply the procedures in practice.

The organisation should use the results of training evaluation to improve future sessions.

16.15 Awareness Materials

Awareness does not always require formal training sessions. The organisation may use simple awareness tools, such as:

- Short internal reminders.
- One-page guidance notes.
- Posters or digital messages.
- Volunteer briefing cards.
- Donation approval checklists.
- Partner due diligence reminders.
- Frequently asked questions.
- Scenario-based examples.
- Internal alerts about new risk indicators.
- Lessons learned from incidents or inspections.

Awareness materials should be clear, practical, and accessible to the relevant audience.

16.16 Examples of Internal Awareness Messages

Examples of internal awareness messages include:

- Do not collect or advertise donations unless approval has been obtained.
- Do not use personal accounts for organisational funds.
- Do not publish donation links without internal approval.
- Do not use the organisation's name or logo outside the approved task.
- Do not share beneficiary information or images without approval.
- Report any unusual donation or unclear condition.
- Check the partner file before transferring funds or resources.
- Keep records complete, dated, and retrievable.
- Escalate risk indicators; do not ignore them.

- Refer to the Ministry or competent authority where requirements are unclear.

Such messages help convert policies into simple daily reminders.

16.17 Scenario-Based Training

Scenario-based training is one of the most effective methods for strengthening practical understanding.

Examples of scenarios include:

- A volunteer publishes a donation link on social media without approval.
- A donor offers a large conditional donation for an unclear beneficiary.
- A partner requests payment to a third-party bank account.
- A beneficiary list is provided by an external party without supporting documents.
- A fundraising campaign receives donations through an unapproved digital platform.
- A staff member discovers that campaign records do not match bank deposits.
- A partner outside the State refuses to provide implementation reports.
- A Board member has a conflict of interest in selecting a supplier.
- A bank requests updated information about the organisation's sources of funding.

Each scenario should ask: What is the risk? What should be documented? Who should be informed? Should the activity be suspended? Is referral to the Ministry or competent authority required?

16.18 Role of the Board of Directors in Building a Compliance Culture

The Board of Directors plays an important role in building a culture of compliance and accountability.

The Board should:

- Approve the training plan where appropriate.
- Ensure that management provides training to relevant persons.
- Review material incidents and lessons learned.
- Support a culture where staff and volunteers report issues without fear.
- Ensure that training is linked to actual risks and not limited to formal topics.
- Receive updates on key training activities and repeated weaknesses.
- Encourage practical application of policies and procedures.

A strong compliance culture begins with leadership and is reflected in the organisation's daily decisions.

16.19 Training and Partners

In some cases, it may be appropriate to provide awareness or guidance to partners, implementers, or service providers, particularly where they deal with funds, beneficiaries, volunteers, data, or the organisation's name.

Partner awareness may cover:

- Purpose of the partnership.
- Reporting obligations.

- Use of funds or resources.
- Evidence of implementation.
- Protection of beneficiary data.
- Prohibition on unauthorised fundraising.
- Prohibition on transferring resources to third parties without approval.
- Risk indicators and reporting obligations.
- Use of the organisation's name and logo.

Partner training or briefing should be proportionate to the nature and risk of the relationship.

16.20 Common Mistakes in Training and Awareness

Common mistakes include:

- Training only one person and assuming the whole organisation understands the requirements.
- Delivering generic training that is not linked to the organisation's actual work.
- Training volunteers without explaining the prohibition on fundraising.
- Failing to train Board members on oversight responsibilities.
- Not documenting attendance or training materials.
- Not updating training after incidents or supervisory observations.
- Treating training as a one-time activity.
- Measuring training only by attendance, not by impact.
- Providing training in language or terminology that staff or volunteers do not understand.
- Not using practical examples or scenarios.

16.21 Self-Assessment Questions for Training and Awareness

The organisation may use the following questions:

- Do we have an annual training plan?
- Are Board members trained on their oversight responsibilities?
- Are finance staff trained on bank accounts, cash, payments, and records?
- Are fundraising staff trained on donation permits and approved channels?
- Are volunteers trained on the prohibition on collecting or advertising donations without approval?
- Are programme teams trained on partners and beneficiaries?
- Are staff trained on risk indicators and escalation?
- Do we keep a training register?
- Do we update training after incidents or supervisory observations?
- Do we use practical scenarios?
- Do we measure whether training is effective?
- Do partners receive guidance where their role creates risk?
- Are awareness messages clear and easy to understand?
- Can we demonstrate that training improved practice?

16.22 Chapter Summary

Awareness, training, and capacity-building are essential tools for protecting Non-Profit Organisations from abuse and strengthening compliance and effectiveness.

The key practical messages of this chapter are as follows:

01 Training should be practical, role-based, and linked to the organisation's actual risks.

02 Training should cover donations, partners, beneficiaries, volunteers, finance, records, risk indicators, and escalation.

03 Volunteers should clearly understand that they may not collect or advertise donations without prior approval.

04 Board members should understand their oversight role.

05 Training should use national risk indicators, supervisory observations, and practical scenarios.

06 Training should be documented through a training register

07 Training effectiveness should be measured by understanding, behaviour, improved records, and reduced repeated weaknesses, not attendance only.

08 Awareness should be continuous, not limited to annual sessions.

09 Where partners or implementers create risk exposure, they should receive appropriate guidance.

By applying these principles, the organisation can build a stronger culture of compliance, improve its ability to detect and respond to risks, and demonstrate that its controls are understood and applied in practice.

Risk Indicators, Internal Reporting, and Escalation

17

Risk Indicators, Internal Reporting, and Escalation

17.1 Purpose of this Chapter

This chapter aims to help Non-Profit Organisations identify risk indicators that may arise in their activities, donations, financial channels, partners, beneficiary entities, final beneficiaries, volunteers, records, or use of the organisation's name and logo.

The purpose of this chapter is not to treat every risk indicator as evidence of a violation or suspicion. Rather, it aims to help the organisation recognise situations that require review, documentation, internal reporting, escalation, or referral to the Ministry or competent authority where appropriate.

Risk indicators are practical warning signs. If they are identified and handled early, the organisation can prevent misuse, correct weaknesses, protect its resources, and demonstrate that its controls are applied in practice.

17.2 What is a Risk Indicator?

A risk indicator is a fact, circumstance, behaviour, pattern, or weakness that may suggest an increased possibility of misuse, abuse, non-compliance, financial irregularity, unauthorised activity, or terrorist financing abuse.

A risk indicator does not automatically mean that abuse has occurred. It means that the organisation should ask further questions, review the relevant records, assess the seriousness of the matter, and take proportionate action.

For example, a missing document may be a simple administrative error. However, if the missing document relates to a large donation, an unclear partner, an unauthorised fundraising link, or a transfer to a third party, the same issue may become more serious and require escalation.

17.3 General Principles for Handling Risk Indicators

The organisation should apply the following principles when dealing with risk indicators:

- Do not ignore the indicator.
- Do not assume that every indicator proves wrongdoing.
- Review the surrounding facts and context.
- Check whether the indicator is isolated or repeated.
- Assess whether it affects funds, donations, beneficiaries, partners, volunteers, data, or public trust.
- Document the indicator and the action taken.
- Escalate the matter internally where needed.
- Suspend the activity or transaction where continuing may increase the risk.
- Refer to the Ministry or competent authority where the matter is unclear, serious, or subject to official approval or notification.
- Update the relevant register, risk assessment, or corrective action plan.

The organisation should ensure that staff and volunteers understand that reporting a risk indicator is not an accusation. It is a protective measure for the organisation and the sector.

17.4 Levels of Risk Indicators

Risk indicators may be classified into three broad levels.

Low-Level Indicator

This may include a minor documentation gap, isolated administrative error, or incomplete record that does not appear to affect funds, beneficiaries, partners, or legal compliance. It should still be corrected and documented.

Medium-Level Indicator

This may include a repeated weakness, unclear information, unusual donation, incomplete partner file, delayed reporting, or a control gap affecting an important area. It requires internal review, documentation, and follow-up.

High-Level Indicator

This may include a serious financial discrepancy, unauthorised fundraising, use of personal accounts, unclear third-party transfers, serious negative information, suspected diversion of funds, misuse of the organisation's name, or volunteers collecting donations without approval. It requires immediate escalation and may require referral to the Ministry or competent authority.

The level of seriousness depends on the facts, value, parties involved, recurrence, impact, and whether the issue relates to a sensitive area such as donations, funds, partners, beneficiaries, or activities outside the State.

17.5 Risk Indicators Related to Donations and Donors

Risk indicators relating to donations and donors may include:

- A large or unusual donation that is inconsistent with the organisation's normal pattern of donations.
- A donation received through an unofficial or unclear channel.
- A donor refusing to provide basic information where such information is required.
- A donation linked to an unclear or unrelated purpose.
- A conditional donation directing funds or resources to an unclear person, entity, partner, or beneficiary.
- A donation from an anonymous or incomplete source that is large, repeated, or conditional.
- Pressure to accept or use the donation quickly without review.
- A request to return, redirect, or transfer the donation to a third party.
- A donation linked to a foreign entity or foreign Non-Profit Organisation of unclear status.
- Use of cash where official channels are available.
- A donation linked to virtual assets or non-traditional digital mechanisms without clarity.

- Negative information relating to the donor, intermediary, proposed beneficiary, or partner.
- Inconsistency between the donor, donation value, purpose, channel, and proposed beneficiary.

The organisation should review such indicators in a risk-based manner, document the outcome, and escalate the matter where appropriate.

17.6 Risk Indicators Related to Fundraising Campaigns

Risk indicators relating to fundraising campaigns may include:

- Launching a campaign without the required permit or approval.
- Publishing donation links before approval.
- Using messages that do not clearly identify the purpose or beneficiary.
- Using the organisation's name or logo in a campaign not approved internally.
- Fundraising through personal accounts, private links, or unofficial platforms.
- Campaign records that do not reconcile with bank or platform reports.
- Lack of a clear campaign file.
- Administrative or operational expenses deducted without clear approval or legal zasis.
- Campaign materials that exaggerate, mislead, or exploit beneficiaries' images or stories.
- Donations collected after the approved period.
- Failure to submit campaign closing reports where required.
- Volunteers or partners advertising or collecting donations without approval.
- Public appeals that appear to be donations but are not treated internally as fundraising.

The organisation should ensure that every campaign has a clear approval basis, official collection channels, reviewed public messaging, complete records, and proper closure.

17.7 Risk Indicators Related to Financial Channels and Accounts

Risk indicators relating to financial channels and accounts may include:

- Use of personal accounts to receive, hold, or transfer funds.
- Use of accounts that do not belong to the organisation, partner, or approved beneficiary entity.
- Cash retained without clear justification.
- Payments made without supporting documents.
- Repeated delays in depositing cash.
- Bank transactions that cannot be matched with internal records.
- Unexplained withdrawals or transfers.
- Payments to unclear third parties.
- Transfers to partners or suppliers without contracts or evidence of delivery.
- Multiple rapid transfers inconsistent with the nature of the activity.

- Unauthorised donation links or digital platforms.
- Discrepancies between platform reports and bank deposits.
- Missing invoices, receipts, or approval documents.
- Repeated audit observations relating to financial controls.
- Pressure to make urgent payments outside normal review procedures.

Financial indicators should be handled carefully because they may affect traceability, accountability, and public trust.

17.8 Risk Indicators Related to Partners and Beneficiary Entities

Risk indicators relating to partners and beneficiary entities may include:

- The partner refuses to provide licence, registration, or legal status documents.
- The identity of authorised representatives is unclear.
- The partner requests payment to a personal account or an account that does not belong to it.
- The partner requests cash payment without justification.
- The partner refuses visits, review, or provision of reports.
- Implementation reports are missing, weak, or inconsistent.
- Beneficiary entities are unclear or not linked to the approved purpose.
- A partner changes its bank account or authorised representatives without explanation.
- The partner's capacity appears inconsistent with the size or nature of the activity.
- The partner requests use of the organisation's name or logo without controls.
- Funds or resources are transferred to another party without prior approval.
- Multiple entities or intermediaries are involved without a clear operational need.
- Negative information exists about the partner, beneficiary entity, or intermediary.
- The relationship is linked to a higher-risk jurisdiction, region, or channel.
- The partner is a foreign Non-Profit Organisation of unclear status.
- The partner requests digital, virtual asset, or unusual payment mechanisms without justification.

The existence of one indicator does not automatically mean that the relationship should be terminated, but it requires review, documentation, and, where appropriate, enhanced due diligence.

17.9 Risk Indicators Related to Final Beneficiaries

Risk indicators relating to final beneficiaries may include:

- Inconsistent or incomplete beneficiary information.
- Beneficiary lists that are not updated or are not supported by evidence.
- External interference in beneficiary selection.
- Beneficiaries selected without clear criteria.
- Repeated requests from the same person or group without justification.
- Request to transfer assistance to a third party.
- Absence of evidence that assistance was received.
- Repeated complaints relating to distribution.
- Manipulation of beneficiary lists.
- An undisclosed relationship between a beneficiary and a Board member, employee, volunteer, partner, or implementer.
- The beneficiary category does not match the approved purpose.
- Distribution patterns inconsistent with the programme objective.
- A partner or external party imposing names without a clear basis.
- Assistance being diverted after delivery.

The organisation should balance verification with beneficiary dignity and data protection. The objective is to confirm that assistance reaches the intended purpose without collecting unnecessary information.

17.10 Risk Indicators Related to Volunteers and Volunteer Teams

Risk indicators relating to volunteers and volunteer teams may include:

- A volunteer collecting donations without approval.
- A volunteer publishing donation links or fundraising messages.
- A volunteer using the organisation's name, logo, badge, or identity outside the assigned task.
- A volunteer contacting beneficiaries outside approved channels.
- A volunteer requesting personal information from beneficiaries without authorisation.
- A volunteer accessing data or systems beyond the task assigned.
- A volunteer refusing to follow instructions or the Volunteer Charter.
- A volunteer retaining entrusted items after the task ends.
- A volunteer influencing beneficiary selection without authority.
- A volunteer requesting gifts, payments, or personal benefits.
- A volunteer sharing beneficiary images, stories, or confidential information without approval.

- Participation of unregistered volunteers where registration is required.
- Repeated complaints about a volunteer or volunteer team.
- A volunteer acting on behalf of an unclear third party.

Such indicators should be reviewed promptly, especially where they involve donations, beneficiaries, data, or the organisation's public reputation.

17.11 Risk Indicators Related to Activities and Projects Inside and Outside the State

Risk indicators relating to activities and projects may include:

- Implementing an activity outside the approved objectives or classification.
- Launching an activity before obtaining required approval or permit.
- Lack of a clear project description, budget, or implementation plan.
- Weak evidence that the activity was implemented.
- Significant differences between budget and actual expenditure without explanation.
- Lack of implementation or financial reports.
- Complete reliance on a third party without follow-up.
- Activities outside the State without sufficient verification or approval.
- Use of foreign partners or beneficiary entities without appropriate due diligence.
- Use of informal financial channels in connection with the activity.
- Inability to verify that resources reached the intended purpose.
- Changes to the project scope without documentation or approval.
- Activities linked to higher-risk environments without additional controls.

The organisation should ensure that activities are planned, approved, implemented, documented, and closed in a manner proportionate to their risk level.

17.12 Risk Indicators Related to Use of the Organisation's Name or Logo

Risk indicators relating to the use of the organisation's name or logo may include:

- Unauthorised use of the organisation's name, logo, identity, or official materials.
- Creation of social media pages, groups, or websites using the organisation's name without approval.
- Unauthorised public statements or fundraising appeals.
- Partners or volunteers using the organisation's logo outside the approved scope.
- Use of the organisation's name to request donations, gifts, or benefits.
- Use of the organisation's name by a person whose relationship with the organisation has ended.

- Failure to recover badges, cards, stamps, or official materials.
- Misleading messages suggesting official endorsement or approval.
- Impersonation attempts or fake donation links.

The organisation should monitor its name and logo, provide clear instructions on authorised use, and act promptly when misuse is identified.

17.13 Risk Indicators Related to Negative Information, Sanctions, and Higher-Risk Parties

Risk indicators in this area may include:

- Negative public information relating to a donor, partner, beneficiary entity, intermediary, or volunteer.
- Association with persons, entities, or jurisdictions that raise concerns.
- Information suggesting links to unlawful activity, extremism, terrorist financing, fraud, or misuse of charitable funds.
- Requests to deal with a party that cannot be adequately identified.
- Use of nominees, intermediaries, or third parties without clear justification.
- Refusal to provide information required for verification.
- Inconsistency between the party's stated purpose and available information.
- Attempts to avoid official banking or documentation channels.
- A link to sanctions exposure or other official restrictions.

Where such indicators arise, the organisation should not proceed automatically. It should review the facts, escalate the matter internally, and refer to the Ministry or competent authority where required or where the appropriate course of action is unclear.

17.14 Risk Indicators Related to Records, Reports, and Transparency

Risk indicators relating to records and reports may include:

- Missing or incomplete records.
- Records kept only on personal devices or personal email accounts.
- Inability to retrieve key documents.
- Inconsistency between internal records and reports submitted to the competent authority.
- Donation records not matching bank or platform reports.
- Partner files lacking agreements or implementation reports.
- Beneficiary records not supporting delivery of assistance.
- Volunteer records missing registration or task information.
- Repeated late submission of reports.
- Alteration of records without explanation.
- Lack of evidence for corrective action closure.
- Weak or absent Board minutes.

- Lack of evidence for corrective action closure.
- Weak or absent Board minutes.
- Reports prepared from estimates instead of records.
- Destruction or deletion of records before the required retention period.

Weak records may not always indicate misuse, but they reduce the organisation's ability to demonstrate compliance, transparency, and effectiveness.

17.15 Additional Indicators Linked to Specialised Typologies of NPO Abuse

Some indicators may be linked to more specialised typologies of abuse of Non-Profit Organisations, including terrorist financing abuse.

These may include:

- Use of the organisation to move funds without a clear charitable, humanitarian, social, or public benefit purpose.
- Use of several entities, partners, or intermediaries without a clear operational need.
- Funds moving quickly through accounts without being linked to implementation.
- Use of foreign Non-Profit Organisations of unclear status.
- Use of unlicensed hawala or informal transfer channels.
- Use of trade, services, invoices, or contracts to justify transfers unrelated to the organisation's purpose.
- Use of virtual assets, digital platforms, or crowdfunding mechanisms without clarity or approval.
- Loan repayments, settlements, or financial arrangements that do not match the organisation's activities.
- Use of family members, associates, nominees, or corporate structures to conceal the real party involved.
- Activities connected to higher-risk jurisdictions or conflict-affected environments without adequate controls.
- Refusal by parties involved to provide implementation reports or evidence of delivery.
- Attempts to keep the final beneficiary, controller, or source of funds unclear.

These indicators require careful review because they may suggest that the organisation or its relationships are being used as a channel, cover, or facilitator.

17.16 Sources for Detecting Risk Indicators

Risk indicators may be detected through several sources, including:

- Staff observations.
- Volunteer reports.
- Board or committee review.
- Financial reviews and bank reconciliations.
- Donation and campaign records.
- Partner reports.
- Beneficiary complaints.
- Internal audits or reviews.
- External audit observations.
- Supervisory observations.

- Requests from the Ministry or competent authority.
- National risk assessments, guidance, and typology reports.
- Media or public information.
- Complaints from donors, beneficiaries, employees, or the public.
- Monitoring of social media and digital channels.

The organisation should encourage reporting of indicators from all relevant persons and should not rely only on formal inspection or audit processes.

17.17 Internal Reporting of Risk Indicators

The organisation should establish a clear internal reporting mechanism for risk indicators, incidents, breaches, or unusual situations.

The mechanism should clarify:

- Who may report.
- What should be reported.
- To whom the report should be made.
- How urgent matters should be escalated.
- How the report is documented.
- Who reviews the report.
- How confidentiality is protected.
- When the Board, senior management, Ministry, or competent authority should be informed.

Staff and volunteers should be encouraged to report concerns in good faith. The organisation should avoid a culture where persons fear reporting issues or where risk indicators are ignored because they are inconvenient.

17.18 Minimum Information When Recording a Risk Indicator

When recording a risk indicator, the organisation should include, where available:

- Date of detection.
- Person or unit identifying the indicator.
- Area affected, such as donation, campaign, finance, partner, beneficiary, volunteer, data, or records.
- Description of the indicator.
- Parties involved.
- Related amount, activity, or file reference.
- Initial assessment of seriousness.
- Immediate action taken.
- Person responsible for review.
- Escalation decision.
- Final decision.
- Corrective action or closure evidence.
- Whether the matter was referred to the Ministry or competent authority.

The record should be factual and should avoid unsupported conclusions.

17.19 Procedures for Handling a Risk Indicator

The organisation should handle risk indicators through a structured process.

This process may include:

01 Detecting the indicator.

02 Recording the indicator.

03 Conducting an initial review.

04 Determining the level of seriousness.

05 Preserving relevant records.

06 Suspending the activity, transaction, or relationship where needed.

07 Requesting additional information or documents.

08 Escalating internally to management, the relevant committee, or the Board.

09 Taking corrective or preventive action.

10 Referring to the Ministry or competent authority where required or where the matter is unclear.

11 Closing the case with evidence.

12 Updating the risk assessment, register, policy, or training materials where needed.

The organisation should ensure that cases are not left open without ownership, deadline, or final decision.

17.20 When Should Immediate Escalation Occur?

Immediate escalation should occur where the indicator may involve serious risk, potential violation, possible misuse of funds or resources, or harm to the organisation's reputation, beneficiaries, or public trust.

Examples include:

- Fundraising without a required permit or approval.
- Use of personal accounts to collect or hold donations.
- Unauthorised donation links or public fundraising appeals.
- Serious unexplained financial discrepancy.
- Transfer of funds to an unclear third party.
- Partner refusing to provide implementation reports or evidence.
- Negative information relating to a donor, partner, beneficiary entity, or intermediary.
- Misuse of the organisation's name, logo, or legal status.
- Volunteers collecting or advertising donations without approval.
- Loss or misuse of donation funds or valuable in-kind resources.
- Suspicion that funds, resources, or activities may have been diverted.
- Attempts to conceal the real donor, controller, intermediary, or final beneficiary.
- Activity outside the State without required approval or verification.
- Serious breach of data confidentiality or beneficiary protection.
- Repeated failure to implement corrective actions required by the competent authority.

Immediate escalation should be documented and should not depend on informal judgement by one person only.

17.21 When Should the Ministry or Competent Authority Be Consulted?

The organisation should consult or refer to the Ministry or competent authority where there is uncertainty, a legal or regulatory requirement, or a serious issue that cannot be resolved internally.

Examples include:

- Unclear legal basis for a fundraising campaign.
- Large, unusual, conditional, anonymous, or unclear donation.
- Use of a new digital donation or crowdfunding channel.
- Donation linked to virtual assets or non-traditional mechanisms.
- Activities, partners, or beneficiary entities outside the State.
- Use of foreign partners or foreign Non-Profit Organisations of unclear status.
- Serious risk indicators relating to funds, partners, beneficiaries, volunteers, or the organisation's name.
- Potential violation of donation, voluntary work, or Public Benefit Organisation requirements.
- Need to amend, suspend, or close an approved activity or campaign.
- Unauthorised use of the organisation's name or logo.
- Inspection observations requiring clarification.
- Any situation where the organisation is uncertain whether it may proceed.

The organisation should document the referral, the response received, and any action taken.

17.22 Risk Indicator and Incident Register

The organisation should maintain a risk indicator and incident register.

The register should include:

- Case number.
- Date.
- Area affected.
- Description of the indicator or incident.
- Related file, donation, partner, beneficiary, volunteer, activity, or transaction.
- Initial risk level.
- Action taken.
- Person responsible.
- Internal escalation.
- Referral to Ministry or competent authority, where applicable.
- Corrective action.
- Closure date.
- Evidence of closure.
- Lessons learned.

The register helps the organisation demonstrate that it identifies, reviews, escalates, and closes risk indicators in a structured manner.

17.23 Simplified Model for Assessing a Risk Indicator

The organisation may use the following simplified assessment model:

Question	Purpose
What happened?	To describe the indicator factually.
Which area is affected?	Donation, finance, partner, beneficiary, volunteer, record, data, or activity.
Who is involved?	To identify the parties connected to the indicator.
Is there a legal or regulatory issue?	To identify whether official referral may be required.
Is money, data, beneficiaries, or public trust affected?	To assess seriousness.
Is the indicator isolated or repeated?	To assess whether the issue is systemic.
What immediate action is needed?	To stop or reduce the risk.
Who should review or approve the decision?	To ensure proper escalation.
Should the Ministry or competent authority be consulted?	To avoid acting without clarity.
What evidence is needed to close the case?	To ensure proper documentation.

This model can be used by management, compliance staff, programme teams, finance teams, volunteer coordinators, or any relevant internal function.

17.24 Practical Examples

Example 1: Unauthorised Donation Link

A volunteer publishes a donation link using the organisation's name without internal approval. The organisation should record the case, request removal of the link, verify whether any funds were collected, prohibit the volunteer from further fundraising activity, review volunteer instructions, and refer to the competent authority where required.

Example 2: Conditional Donation to an Unclear Beneficiary

A donor offers a large donation on condition that it be directed to a specific external entity that cannot provide clear legal documents. The organisation should suspend acceptance, request information, review the proposed beneficiary or partner, escalate internally, and refer to the competent authority if the matter remains unclear.

Example 3: Partner Requests Third-Party Transfer

A partner requests that funds be transferred to an account that does not belong to it. The organisation should stop the payment, request justification and documents, verify the account and third party, review the agreement, escalate the case, and proceed only if the legal and operational basis is clear and approved.

Example 4: Missing Campaign Records

A fundraising campaign file does not reconcile with bank deposits. The organisation should review the records, compare bank statements with platform or receipt records, identify the discrepancy, assign responsibility, correct the records where possible, and escalate if funds cannot be traced.

Example 5: Beneficiary Data Misuse

A staff member or volunteer shares beneficiary images or personal data without approval. The organisation should remove the content where possible, record the incident, assess harm, restrict access if needed, remind staff and volunteers of confidentiality obligations, and take corrective action.

17.25 Using Risk Indicators to Improve Controls

Risk indicators should not be treated only as isolated incidents. They should be used to improve the organisation's controls.

For example:

01 If unauthorised donation links appear, the organisation should strengthen controls over public communications and digital platforms.

02 If volunteers misunderstand their role, the organisation should improve volunteer training and undertakings.

03 If partner reports are weak, the organisation should update agreement templates and reporting requirements.

04 If donation records are incomplete, the organisation should improve donation registers and reconciliation.

05 If repeated conflicts of interest arise, the organisation should update disclosure and decision-making procedures.

06 If staff are unsure when to escalate, the organisation should clarify internal reporting lines.

The objective is to turn risk indicators into lessons learned and stronger controls.

17.26 Self-Assessment Questions

The organisation may use the following questions:

- Do we have a clear definition of risk indicators?
- Do staff and volunteers know what to report?
- Do we have an internal reporting mechanism?
- Do we maintain a risk indicator and incident register?
- Do we distinguish between low-, medium-, and high-level indicators?
- Do we know which indicators require immediate escalation?
- Do we know when to refer to the Ministry or competent authority?
- Do we document decisions and corrective actions?
- Do we review whether indicators are isolated or repeated?
- Do we use indicators to update training and policies?
- Do we review donation, partner, volunteer, and financial indicators regularly?
- Do we respond to unauthorised use of our name or logo?
- Can we demonstrate that risk indicators were identified, reviewed, and closed?

17.27 Chapter Summary

Risk indicators are practical warning signs that help Non-Profit Organisations identify weaknesses, unusual situations, or possible misuse before they become more serious.

The key practical messages of this chapter are as follows:

01 A risk indicator is not proof of wrongdoing, but it must not be ignored.

02 Indicators should be reviewed in context and documented.

03 Indicators may relate to donations, campaigns, financial channels, partners, beneficiary entities, final beneficiaries, volunteers, activities, records, or use of the organisation's name.

04 Higher-risk indicators require internal escalation and may require referral to the Ministry or competent authority.

05 The organisation should maintain a risk indicator and incident register.

06 Staff and volunteers should know how to report concerns in good faith.

07 Corrective actions should address the root cause of the indicator.

08 Repeated indicators should lead to updates in policies, training, and controls.

09 Where the correct action is unclear, the organisation should consult the Ministry or competent authority before proceeding.

By applying these principles, the organisation can build a stronger culture of compliance, improve its ability to detect and respond to risks, and demonstrate that its controls are understood and applied in practice.

Protecting Access to Financial Services and Dealing with Banks

18

Protecting Access to Financial Services and Dealing with Banks

18.1 Purpose of this Chapter

This chapter aims to help Non-Profit Organisations build a transparent and organised relationship with banks and financial institutions, in a manner that ensures continued access to the accounts and financial services necessary for carrying out their legitimate activities, while enabling banks to properly understand the nature of the organisation, its sources of funding, activities, and risks.

This chapter is based on an important principle: protecting the sector from abuse should not lead to disrupting legitimate work or depriving compliant organisations of access to financial services. Access to bank accounts and formal financial channels is essential for transparency, traceability of funds, protection of donors' funds, and demonstrating that resources are used for their specified purposes.

18.2 Why is Access to Financial Services Important?

Recommended Good Practice / FATF Recommendations

Non-Profit Organisations rely on formal financial services for several purposes, including:

- Opening and managing bank accounts.
- Receiving donations through official channels.
- Paying operational expenses.
- Transferring funds to partners, suppliers, or beneficiary entities.
- Documenting revenues and expenditures.
- Preparing financial reports.
- Evidencing the source and use of funds.
- Reducing reliance on cash and informal channels.

The FATF Best Practices Paper on combating the abuse of Non-Profit Organisations for terrorist financing has emphasised that protecting the sector from abuse should not disrupt legitimate activities or unjustifiably restrict access to financial services. It also noted that certain cases of misapplication of Recommendation 8 have resulted in the restriction or termination of financial relationships with legitimate organisations.

18.3 Relationship Between Financial Services and Transparency

Recommended Good Practice

Using formal financial channels enhances transparency because it helps the organisation to:

- Evidence receipt of funds.
- Evidence the source of donations.
- Trace expenditure.
- Reconcile records with bank accounts.
- Reduce cash-related risks.
- Prepare accurate reports.
- Respond to requests from the Ministry or competent authority.
- Reassure donors, partners, and banks.

Accordingly, the organisation should not view bank requirements only as an obstacle. Rather, they should be understood as part of the wider transparency and governance framework.

18.4 Legal Basis for Bank Accounts

Legal Obligation

The Decree-Law regulating Non-Profit Organisations requires each association to have one or more bank accounts with national banks operating in the State. The local currency must be the primary currency of such accounts, with the possibility of opening one or more foreign currency accounts after obtaining the approval of the competent authority and providing the justified reasons for doing so. Bank accounts are to be opened based on a certificate issued by the competent authority.

Banks and financial institutions are also prohibited from opening bank accounts for Non-Profit Organisations unless they are declared and licensed, and after obtaining the certificate referred to in the Decree-Law. The association must notify the competent authority of the details of its bank accounts within ten days from the date of opening them, and of any change to the bank in which its funds are deposited.

Practical Impact

The organisation should ensure that:

01 The bank account is in the name of the organisation and not in the name of an individual.

02 The organisation is licensed and declared in accordance with the applicable requirements.

03 The account was opened based on the required certificate or approval.

04 Account details and authorised signatories are up to date.

05 The competent authority has been notified of account details and changes where required.

06 Any foreign currency account is supported by approval and justified reasons where applicable.

18.5 Risks of Using Cash and Informal Channels

Recommended Good Practice / Based on National Analysis

The more the organisation relies on cash or informal channels, the more difficult it becomes to trace funds and demonstrate that they were used for the specified purpose. This may also increase concerns for banks or the competent authority.

The UAE Financial Intelligence Unit report on terrorist financing typologies and facilitators referred to patterns involving the movement and concealment of funds through unlicensed hawala, local accounts, corporate networks, virtual assets, and crowdfunding through multiple channels.

Accordingly, the organisation should:

- Reduce the use of cash as much as possible.
- Use official accounts in the name of the organisation.
- Avoid using personal accounts.
- Avoid unlicensed hawala or informal channels.

- Document all transfers and payments.
- Periodically reconcile records with bank accounts.
- Ensure that any new financial channel is approved and authorised.

18.6 What Do Banks Need to Understand About the Organisation?

Recommended Good Practice

Banks may request information about the organisation in order to understand its nature and risks. The clearer and more organised the organisation's file is, the stronger its banking relationship is likely to be.

Information that the organisation may need to explain to the bank includes:

- The organisation's legal status.
- Licence and declaration decision.
- Approved classification.
- Objectives and activities.
- Board members.
- Authorised signatories.
- Sources of funding.
- Nature of donations, if any.
- Countries or areas in which the organisation operates, if any.
- Main partners.
- Beneficiary entities or beneficiary categories.
- Average volume of financial transactions.
- Channels used to collect or receive funds.
- Internal controls over disbursement and donations.
- Financial reports and final accounts.

18.7 Updated Bank File

Recommended Good Practice

To avoid delays in providing charitable or public benefit activities, the organisation is advised to maintain an updated file that can be provided to the bank when opening an account, reviewing the relationship, or responding to a request for updated information.

Suggested Contents of the Bank File

The bank file may include:

- Copy of the licence and declaration decision.
- Certificate or approval required to open the account.
- Approved classification of the organisation.
- Articles of association or founding document.
- Details of Board members.
- Details of authorised signatories.
- Minutes or decision approving account opening or updating signatories.
- Summary of the organisation's activities.
- Expected sources of funding.
- Donations policy or summary of donation controls.
- Disbursement policy or authority matrix.
- Final accounts or available financial statements.

- List of main campaigns or programmes, if any.
- List of main partners, where applicable.
- Clarification of whether the organisation operates outside the State.
- Approved point of contact with the bank.

18.8 How Should the Organisation Explain its Sources of Funding to the Bank?

Recommended Good Practice

The organisation should provide a clear and concise explanation of its sources of funding, without exaggeration or ambiguity.

Examples of sources of funding that should be explained include:

- Authorised public donations.
- Donations from legal persons.
- Government or semi-government support.
- Membership subscriptions, where applicable.
- Returns from authorised activities.
- Sponsorships or contributions linked to specific activities.
- In-kind donations, where they have a financial impact.
- Support from local or international partners, where applicable.

The organisation should clarify:

- Whether it collects donations.
- Whether permits are required.
- What channels are used.
- The average size of donations.
- Whether there are foreign donations.
- Whether there are cash donations.
- How donations are documented.
- How funds are used.

18.9 How Should the Organisation Explain its Activities to the Bank?

Recommended Good Practice

The explanation of the organisation's activities should be consistent with its licence and approved classification, and should not include unclear or unauthorised activities.

The activity explanation should clarify:

- The main field of the organisation.
- Beneficiary categories.
- Nature of programmes.
- Whether activities are inside or outside the State.
- Whether there are partnerships.
- Whether there are fundraising campaigns.
- Whether there is financial or in-kind assistance.
- Whether there is voluntary work.
- How programmes and results are documented.

Practical Drafting Example

The organisation operates in the field of [insert field according to the approved classification], and its activities focus on [insert beneficiary categories or programmes]. Activities are implemented in accordance with the licence and approved classification. The organisation maintains records of programmes, donations, partners, and beneficiaries, and applies internal controls for approving disbursements and monitoring the use of funds for their specified purposes.

18.10 Dealing with Bank Requests for Updated Information

Recommended Good Practice

Banks may request periodic updates of the organisation's information. Such requests should be handled promptly and accurately, as delay or inconsistency in information may lead to account restrictions or an increase in the organisation's perceived risk by the bank.

Proposed Procedure

The organisation should:

- Record the bank's request.
- Identify the documents required.
- Review the accuracy of information before submission.
- Ensure that information is consistent with what has been submitted to the competent authority.
- Have the response approved by the authorised person.
- Retain a copy of the response and attachments.

The organisation should avoid:

- Ignoring bank requests.
- Providing information that differs from information submitted to the competent authority.
- Sending expired or outdated documents.
- Changing authorised signatories without appropriate notification.
- Responding with general answers that do not explain the nature of the activity.

18.11 Dealing with Bank Questions About Donations

Recommended Good Practice

If the bank requests information about donations, a campaign, or transfers, the organisation should provide documented responses.

Expected Questions

The bank may ask:

- What is the source of these funds?
- What is the purpose of the campaign?
- Is the campaign authorised?
- Who are the main donors?
- What channels are used?
- Why are there cash deposits?
- Why are there repeated transfers from multiple parties?
- To whom will the funds be disbursed?
- Is there a beneficiary entity or partner?
- Are there donations from outside the State?

Supporting Documents

Supporting documents may include:

- Campaign permit.
- Donation register.
- Electronic platform report.
- Bank statement.
- Approved advertising materials.
- Campaign report.
- Disbursement decisions.
- Partner or beneficiary entity agreement.
- Evidence of use of funds.

18.12 Dealing with Digital Channels and Electronic Donations

Recommended Good Practice

Digital channels may be useful and transparent if they are approved. However, they may raise additional questions for banks if they are not clearly documented.

Proposed Controls

The organisation should:

- Use approved platforms only.
- Link each electronic campaign to a permit or approval where applicable.
- Reconcile platform reports with the bank account.
- Prohibit unofficial links.
- Prohibit the use of personal accounts.
- Monitor impersonated campaigns.
- Document any platform fees or deductions.
- Retain detailed reports on the campaign.

18.13 Dealing with Virtual Assets and Crypto-Assets

Risk Indicator / Requires Confirmation

The UAE Financial Intelligence Unit report referred to the misuse of virtual assets in crowdfunding and the movement of funds, and also referred to crypto-asset crowdfunding as an emerging typology.

Practical Rule

The organisation should not accept donations or support through virtual assets, crypto-assets, or non-traditional digital wallets unless it has verified:

01 The legality of the channel.

02 Whether approval or authorisation is required.

03 The organisation's ability to identify the source of funds.

04 The organisation's ability to retain records.

05 That this does not conflict with the instructions of the Ministry or competent authority.

06 That this does not conflict with the requirements of the bank or relevant regulatory authorities.

Clear guidance should be obtained from the Ministry or competent authority and relevant regulatory authorities before accepting any donations in virtual assets or crypto-assets.

18.14 How Can the Organisation Reduce the Risk of Account Restriction or Closure?

Recommended Good Practice

The organisation cannot guarantee that banking restrictions will never occur. However, it can reduce the risk through transparency and organisation.

Measures that may help reduce the risk of restrictions include:

- Updating bank information regularly.
- Providing licence and classification documents upon request.
- Using official accounts only.
- Avoiding personal accounts.
- Reducing cash.
- Documenting donations.
- Documenting the purpose of transfers.
- Responding promptly to bank enquiries.
- Preparing clear financial reports.
- Explaining any unusual transactions before or when they occur.
- Maintaining files for partners and beneficiary entities.
- Updating the bank when authorised signatories, activities, or sources of funding change.
- Having one point of contact responsible for the banking relationship.

18.15 If the Bank Requests Additional Information or Restricts the Account

Recommended Good Practice

If the bank requests additional information or restricts a particular service, the organisation should deal with the matter quickly, calmly, and with clear documentation.

Proposed Procedure

The organisation should:

- Request written clarification where possible.
- Identify the reason for the request or restriction.
- Collect the required documents.
- Provide a clear explanation of the nature of the transactions.
- Provide supporting documents.
- Involve senior management or the Board of Directors where necessary.
- Communicate with the competent authority if the restriction affects material obligations or programmes.
- Retain all correspondence.
- Review whether the reason for the restriction is linked to an internal weakness in records or data.
- Implement corrective action where needed.

18.16 Relationship Between the Bank and the Competent Authority

Recommended Good Practice

The organisation should understand that the bank has its own anti-money laundering and counter-terrorist financing obligations, while the competent authority has its role in licensing and supervising the organisation. The organisation should not assume that the approval of one party automatically satisfies the requirements of the other.

Accordingly, the organisation should:

01 Maintain consistent information between the bank and the competent authority.

02 Update both parties when material changes occur, according to the applicable requirements.

03 Avoid providing different descriptions of activities or funding sources.

04 Document approvals and permits.

05 Provide evidence of the legality of campaigns or donations when asked by the bank.

06 Refer to the competent authority where the bank's requirements relating to a licensed or authorised activity are unclear.

18.17 Preventing Over-Compliance or Unnecessary Disclosure

Recommended Good Practice

Transparency does not mean providing all data to every party without controls. The organisation should be transparent and organised, while at the same time protecting the data of donors, beneficiaries, and volunteers.

Practical Rule

The organisation should provide the bank with what is necessary to understand the activity, source of funds, and nature of transactions, while observing:

- Protection of beneficiary data.
- Avoiding the sharing of sensitive information unless needed.
- Not publishing or circulating beneficiary lists outside their intended purpose.
- Using aggregated data where sufficient.
- Compliance with national legislation and the instructions of the competent authority.

If the bank requests detailed sensitive information about beneficiaries or donors, the organisation should verify the legality and limits of sharing such information in accordance with applicable laws and instructions.

18.18 Role of the Board of Directors in the Banking Relationship

Recommended Good Practice

The banking relationship should not be the responsibility of the finance officer alone. The Board of Directors should have an oversight role.

The Board of Directors should:

- Approve the opening or closing of accounts where applicable.
- Approve authorised signatories.
- Review any restriction or closure of an account.
- Follow up on material bank enquiries.
- Ensure that clear financial records exist.
- Ensure that personal accounts are not used.
- Review unusual donations or transfers.
- Support management in providing accurate documents to the bank.
- Transfers to unusual accounts.
- Sudden change in the nature of activities.
- Use of new digital platforms.
- Crowdfunding campaigns.
- Transactions inconsistent with the organisation's declared activity.

Practical Procedure

Each unusual transaction should have a documented explanation:

- What is the purpose?
- Who is the other party?
- What supporting document exists?
- Who approved it?
- Is there an approval or permit?
- How was the money used?

18.19 Indicators that May Raise Questions from the Bank

Recommended Good Practice

The organisation should be prepared to explain transactions that may raise banking questions, such as:

- Sudden increase in donations.
- Repeated cash deposits.
- Transfers to new partners.
- Transfers outside the State.
- Donations from foreign entities.
- Donations split across multiple accounts.
- Returned donations.
- Transfers to unusual accounts.
- Sudden change in the nature of activities.
- Use of new digital platforms.
- Crowdfunding campaigns.
- Transactions inconsistent with the organisation's declared activity.

Practical Procedure

Each unusual transaction should have a documented explanation:

- What is the purpose?
- Who is the other party?
- What supporting document exists?
- Who approved it?
- Is there an approval or permit?
- How was the money used?

18.20 Banking Readiness Checklist

The organisation may use the following checklist:

Area	Available? Notes
Licence and declaration	Yes / No
Approved classification	Yes / No
Certificate or approval to open the account	Yes / No
Details of authorised signatories	Yes / No
Internal decision to open or update the account	Yes / No
Clear summary of activities	Yes / No
Explanation of sources of funding	Yes / No
Donations policy	Yes / No
Disbursement authority matrix	Yes / No
Donation register	Yes / No
Fundraising campaign reports	Yes / No
Files of main partners	Yes / No
Final accounts or financial statements	Yes / No
Bank update register	Yes / No
Point of contact with the bank	Yes / No

18.21 Self-Assessment Questions for the Banking Relationship

The organisation may ask itself:

- Are all bank accounts in the name of the organisation?
- Are account details and authorised signatories up to date?
- Has the competent authority been notified of accounts and changes where required?
- Do we have a file ready for the bank?
- Can we clearly explain our sources of funding?
- Can we explain any major donation or transfer?
- Do we use personal accounts? If yes, this should be stopped immediately.
- Do we have an updated donation register?
- Do we reconcile records with bank accounts?
- Do we respond to bank requests in a timely manner?
- Do we have a policy for handling information update requests?
- Do we protect donor and beneficiary data when sharing information?
- Do we know how to act if the bank restricts the account?
- Does the Board review material banking matters?

18.22 Chapter Summary

Access to formal financial services is essential for the transparency and protection of Non-Profit Organisations. An official bank account is not merely a financia tool; it is a means of evidencing the source of funds, tracing their use, and reducing the risks associated with cash and informal channels.

The rules of this chapter may be summarised as follows:

- Accounts must be in the name of the organisation, not in the name of individuals.
- Accounts must be opened in accordance with legal requirements and the necessary approvals.
- Bank and competent authority information must be updated when material changes occur.
- The organisation should maintain a ready file explaining its legal status, activities, and sources of funding.
- Donations and transfers should be documented, and bank enquiries should be answered clearly.
- Cash, personal accounts, and informal channels should be avoided.
- Virtual assets or non-traditional digital channels should be handled with caution.
- Donor and beneficiary data should be protected when information is shared.
- The Board of Directors should review material banking matters.
- The organisation should refer to the Ministry or competent authority where matters are unclear or where a restriction affects legitimate activity.
- In this way, the relationship with banks becomes part of the governance and transparency framework, rather than a separate financial procedure.

Institutional Communication, Media, and the Use of Images and Humanitarian Stories

19

Institutional Communication, Media, and the Use of Images and Humanitarian Stories

19.1 Purpose of this Chapter

This chapter aims to explain the controls that Non-Profit Organisations should observe when communicating with the public, using media channels, publishing content, using their name or logo, presenting humanitarian stories, or publishing images of beneficiaries, volunteers, activities, or fundraising campaigns.

Institutional communication is an important tool for building trust, raising awareness, and demonstrating the organisation's impact. However, it may also create legal, reputational, privacy, and fundraising risks if it is not properly managed.

This chapter therefore focuses on ensuring that communication is accurate, lawful, respectful, approved, and consistent with the organisation's objectives, legal status, and applicable permits or approvals.

19.2 Importance of Controlling Institutional Communication

Communication by a Non-Profit Organisation may influence donors, beneficiaries, volunteers, partners, banks, the public, and competent authorities. Therefore, it should be managed carefully.

Proper communication helps the organisation to:

- Explain its legitimate activities and public benefit objectives.
- Strengthen public trust.
- Protect the dignity and privacy of beneficiaries.
- Avoid misleading donors or the public.
- Prevent unauthorised fundraising.
- Prevent misuse of the organisation's name or logo.
- Ensure consistency between public messages and approved activities.
- Protect the organisation from reputational and regulatory risks.

Institutional communication should not be treated as a purely media-related matter. It is also a governance, compliance, risk management, and data protection matter.

19.3 Official Communication Channels

The organisation should identify its official communication channels and ensure that they are managed by authorised persons.

Official channels may include:

- Official website.
- Official email accounts.
- Official social media pages.
- Approved messaging channels.
- Media statements.
- Publications and brochures.
- Public events.
- Awareness campaigns.
- Fundraising campaign pages, where authorised.
- Annual reports or public activity reports.
- The organisation should avoid using personal pages, personal email accounts, or unofficial groups to publish messages in the organisation's name or to communicate donation-related information.

19.4 Approval of Public Messages

The organisation should establish a procedure for approving public messages before publication, particularly where the message relates to donations, beneficiaries, campaigns, partners, sensitive activities, or the organisation's official position.

The approval process should clarify:

- Who prepares the message.
- Who reviews it.
- Who approves it.
- Whether legal, compliance, or management review is required.
- Whether the message is linked to a permit or approval.
- Whether it includes beneficiary data or images.
- Whether it may be interpreted as a fundraising appeal.
- Where the approved version is retained.

No employee, volunteer, partner, or third party should publish content in the organisation's name unless this is authorised through the approved internal procedures.

19.5 Distinguishing Awareness Content from Fundraising Content

The organisation should distinguish between general awareness or activity-related content and content that may be considered fundraising.

Awareness content may explain an activity, provide public information, promote social responsibility, or present general messages.

Fundraising content, on the other hand, may involve inviting the public to donate, providing donation links, requesting financial or in-kind support, asking for sponsorship, promoting a campaign, or encouraging the provision of resources for a charitable or public benefit purpose.

A message may be considered fundraising even if it does not use the word "donation", if its practical effect is to invite the public to provide funds, goods, or support.

Accordingly, any public content that may be understood as a fundraising appeal should be reviewed against the applicable permit, approval, and donation-related requirements before publication.

19.6 Use of the Organisation's Name and Logo

The organisation's name, logo, identity, official stamp, badges, uniforms, templates, and communication materials are important assets that should be protected.

The organisation should define who may use its name and logo, and for what purposes.

Use of the organisation's name or logo should be prohibited where it involves:

- Fundraising without approval.
- Public communication not authorised by the organisation.
- Personal promotion or private benefit.
- Misleading the public regarding the organisation's role.
- Use by a partner outside the agreed scope.
- Use by volunteers outside their assigned task.
- Use after the end of employment, volunteering, or partnership.

- Association with activities, persons, or entities not approved by the organisation.

The organisation should maintain records of any approved use of its name or logo by partners, sponsors, volunteers, or third parties.

19.7 Use of Beneficiary Images and Humanitarian Stories

The use of beneficiary images, personal stories, or humanitarian cases may raise important privacy, dignity, and ethical considerations.

The organisation should ensure that such content is used only where lawful, necessary, respectful, and approved.

Before publishing beneficiary images or stories, the organisation should consider:

- Whether consent is required and has been obtained.
- Whether the beneficiary is a child or vulnerable person.
- Whether the image or story may expose the beneficiary to harm, stigma, embarrassment, or exploitation.
- Whether the same message can be communicated without identifying the beneficiary.
- Whether personal data can be masked or anonymised.
- Whether the story is accurate and not exaggerated.
- Whether the content is linked to fundraising and therefore requires approval.
- Whether the publication is consistent with the dignity and privacy of the beneficiary.

Humanitarian stories should not be used in a manner that exploits suffering or creates misleading emotional pressure on donors or the public.

19.8 Consent and Data Protection

Where beneficiary, donor, volunteer, employee, or partner data is used in public communication, the organisation should ensure that the use is lawful and limited to the approved purpose.

Consent, where required, should be clear, informed, and documented.

The organisation should avoid publishing:

- Full names of beneficiaries where not necessary.
- Identification documents.
- Contact details.
- Sensitive health, financial, family, or social information.
- Images of children or vulnerable persons without appropriate safeguards.
- Beneficiary lists.
- Information that may reveal location, vulnerability, or personal circumstances unnecessarily.
- Donor information without permission or lawful basis.

Where possible, the organisation should use aggregated information, anonymised case studies, or general descriptions instead of personal details.

19.9 Communication by Volunteers

Volunteers may not speak on behalf of the organisation, publish content in its name, use its logo, publish donation links, or communicate with donors or beneficiaries outside the limits of their assigned task and approved procedures.

- Volunteer communication controls should include:
- Clear instructions before the volunteering opportunity.
- Prohibition on publishing unauthorised content.
- Prohibition on fundraising or advertising donations without approval.
- Prohibition on sharing beneficiary images or personal data.
- Approval requirement for using the organisation's name or logo.
- Reporting of any media enquiry or public communication request.
- Returning badges, cards, or materials after the task ends.

The organisation should include these controls in volunteer briefings, undertakings, and training materials.

19.10 Communication by Partners and Third Parties

Partners, sponsors, implementers, suppliers, or other third parties should not use the organisation's name, logo, project materials, beneficiary images, or campaign messages unless this is clearly approved and documented.

Any agreement with a partner should address:

- Whether the partner may mention the organisation publicly.
- Whether the partner may use the organisation's logo.
- Whether public announcements require prior approval.
- Whether the partner may communicate with donors or beneficiaries.
- Whether the partner may publish images or stories.
- Whether the partner may refer to donations or fundraising.
- How unauthorised use will be handled.

Partners should be prohibited from using the organisation's name to collect donations or resources unless this is legally permitted and approved.

19.11 Social Media Controls

Social media is one of the most sensitive communication channels because content can spread quickly and may be shared, copied, edited, or misused.

The organisation should adopt controls for social media, including:

- Limiting access to official accounts to authorised persons.
- Using secure passwords and access controls.
- Approving posts before publication.
- Reviewing donation-related content against permit requirements.
- Monitoring comments and unauthorised links.

19.12 Digital Fundraising Links and Public Appeals

Any digital fundraising link, payment page, QR code, crowdfunding page, or public appeal must be treated as donation-related content and should be reviewed in accordance with the donation regulation requirements.

Before publishing such content, the organisation should verify:

- Whether the organisation is licensed or authorised to collect donations.
- Whether a permit or approval is required.
- Whether the platform or payment channel is approved.
- Whether the campaign purpose is clear.
- Whether the approved period and target amount are reflected accurately.
- Whether the public message is consistent with the permit or approval.
- Whether the link is official and secure.
- Whether the organisation can reconcile collected amounts with bank or platform records.

No digital donation link should be published through personal accounts, unauthorised groups, or unofficial pages.

19.13 Media Enquiries and Public Statements

The organisation should identify who is authorised to respond to media enquiries and issue public statements.

Public statements should be accurate, consistent, and aligned with the organisation's approved position.

Where a media enquiry relates to a sensitive issue, complaint, inspection, donation campaign, beneficiary case, incident, or risk indicator, the organisation should ensure that the response is reviewed by the appropriate internal authority before being issued.

The organisation should avoid:

- Providing unverified information.
- Disclosing confidential supervisory correspondence.
- Commenting on matters under review without approval.
- Sharing personal data.
- Blaming partners, beneficiaries, or volunteers publicly before completing internal review.
- Making statements that contradict records submitted to the Ministry or competent authority.

19.14 Public Reporting and Impact Communication

The organisation may publish annual reports, activity summaries, impact reports, or public updates to demonstrate transparency and accountability.

Such reports may include:

- General description of activities.
- Summary of programmes.
- Beneficiary categories.
- Number of activities or beneficiaries.
- General financial information where appropriate.
- Summary of donations and use of funds.

- Volunteer participation.
- Partnerships.
- Impact stories presented respectfully.
- General risk management or governance improvements.

Public reporting should be consistent with internal records and reports submitted to the Ministry or competent authority. It should not disclose confidential, personal, or sensitive information unnecessarily.

19.15 Use of Before-and-After Images or Emotional Content

Some organisations may use images or stories to show the impact of assistance. This should be handled carefully.

The organisation should avoid content that:

- Humiliates beneficiaries.
- Exposes children or vulnerable persons.
- Exaggerates suffering.
- Uses distressing images for emotional pressure.
- Discloses sensitive personal circumstances.
- Suggests that assistance is conditional on publicity.
- Misleads the public about the nature or scale of the activity.
- Uses images unrelated to the actual campaign or project.
- Where impact images are used, they should be truthful, respectful, and supported by consent and documentation where required.

19.16 Correction of Inaccurate Public Information

If the organisation publishes inaccurate, incomplete, or misleading information, it should correct the issue promptly.

The correction procedure may include:

- Identifying the inaccurate content.
- Removing or amending the content.
- Documenting the correction.
- Assessing whether donors, beneficiaries, partners, or the public were affected.
- Informing the Ministry or competent authority where required.
- Reviewing the approval process to prevent recurrence.
- Updating training or communication procedures.

The organisation should not ignore inaccurate content merely because it has already been published.

19.17 Impersonation and Unauthorised Use

The organisation should monitor and respond to impersonation, fake accounts, unauthorised donation links, misuse of its logo, or false claims of affiliation.

Where impersonation or unauthorised use is identified, the organisation should:

- Record the case.
- Preserve evidence, such as screenshots and links.
- Request removal where possible.
- Notify the platform or service provider.
- Inform internal management.

- Warn the public where appropriate.
- Verify whether any donations were collected.
- Notify the Ministry or competent authority where required.
- Review controls to prevent recurrence.

Impersonation may create serious risks because the public may believe that the organisation is responsible for unauthorised fundraising or misleading content.

19.18 Communication Risk Indicators

Communication-related risk indicators may include:

- Donation links published without approval.
- Public fundraising messages not linked to a permit.
- Use of personal accounts for campaign communication.
- Volunteers publishing content in the organisation's name.
- Partners using the logo outside the agreed scope.
- Beneficiary images published without safeguards.
- Public information inconsistent with internal records.
- Social media accounts managed without access controls.
- Fake pages or impersonation attempts.
- Media statements made without approval.
- Emotional or misleading content used to attract donations.
- Unauthorised use of the organisation's name by former employees or volunteers.
- Public promises that exceed the organisation's approved objectives or capacity.

The organisation should record and review such indicators and escalate serious cases where appropriate.

19.19 Communication Approval Register

The organisation may maintain a communication approval register, particularly where it frequently publishes public content, fundraising messages, or beneficiary stories.

The register may include:

- Date of proposed publication.
- Type of content.
- Channel.
- Person preparing the content.
- Person approving the content.
- Whether the content relates to fundraising.
- Permit or approval reference, where applicable.
- Whether beneficiary or donor data is included.
- Whether consent was obtained, where required.
- Final approved version.
- Date of publication.
- Any later amendment or removal.

The register helps demonstrate that public communication is controlled and reviewable.

19.20 Crisis Communication

The organisation should have a simplified procedure for responding to communication crises, such as allegations of misuse, unauthorised fundraising, data leakage, beneficiary complaints, media attention, or account impersonation.

The crisis communication procedure should identify:

- Who assesses the issue.
- Who approves public statements.
- Who communicates with the Ministry or competent authority.
- Who communicates with the bank or partner, where relevant.
- What information may be shared.
- How beneficiary and donor data will be protected.
- How internal records will be preserved.
- How corrective action will be communicated, if appropriate.

The organisation should avoid rushed public statements that are not supported by facts or approved internally.

19.21 Self-Assessment Questions for Communication and Media

The organisation may use the following questions:

- Do we have official communication channels?
- Who is authorised to publish content?
- Are donation-related posts reviewed before publication?
- Do we know when a message may be considered fundraising?
- Do partners need approval to use our name or logo?
- Do we protect beneficiary images, stories, and personal data?
- Do we keep evidence of consent where required?
- Do we monitor fake accounts or unauthorised links?
- Do we correct inaccurate public information?
- Are public reports consistent with internal records?
- Do we have a process for media enquiries?
- Do we know how to respond to a communication incident?

19.22 Chapter Summary

Institutional communication is an important tool for transparency, awareness, and public trust, but it must be managed through clear controls.

The key practical messages of this chapter are as follows:

01 Public communication should be accurate, approved, and consistent with the organisation's legal status and approved activities.

02 Donation-related content must be reviewed against applicable permit and approval requirements.

03 The organisation's name, logo, and identity should not be used without authorisation.

04 Volunteers and partners should not publish content or fundraising messages in the organisation's name without approval.

05 Beneficiary images and humanitarian stories should be used respectfully, lawfully, and only where appropriate safeguards exist.

06 Social media and digital channels require access controls and monitoring.

07 Impersonation, fake accounts, and unauthorised donation links should be addressed promptly.

08 Public reports should be consistent with internal records and should protect confidential and personal information.

09 Communication incidents and risk indicators should be recorded, reviewed, and escalated where necessary.

By applying these principles, the organisation can communicate its mission and impact effectively while protecting beneficiaries, donors, volunteers, partners, and the organisation's reputation.

Activities Outside the State, Cross-Border Partnerships, and External Assistance

20

Activities Outside the State, Cross-Border Partnerships, and External Assistance

20.1 Purpose of this Chapter

This chapter aims to explain the practical controls that Non-Profit Organisations should observe when implementing activities, partnerships, assistance, or volunteering opportunities outside the United Arab Emirates, or when dealing with partners, beneficiary entities, donors, or financial channels with a cross-border dimension.

Cross-border activities are particularly important from a governance and risk management perspective because they may involve different legal and operational

environments, greater difficulty in verifying partners and beneficiaries, multiple intermediaries, cross-border financial channels, and the possible association of certain areas or channels with higher risks.

This does not mean that external activities are prohibited or inherently high risk. Rather, it means that such activities require clearer assessment, approvals through the official authority, namely the UAE Aid Agency, stronger documentation, and more regular follow-up according to the nature of the activity and the level of risk.

20.2 What is Meant by a Cross-Border Activity?

Recommended Good Practice

For the purposes of this Manual, a cross-border activity means any activity, relationship, financial flow, in-kind flow, or operational arrangement whose effect extends outside the United Arab Emirates, or which involves a party outside the State.

This may include:

- Providing assistance or donations to an entity or person outside the State.
- Implementing a humanitarian, charitable, social, or public benefit project outside the State.
- Dealing with a foreign partner or implementer.
- Receiving donations from an entity or person outside the State.
- Cooperating with a foreign Non-Profit Organisation.
- Transferring funds or resources abroad.
- Sending volunteers or organising a volunteering opportunity outside the State.
- Using an international platform to collect or receive support.
- Implementing a campaign targeting an audience or beneficiaries outside the State.
- Purchasing or supplying goods or services for a project outside the State.

20.3 Why Do Cross-Border Activities Require Additional Care?

Recommended Good Practice / FATF Recommendations

Cross-border activities require additional care because they may involve factors that make verification and follow-up more difficult, such as:

- Differences in laws and procedures in the other country.
- Difficulty in verifying the partner or beneficiary entity.
- Difficulty in confirming that assistance reached the final beneficiaries.
- Use of intermediaries or third parties.
- External transfer or payment channels.
- Higher risks associated with certain areas or operating environments.
- Difficulty in conducting visits or field reviews.
- Possible use of unclear organisations or fronts.
- Weak ability to recover funds or resources if they are misused.

The FATF Best Practices Paper emphasises that measures relating to Non-Profit Organisations should be focused, proportionate, and risk-based, and that the nature of the activity and the operating environment affect the degree of risk exposure.

20.4 External Activities Are Not Prohibited in Themselves

Core Guidance Message

This Manual should be balanced. Humanitarian, charitable, developmental, and social work may sometimes require cross-border cooperation, and concerns about risk should not disrupt legitimate activity.

At the same time, an external activity should not be implemented without a clear understanding of the applicable legal and regulatory requirements, the partner, the purpose, the beneficiary, the financial channel, and the documentation mechanism.

Practical Rule

A legitimate external activity should be:

- Clear in purpose.
- Consistent with the organisation's objectives and classification.
- Supported by approvals or permits where required.
- Implemented through trusted partners.
- Funded or disbursed through formal channels.
- Documented through reports and evidence of implementation.
- Capable of follow-up and review.

20.5 Approvals and Permits Before Implementing an External Activity

Before implementing any activity, project, campaign, partnership, or assistance outside the State, the organisation should verify the official requirements and obtain the necessary approvals from the Ministry, the competent authority, and any relevant government entity, depending on the nature of the activity.

The approvals required may vary according to:

- Type of organisation.
- Nature of the activity.
- Target country or region.
- Whether the activity involves donations.
- Whether the activity involves transferring funds or resources.
- Whether the activity involves volunteers.
- Whether the activity is linked to a foreign entity.
- Whether the activity is humanitarian, relief, charitable, training-related, or social.

Practical Procedure

The organisation should not begin any external activity before preparing a file that includes:

- Description of the activity.
- Target country or region.
- Purpose.
- Partner or beneficiary entity.
- Sources of funding.
- Transfer or delivery channels.
- Expected beneficiaries.
- Risk assessment.
- Required approvals.
- Documentation and reporting plan.

20.6 Risk Assessment of the External Activity

Recommended Good Practice

A risk assessment should be conducted before any external activity. The assessment should be proportionate to the size and sensitivity of the activity.

- The country or region where the activity will be implemented.
- The legal and regulatory environment.
- The nature of the activity.
- The amount or value of funds or resources involved.
- The source of funding.
- The partner or implementer.
- The beneficiary entity or final beneficiary category.
- The financial or delivery channel.
- The availability of implementation evidence.
- The presence of intermediaries or third parties.
- Any sanctions, negative information, or higher-risk indicators.
- The organisation's ability to monitor, report, and close the activity.

20.7 Risk Classification of the External Activity

Recommended Good Practice

The external activity may be classified into three levels.

Low Risk

Examples may include:

- Knowledge-sharing or training cooperation with a known entity.
- An activity that does not involve transfers of funds or assistance.
- Participation in an official event or conference.
- A relationship with a well-known and documented international entity.

Appropriate measures may include:

- Documenting the activity.
- Basic verification of the partner.
- Internal approval.
- Referring to the competent authority where needed.

Medium Risk

Examples may include:

- Supporting a limited project outside the State through a known partner.
- Limited in-kind donations.
- A training or social activity with a foreign entity.
- A limited financial transfer through a formal banking channel.

Appropriate measures may include:

- Brief risk assessment.
- Partner file.
- Written agreement.
- Higher internal approval.
- Documentation of the transfer or delivery.
- Implementation report.

High Risk

Examples may include:

- Providing large-scale financial or in-kind assistance outside the State.
- Operating in a higher-risk area.
- Using a new or unknown partner.
- Multiple intermediaries.
- Difficulty in evidencing the final beneficiary.
- Public donations allocated to the external activity.
- Use of unusual financial channels.
- Presence of reputational indicators or negative news.

Appropriate measures may include:

- Detailed risk assessment.
- Enhanced due diligence.
- Board of Directors approval.
- Obtaining official approvals.
- Formal financial channels only.
- Detailed agreement.
- Periodic reports.
- Evidence of implementation and distribution.
- Post-implementation review.
- Referring to the Ministry or competent authority where any matter is unclear.

20.8 Foreign Partners and Foreign Non-Profit Organisations

Recommended Good Practice / Based on National Analysis

When dealing with a foreign partner or foreign Non-Profit Organisation, the organisation should not rely only on the party's name or stated reputation. It should verify the party's legal status and its capacity to implement the activity.

The UAE Financial Intelligence Unit report referred to crowdfunding through local accounts and foreign Non-Profit Organisations among the typologies requiring attention in the context of terrorist financing, in addition to the use of intermediaries, corporate networks, and various channels to move or conceal funds.

Minimum Due Diligence on a Foreign Partner

The organisation should obtain:

Full legal name.

Country of registration.

Evidence of registration or licensing.

Names of responsible persons or authorised representatives.

Official contact details.

Description of activities.

Previous experience.

Purpose of the relationship.

Official bank account.

Internal policies or controls where needed.

Previous reports or references where possible.

Any reputational information or negative news.

20.9 Agreements with Foreign Partners

Recommended Good Practice

A significant external activity should not be implemented without a written agreement.

The agreement should include:

- Legal names of the parties.
- Purpose of the activity.
- Target country or region.
- Scope of work.
- Roles and responsibilities.
- Budget or resources.
- Payment or delivery channels.
- Prohibition on the use of personal accounts.
- Prohibition on transferring funds to a third party without approval.
- Beneficiary selection criteria.
- Reporting requirements.
- Evidence of implementation required.
- Data protection and confidentiality.
- Use of the organisation's name and logo.
- The organisation's right to review or request documents.
- Mechanism for dealing with breaches.
- Right of termination.
- Obligation to comply with applicable laws and instructions.

20.10 Financial Transfers Abroad

Recommended Good Practice

External transfers should be made through formal and documented channels, and should be linked to a clear purpose and appropriate approval.

Before the Transfer

The organisation should verify:

- Internal approval exists.
- Official approval or permit exists where required.
- The purpose is clear.
- An agreement or supporting document exists.
- The bank account is in the name of the beneficiary entity or partner.
- There is no unjustified third party.
- There are no unresolved reputational or risk indicators.
- It is possible to obtain a report on the use of funds.

After the Transfer

The organisation should retain:

- Proof of transfer.
- Invoice, payment request, or approval decision.
- Confirmation of receipt.
- Report on the use of funds.
- Evidence of implementation or distribution.
- Any related correspondence.

20.11 Prohibition on Informal Channels and Personal Accounts

Risk Indicator / Recommended Good Practice

The organisation should avoid using informal channels or personal accounts in external activities.

Risk Indicators

- Request to transfer funds to a personal account.
- Request to use an unlicensed hawala channel.
- Request to split transfers without justification.
- Request to transfer funds to an entity not mentioned in the agreement.
- Request for cash delivery outside formal channels.
- Change of bank account immediately before the transfer.
- Refusal to provide official account documents.

Appropriate Action

- Do not execute the transfer.
- Request clarification and documents.
- Escalate the case internally.
- Refer to the Ministry or competent authority where needed.
- Document the decision.

20.12 Cross-Border In-Kind Assistance

Recommended Good Practice

The organisation may provide in-kind assistance outside the State, such as food items, clothing, equipment, devices, or medical materials. Such assistance requires careful documentation because it may be difficult to trace after delivery.

The organisation should document:

- Type of items.
- Estimated value.
- Quantity.
- Source of items.
- Purpose.
- Beneficiary entity.
- Method of transport.
- Shipping or delivery documents.
- Proof of receipt.
- Distribution or use report.
- Any customs or regulatory requirements.

Any sending or transfer of in-kind assistance outside the State should observe the requirements of the competent authorities.

20.13 Final Beneficiaries Outside the State

Recommended Good Practice

In external activities, the organisation may not be able to verify every final beneficiary directly. However, it should have a reasonable and proportionate system to evidence that assistance reached the target group.

- Proposed Controls
- Identify the beneficiary category.
- Establish clear selection criteria.
- Do not accept beneficiary lists without review.
- Request distribution lists or reports.
- Use codes or limited data to protect privacy.
- Review a sample of cases where possible.
- Request photographs or implementation evidence while respecting dignity and privacy
- Maintain a complaints or feedback mechanism where possible.

20.14 Activities or Volunteering Opportunities Outside the State

Legal Obligation / Requires Confirmation When Applied

The Executive Regulation of the Voluntary Work Law refers to controls relating to the practice of voluntary work outside the State, including that the volunteering opportunity outside the State must not conflict with the policies and legislation of the State, must serve the State's vision and directions regarding its foreign policy, and must meet the conditions and requirements of the authorities concerned with foreign affairs.

Before Organising a Volunteering Opportunity Outside the State

The organisation should verify:

- Appropriate approval or licensing exists.
- The organising entity is clear.
- The country or region targeted is clear.
- Travel or implementation risks have been assessed.
- Volunteers are protected.
- The partner or beneficiary entity is identified.
- No fundraising is conducted without approval.
- Health and safety arrangements exist.
- The activity is consistent with the State's policies and the instructions of the competent authorities.
- Communication and emergency plans exist.

20.15 Fundraising for Activities Outside the State

Legal Obligation / Requires Confirmation When Applied

If the external activity is funded by donations, the organisation must ensure compliance with the Donation Regulation Law and its Executive Regulation, including the permit, purpose, beneficiary entity or category, methods, collection period, donation provision period, and reports. The Donation Regulation Law prohibits natural persons from collecting donations and requires a permit for entities that are not licensed entities.

Practical Requirements

The campaign file should be clear regarding:

- The external or cross-border purpose.
- Country or beneficiary entity.
- Implementing partner.
- Method of transferring funds or resources.
- Campaign duration.
- Channels used.
- Reporting plan.
- How delivery of assistance will be evidenced.

20.16 Crowdfunding and Cross-Border Platforms

Risk Indicator / Based on National Analysis

Crowdfunding through cross-border platforms or accounts may be legitimate in some cases, but it requires particular care.

The UAE Financial Intelligence Unit report referred to crowdfunding through local accounts and foreign Non-Profit Organisations, as well as crypto-asset crowdfunding, among the typologies requiring attention in the context of terr orist financing.

Proposed Controls

- Do not use unapproved crowdfunding platforms.
- Do not receive funds through personal accounts.
- Verify the permit before launching the campaign.
- Understand who manages the platform and who receives the funds.
- Reconcile platform reports with the bank account.
- Monitor large, structured, or unusual donations.
- Document donors and amounts according to applicable requirements.
- Refer to the competent authority where matters are unclear.

20.17 Virtual Assets and Crypto-Assets in Cross-Border Activities

Risk Indicator / Requires Confirmation

Virtual assets or crypto-assets may be used to transfer or collect funds across borders, but they raise higher risks relating to source identification, traceability, compliance, and volatility.

The UAE Financial Intelligence Unit report referred to crypto-asset crowdfunding and the use of virtual assets within certain fund movement typologies.

Practical Rule

The organisation should not accept, transfer, or use any virtual assets or cryptoassets in cross-border activities unless it has obtained clear guidance from the Ministry, the competent authority, and the relevant regulatory authorities.

20.18 Data Protection in Cross-Border Activities

Recommended Good Practice

External activities may require the sharing of beneficiary, volunteer, or partner data with parties outside the State. This requires particular care.

The organisation should observe:

- Sharing the minimum necessary data.
- Having a lawful and clear purpose.
- Protecting data from unauthorised access.
- Not sharing sensitive data unless necessary.
- Using aggregated or anonymised data where possible.
- Agreeing with the partner on confidentiality and data protection.
- Not publishing beneficiary images without appropriate consent.

Any transfer or sharing of personal data outside the State should be aligned with national legislation, the instructions of the competent authority, and data protection requirements.

20.19 Use of the Organisation's Name Abroad

Recommended Good Practice

When implementing an external activity, the organisation should control the use of its name and logo.

The organisation should prohibit:

01 Use of the organisation's logo by the foreign partner without approval.

02 Launching external campaigns in the organisation's name without a permit.

03 Publishing donation links in the organisation's name outside official channels.

04 Using the organisation's name in political, partisan, military, or unclassified activities.

05 Issuing external media statements without approval.

External partnership agreements should include a clear clause on the use of the organisation's name, logo, and media materials.

20.20 Reports and Evidence After Implementation

Recommended Good Practice

After implementing any external activity, a closing report should be prepared in a manner proportionate to the size and risk of the activity.

The report should include:

- Description of the activity.
- Country or region.
- Partner or beneficiary entity.
- Purpose.
- Sources of funding.
- Amounts or resources used.
- Transfer or delivery channels.
- Beneficiary categories.
- Evidence of implementation.

- Photographs or documents where appropriate.
- Challenges.
- Any risk indicators or complaints.
- Remaining balance, if any.
- Recommendations or lessons learned.

20.21 Risk Indicators in Cross-Border Activities

The organisation should pay attention to the following indicators:

- A foreign partner does not provide registration documents.
- A request is made to transfer funds to an account not belonging to the partner.
- A third party directs the relationship without appearing in the agreement.
- A request is made to use informal channels.
- Pressure is applied to execute the transfer quickly.
- Difficulty in evidencing the final beneficiary.
- Refusal to provide reports or evidence of distribution.
- Multiple intermediaries without justification.
- Bank account changes before the transfer.
- Use of a foreign Non-Profit Organisation of unclear status.
- Use of an unapproved crowdfunding platform.
- Request to donate or transfer through virtual assets.
- External activity is inconsistent with the organisation's classification.
- Negative information exists about the partner, region, or channel.
- Use of the organisation's name abroad without approval.

20.22 Cross-Border Activities Register

Recommended Good Practice

The organisation should maintain a dedicated register for cross-border activities or relationships.

The register should include:

- Name of the activity.
- Country or region.
- Partner or beneficiary entity.
- Purpose.
- Date of internal approval.
- Official approvals, if any.
- Risk level.
- Source of funding.
- Transfer or delivery channel.
- Value of funds or resources.
- Required reports.
- Closure date.
- Any risk indicators or corrective actions.

20.23 Checklist Before Implementing an External Activity

Before implementing an external activity, the organisation should verify:

- The activity is consistent with the organisation's objectives and classification.
- The official approvals or permits required have been identified.

- The target country or region is clear.
- The partner or beneficiary entity has been verified.
- The final beneficiary category is defined.
- The source of funding is clear.
- Donation requirements have been checked, where donations are involved.
- Formal financial channels will be used.
- No personal accounts or informal channels will be used.
- A written agreement exists where a partner is involved.
- Risks relating to the country, partner, channel, and beneficiaries have been assessed.
- Data protection arrangements are in place.
- Volunteer requirements have been checked, where volunteers are involved.
- Reporting and evidence of implementation are defined.
- The Ministry or competent authority has been consulted where the requirement is unclear.

20.24 Self-Assessment Questions for Cross-Border Activities

The organisation may use the following questions:

- Do we have a policy or procedure for external activities?
- Do we know when official approval is required?
- Do we verify foreign partners?
- Do we use formal financial channels only?
- Do we prohibit personal accounts and informal channels?
- Do we know who the final beneficiary is?
- Can we evidence delivery of assistance?
- Do we assess country, region, or partner risks?
- Do we have written agreements with external partners?
- Do we review national risk indicators relating to cross-border activities?
- Do we protect beneficiary data when sharing it with external parties?
- Do we prepare closing reports for external activities?
- Does the Board review higher-risk external activities?
- Do we refer to the Ministry or competent authority where matters are unclear?

20.25 Chapter Summary

Cross-border activities may be a legitimate and important part of the work of Non-Profit Organisations, but they require clearer governance, stronger due diligence, more accurate documentation, and more regular follow-up.

The rules of this chapter may be summarised as follows:

01 No external activity should be carried out without a clear understanding of the purpose and scope.

02 No external partnership should be entered into without verifying the partner.

03 No external transfers should be made without formal channels and supporting documents.

04 Personal accounts and informal channels should not be used.

05 Fundraising for external activities should not be carried out without a permit or approval where required.

06 Virtual assets or crypto-assets should not be used without official confirmation.

07 The organisation should not rely entirely on the partner without reports and evidence of implementation.

08 Beneficiary data and dignity should be protected.

09 Every external activity should be documented from planning to closure.

10 The Ministry or competent authority should be consulted where matters are unclear.

By applying these principles, cross-border activities become an organised and protected area of work, rather than a vuln erability that may be exploited or misunderstood.

Preparing for Mutual Evaluation and Demonstrating Effectiveness

21

Preparing for Mutual Evaluation and Demonstrating Effectiveness

21.1 Purpose of this Chapter

This chapter aims to help Non-Profit Organisations understand how to demonstrate the effectiveness of their systems and controls in protecting the sector from abuse, particularly in the context of national assessments, supervisory reviews, or mutual evaluations conducted under the FATF Methodology. This chapter does not mean that Non-Profit Organisations become responsible for the State's mutual evaluation. That role belongs to the competent government authorities. Rather, the purpose is to enable organisations to present a clear and documented picture of their understanding of risks, their application of controls, their cooperation with the Ministry or competent authority, and their ability to demonstrate that their activities, resources, donations, partnerships, and volunteers are managed in an effective, transparent, and risk-based manner.

21.2 What is Meant by Demonstrating Effectiveness?

FATF Recommendations / Recommended Good Practice

Demonstrating effectiveness means that the organisation is able to show that it has a practical system that is actually applied, not merely written documents.

Effectiveness does not mean only having:

- A donations policy.
- A risk assessment.
- A volunteer register.
- A partner file.
- A Board decision.
- A training record.

These documents are important, but they are not sufficient by themselves. The organisation should be able to show how these documents affected actual decisions and behaviours.

For example, effectiveness may be demonstrated where:

01 A high-risk donation was reviewed before acceptance.

02 A donation was rejected or suspended because of risk indicators.

03 A partner was approved only after due diligence.

04 A volunteer was trained and prevented from collecting donations without approval.

05 A risk indicator was reported, escalated, and closed.

06 A supervisory observation was addressed through corrective action.

07 The Board reviewed key risks and made documented decisions.

08 Records showed that assistance reached the intended beneficiary category.

In other words, effectiveness is about practical application, results, and evidence.

21.3 Relationship Between this Chapter and Immediate Outcome 10

Immediate Outcome 10 under the FATF Methodology assesses, among other matters, whether terrorists, terrorist organisations, and terrorist financiers are prevented from abusing the Non-Profit Organisation sector.

Although Immediate Outcome 10 primarily assesses the effectiveness of the State and competent authorities, Non-Profit Organisations contribute to demonstrating effectiveness through their day-to-day application of controls.

The organisation can support effectiveness by showing that it:

- Understands its risk exposure.
- Knows whether it falls within activities that may be more exposed to abuse.
- Applies controls proportionate to risk.
- Cooperates with the Ministry and competent authority.
- Maintains records and reports.
- Implements donation, partner, beneficiary, and volunteer controls.
- Identifies and escalates risk indicators.
- Takes corrective action when weaknesses are identified.
- Avoids measures that unnecessarily disrupt legitimate activity.

21.4 Difference Between Having a System and Applying a System

There is an important difference between having a system and applying a system.

Having a System means that the rganisation has written policies, procedures, templates, registers, and files.

Applying a System means that these olicies, procedures, templates, registers, and files are used in real cases and influence actual decisions.

For example:

01 A donations policy exists, but a large conditional donation was accepted without review. This shows that the policy exists but may not be applied.

02 A donations policy exists, but a large conditional donation was accepted without review. This shows that the policy exists but may not be applied.

03 A volunteer undertaking prohibits fundraising, and a volunteer who published a donation link was stopped, recorded, and retrained. This shows practical application.

04 A Board meeting discussed a serious financial discrepancy and approved corrective action. This shows oversight in practice.

The organisation should therefore focus not only on presenting documents, but alsoon explaining how they are used.

21.5 What Evidence Demonstrates Effectiveness?

Evidence of effectiveness may include different types of documents, records, decisions, reports, and practical examples.

Examples include:

- Approved internal policies and procedures.
- Risk assessment and risk register.
- Donation register.
- Fundraising campaign files.
- Donation acceptance, suspension, rejection, or return decisions.
- Partner due diligence files.
- Agreements or memoranda of understanding with partners.
- Beneficiary eligibility records and evidence of delivery.
- Volunteer registration records and Volunteer Charter acceptance.
- Records showing that volunteers were instructed not to collect donations.
- Bank statements and bank reconciliations.
- Campaign closing reports.
- Board meeting minutes.
- Conflict of interest disclosures.
- Training records and materials.
- Risk indicator and incident register.
- Bank statements and bank reconciliations.
- Campaign closing reports.
- Board meeting minutes.
- Conflict of interest disclosures.
- Training records and materials.
- Risk indicator and incident register.
- Corrective action plans and closure evidence.
- Supervisory correspondence with the Ministry or competent authority.
- Examples of referrals made where matters were unclear.
- Internal review or inspection reports.
- Evidence that policies were updated after incidents or observations.

The strongest evidence is not the largest number of documents, but the evidence that shows a clear link between risk, decision, action, and result.

21.6 How Should the Organisation Explain its Risks?

When explaining its risks, the organisation should avoid general answers. It should explain its actual operating context.

A strong explanation should cover:

- The organisation's approved objectives and classification.
- Main activities and programmes.
- Whether it collects or receives donations.
- Main sources of funding.

- Whether it uses digital channels or cash.
- Whether it works with partners or beneficiary entities.
- Whether it has activities outside the State.
- Whether it uses volunteers.
- Types of beneficiaries or beneficiary categories.
- Main risk indicators relevant to its work.
- Controls applied to manage those risks.
- How risks are reviewed and updated.

For example, rather than saying "our organisation is low risk", the organisation should explain why:

"The organisation carries out local awareness and cultural activities, does not collect public donations, does not transfer funds outside the State, does not use cash donation channels, and maintains records of activities, volunteers, and Board approvals. Therefore, its risk exposure is limited, while basic governance, recordkeeping, and volunteer controls are applied."

Similarly, a higher-risk organisation should not deny its exposure. It should show that it understands and manages it:

"The organisation collects donations through approved channels and implements assistance programmes through partners. For this reason, it applies donor review, campaign files, partner due diligence, formal payment channels, beneficiary documentation, and post-implementation reporting."

21.7 How Can the Organisation Demonstrate that it Applies the Risk- Based Approach?

The organisation demonstrates the risk-based approach when it can show that it does not apply the same controls to every case, but adjusts controls according to risk.

Evidence may include:

- Simplified review for low-risk activities.
- Standard review for ordinary activities, partners, or donations.
- Enhanced review for higher-risk donations, partners, cross-border activities, or unusual channels.
- Escalation of higher-risk cases to management or the Board.
- Additional information requested where risk indicators arise.
- Rejection or suspension of cases where risk remains unclear.
- Updating the risk assessment when activities change.
- Referring to the Ministry or competent authority where requirements are unclear.

A strong organisation should be able to explain why a case was considered low, medium, or high risk, and what measures were applied accordingly.

21.8 Strong Examples of Evidence of Effectiveness

Examples of strong evidence include:

- A fundraising campaign file showing the permit, approved materials, collection channels, amounts collected, expenditure, beneficiary records, and closing report.
- A donation case where a large conditional donation was reviewed, escalated, and accepted only after clarification, or rejected because the condition was unclear.
- A partner file showing legal status, agreement, due diligence, bank account verification, reports, evidence of implementation, and closure.
- A volunteer file showing registration, task assignment, Volunteer Charter acceptance, training, prohibition on fundraising, and return of entrusted items.
- A risk indicator register showing that an unauthorised donation link was detected, removed, reviewed, and followed by updated training.
- Board minutes showing that management reported supervisory observations and that the Board approved corrective action.
- A corrective action plan showing the root cause, action taken, responsible person, deadline, and evidence of closure.
- Training materials updated after a national risk indicator or supervisory observation.
- Evidence that the organisation consulted the Ministry or competent authority before proceeding with an unclear or higher-risk activity.

21.9 Using the UAE Financial Intelligence Unit Report to Demonstrate Readiness

The UAE Financial Intelligence Unit report on terrorist financing typologies and facilitators is an important source for understanding national risk indicators and updating internal controls, training, and supervision.

The organisation may use the report to demonstrate readiness by showing that it has:

- Reviewed relevant typologies and indicators.
- Updated training materials based on relevant indicators.
- Considered risks relating to crowdfunding, virtual assets, foreign Non-Profit
- Organisations, intermediaries, local accounts, corporate networks, and informal channels.
- Updated donation and partner due diligence procedures.
- Trained staff and volunteers on relevant indicators.
- Incorporated relevant indicators into its risk and incident register.
- Used national indicators in internal review or inspection planning.

The organisation does not need to reproduce the entire report. It should use the parts relevant to its activities and risk exposure.

21.10 What May Assessors or Inspectors Ask About?

Assessors or inspectors may ask practical questions such as:

- What does the organisation do?
- What is its legal status and classification?
- Does it collect donations?
- How does it ensure that donations are authorised and recorded?
- How does it deal with anonymous, conditional, or unusual donations?
- Does it work with partners?
- How are partners reviewed and approved?
- How does the organisation know that assistance reached beneficiaries?
- Does it work outside the State?
- What approvals and controls are applied to external activities?
- Does it use volunteers?
- How are volunteers registered, trained, and supervised?
- How does the organisation prevent volunteers from collecting donations without approval?
- How does it protect beneficiary data and dignity?
- How does it identify and escalate risk indicators?
- What corrective actions were taken after observations or incidents?
- How does the Board oversee risks?
- What training was provided?
- Can the organisation show practical examples?

The organisation should prepare to answer these questions with evidence, not only general statements.

21.11 How Should the Organisation Answer Effectively?

A strong answer should be clear, factual, and supported by records.

A useful answer structure is:

01 Explain the rule or procedure.

02 Explain how it is applied in practice.

03 Provide a concrete example.

04 Refer to the supporting evidence.

05 Explain what was improved or learned.

For example:

"We have a procedure for reviewing higher-risk donations. In 2026, we received a conditional donation that required additional review because the beneficiary entity was unclear. The donation was suspended additional information was requested, the case was escalated to management, and the donation was not accepted until the purpose and beneficiary were clarified. The decision is recorded in the donation register and the related file."

This type of answer is stronger than saying: "We have a donations policy."

21.12 Answers to Avoid

The organisation should avoid answers that are general, unsuppor ted, or inconsistent with records.

Examples of weak answers include:

- "We have no risks because we are charitable."
- "We trust our donors."
- "Our partners are known to us."
- "We have policies, but we do not have examples."
- "The volunteer knows what to do."
- "We do not keep this record, but we can explain verbally."
- "We do not need approvals because our purpose is good."
- "We have never had a problem, so we are low risk."
- "The partner handles the beneficiaries; we do not follow up."
- "We collect donations through personal contacts, but only for good purposes."
- "We will prepare the records later if needed."

Such answers may suggest that controls are not applied in practice

21.13 Effectiveness Evidence File

The organisation may maintain an effectiveness evidence file to demonstrate its practical implementation of governance, compliance, and risk-based controls.

The file may include:

- Legal status, licence, declaration, and classification.
- Summary of activities and risk profile.
- Internal risk assessment and risk register.
- Donations policy and donation register.
- Sample fundraising campaign files.
- Sample donation review cases.
- Partner due diligence files.
- Beneficiary and delivery evidence.
- Volunteer records and training evidence.
- Bank account and financial control records.
- Board minutes relating to risks and oversight.
- Training plan and training register.
- Risk indicator and incident register.
- Corrective action plans.
- Supervisory correspondence and responses.
- Examples of referrals to the Ministry or competent authority.
- Evidence of improvements made after observations.

The file should be organised and updated periodically. It should not include unnecessary sensitive personal data unless needed and properly protected.

21.14 Effectiveness Matrix

The organisation may use an effectiveness matrix to connect requirements with evidence.

Area	What Should Be Demonstrated?	Possible Evidence
Risk Understanding	The organisation understands its activities and exposure to risk.	Risk assessment, risk register, Board discussion, updated controls.
Donations	Donations are authorised, recorded, reviewed, and used for approved purposes.	Donation register, campaign file, permits, bank records, clos ingreports.
Partners	Partners are reviewed, approved, and followed up.	Partner file, due diligence form, agreement, reports, evidence of implementation.
Beneficiaries	Assistance reaches the intended purpose or beneficiary category.	Eligibility records, delivery evidence, partner reports, complaints records.
Volunteers	Volunteers are registered, trained, and prevented from unauthorised fundraising.	Volunteer register, task assignment, Volunteer harter, training record.
Financial Controls	Funds are managed through official channels and documented.	Bank statements, reconciliations, payment approvals, audit reports.
Risk Indicators	Indicators are identified, escalated, and closed.	Incident register, escalation record, corrective action evidence.
Governance	The Board oversees risks and key decisions.	Board minutes, decisions, reports to the Board, policy approvals.
Training	Relevant persons understand their responsibilities.	Training plan, materials, attendance, scenario exercises.
Corrective Actions	Weaknesses are addressed and not repeated.	Corrective action plan, closure evidence, updated procedure.

21.15 How Should the Organisation Prepare for an Assessment Interview or Visit?

Before an assessment interview, supervisory visit, or inspection, the organisation should prepare in a structured manner.

Preparation may include:

- Reviewing the organisation's legal status and classification.
- Preparing a short summary of activities and risk profile.
- Identifying key documents and evidence.
- Reviewing recent donations, campaigns, partners, volunteers, and risk indicators.
- Preparing examples of decisions and controls applied.
- Ensuring that staff know their roles and procedures.
- Ensuring that answers are consistent with records.
- Reviewing supervisory observations and corrective actions.
- Preparing to explain both strengths and improvements.
- Avoiding unsupported claims.

The organisation should not prepare by creating artificial evidence. It should organise existing evidence and be transparent about any weaknesses and corrective actions.

21.16 Key Messages the Organisation Should Demonstrate

In an assessment or inspection context, the organisation should be able to demonstrate the following messages:

- We understand our legal status and approved classification.
- We understand our activities and risk exposure.
- We apply controls that are proportionate to risk.
- We do not treat policies as paper documents only.
- We document donations, partners, beneficiaries, volunteers, and decisions.
- We use official financial channels and avoid personal accounts.
- We train relevant persons according to their roles.
- We identify and escalate risk indicators.
- We cooperate with the Ministry or competent authority.
- We update controls when observations or incidents arise.
- We protect legitimate activity while preventing abuse.

21.17 Common Mistakes in Demonstrating Effectiveness

Common mistakes include:

- Focusing only on laws and policies without practical examples.
- Saying the organisation is low risk without explaining why.
- Not being able to show donation or partner files.
- Providing answers that contradict records.
- Treating volunteers as informal helpers without records or controls.

- Saying that partners handle everything without follow-up.
- Not documenting risk indicators or corrective actions.
- Not involving the Board in key risk decisions.
- Not being able to explain how training changed behaviour.
- Not updating policies after incidents or supervisory observations.
- Providing excessive documents without explaining their relevance.
- Not distinguishing between legal obligations and recommended practices.

21.18 Role of the Board of Directors in Demonstrating Effectiveness

Recommended Good Practice

The Board of Directors plays an important role in demonstrating effectiveness because senior oversight reflects the seriousness of the organisation 's governance system.

The Board should be able to show that it:

- Approves core policies.
- Reviews financial and supervisory reports.
- Follows up on material observations.
- Discusses risks.
- Approves sensitive decisions.
- Follows up on corrective actions.
- Ensures that adequate training and resources are available.
- Reviews important cases, such as rejection of a donation or termination of a partnership.

Appropriate evidence may include:

- Meeting minutes.
- Board decisions.
- Management reports submitted to the Board.
- Corrective action plans.
- Annual reviews of risks and policies.

21.19 Role of the Ministry or Competent Authority

Supervisory Requirement / Requires Confirmation When Applied

The organisation is not alone in demonstrating effectiveness. It operates within a national system led by the Ministry or competent authority, including licensing, classification, supervision, awareness, risk assessment, and identification of the subset most exposed to risk.

The organisation should demonstrate cooperation with this system through:

- Compliance with its classification.
- Submission of data when requested.
- Implementation of guidance and observations.
- Participation in awareness or training where applicable.
- Responding to inspection findings.
- Referring unclear matters through approved channels.
- Maintaining records that support supervisory review.
- Cooperation with the Ministry or competent authority is itself an important indicator of governance and effectiveness.

21.20 Self-Assessment Questions for Demonstrating Effectiveness

The organisation may use the following questions:

- Can we explain our legal status and classification clearly?
- Can we explain our main risks and why they are low, medium, or high?
- Can we show practical examples of controls applied?
- Can we show a donation that was reviewed, suspended, rejected, or escalated?
- Can we show a partner file with due diligence and follow-up?
- Can we evidence delivery of assistance or services?
- Can we show that volunteers were registered, briefed, and instructed not to collect donations?
- Can we show that risk indicators were recorded and closed?
- Can we show that the Board discussed risks and corrective actions?
- Can we show that training was delivered and used in practice?
- Can we show how we responded to supervisory observations?
- Are our answers consistent with our records?
- Can we explain what we improved after a weakness or incident?
- Do we know when to refer to the Ministry or competent authority?
- Can we demonstrate that our controls protect legitimate work rather than
- disrupt it?

21.21 Chapter Summary

Preparing for mutual evaluation or supervisory review is not about memorising answers. It is about being able to demonstrate that the organisation's controls are real, proportionate, and applied in practice.

The key messages of this chapter are as follows:

01 Effectiveness means practical implementation, not merely written policies.

02 Evidence should show how risks were identified, decisions were made, controls were applied, and outcomes were documented.

03 The organisation should be able to explain its actual risk profile.

04 The risk-based approach should be demonstrated through different levels of controls according to risk.

05 Strong evidence includes real examples, such as reviewed donations, partner due diligence, volunteer controls, Board oversight, training, and corrective actions.

06 The organisation should avoid unsupported or overly general answers.

07 An effectiveness evidence file and effectiveness matrix can help organise evidence.

08 The Board of Directors has a key role in demonstrating oversight.

09 Cooperation with the Ministry or competent authority supports the national effectiveness framework.

10 Where weaknesses exist, the organisation should explain corrective action and improvement.

By applying these principles, the organisation can present itself clearly and professionally in any supervisory review, national assessment, or mutual evaluation context, and can demonstrate that it contributes to protecting the Non-Profit Organisation sector from abuse while enabling legitimate public benefit work.

Roles and Responsibilities within the Organisation

22

Roles and Responsibilities within the Organisation

22.1 Purpose of this Chapter

This chapter aims to clearly define roles and responsibilities within Non-Profit Organisations, so that each internal party understands what is required of it in relation to governance, donations, financial management, partners, beneficiaries, volunteers, records, risk indicators, and communication with the Ministry or the competent authority.

Having good policies and procedures is not sufficient if responsibilities are not clearly assigned. Many weaknesses do not arise because rules are absent, but because it is unclear who approves, who implements, who reviews, who escalates, and who retains the evidence.

22.2 Principle of Shared Responsibility

Recommended Good Practice

Compliance and protecting the organisation from misuse are not the responsibility of one person only. They are a shared responsibility among:

- The Board of Directors.
- Executive management.
- The finance officer.
- The compliance officer or focal point.
- Donations teams.
- Programme and project teams.
- The volunteer coordinator.
- Employees.
- Volunteers.
- Partners, within the scope of the contractual relationship.

However, shared responsibility does not mean overlapping authorities or absence of accountability. The role of each party should therefore be clearly defined.

22.3 Board of Directors

Governance Obligation / Recommended Good Practice

The Board of Directors represents the oversight level within the organisation. It should ensure that the organisation operates within its approved purposes, that its resources are used for the purposes for which it was established, and that risks are understood and managed.

Key Responsibilities

Subject to the articles of association and approved authorities, the Board of Directors is responsible for:

- Approving core policies.
- Approving the authority matrix.
- Reviewing the institutional risk assessment.
- Approving higher-risk activities, partnerships, or donations.
- Reviewing financial reports and final accounts.
- Following up on major fundraising campaigns.
- Following up on supervisory observations and corrective actions.
- Reviewing material conflicts of interest.
- Monitoring the performance of executive management.
- Ensuring that adequate resources are available for compliance and training.

- Ensuring cooperation with the Ministry or competent authority.
- Reviewing material cases relating to risk indicators.

Examples of Decisions that Should be Referred to the Board

- Approval of the donations policy.
- Acceptance of a large or high-risk donation.
- Entering into an external or higher-risk partnership.
- Approval of an activity outside the State.
- Termination of a partner relationship due to a material breach.
- Approval of a corrective action plan following a significant supervisory observation.
- Review of a financial or audit report containing material findings.
- Change of authorised signatories or bank accounts.

22.4 Executive Management

Recommended Good Practice

Executive management is responsible for translating Board decisions and approved policies into daily practical implementation. It acts as the link between the oversight level and the operational level.

Key Responsibilities

- Executive management is responsible for:
- Implementing policies and procedures.
- Supervising work teams.
- Ensuring that records are maintained.
- Following up compliance with the approved classification and activities.
- Monitoring fundraising campaigns in accordance with permits.
- Overseeing paratners and beneficiaries.
- Ensuring training of employees and volunteers.
- Escalating material matters to the Board of Directors.
- Following up on requests from the Ministry or competent authority.
- Implementing corrective action plans.
- Ensuring that operational decisions are documented.
- Managing the organisation's day-to-day risks.

Executive Management Should Avoid

- Implementing activities outside the approved classification or licence without confirmation.
- Launching fundraising campaigns without permit or review.
- Relying on verbal decisions in material matters.
- Leaving partner or volunteer files incomplete.
- Delaying escalation of risk indicators.
- Sending information to the competent authority or the bank without review and consistency.

22.5 Finance Officer

Recommended Good Practice / Legal Obligation where linked to financial records

The finance officer plays a central role in protecting the organisation's funds and ensuring that donations, resources, and expenditures are documented and traceable.

Key Responsibilities

The finance officer is responsible for:

- Managing financial records.
- Recording revenues and donations.
- Monitoring bank accounts.
- Performing bank reconciliations.
- Ensuring the existence of supporting documents for disbursements.
- Verifying approvals before payment.
- Preparing financial reports.
- Preparing fundraising campaign financial data.
- Monitoring administrative and operational expenses related to donations.
- Supporting the preparation of final accounts and budgets.
- Retaining transfer and payment documents.
- Escalating any unusual discrepancies or financial indicators.

The Donation Regulation Law requires licensed and authorised entities to maintain regular electronic accounting records relating to donations. The Executive Regulation specifies that donation records should include the sources of donations, proceeds, purpose, methods and areas of expenditure, and beneficiary entities, and that such records should be retained for no less than ten years.

Indicators that the Finance Officer Should Escalate

- Use of a personal account.
- Large or unusual donation.
- Transfer to an account that does not belong to the partner or supplier.
- Repeated discrepancies in cash or records.
- Request to return a donation to a different account.
- Payment without sufficient supporting documents.
- Donation register not matching the bank account.
- Request for urgent transfer without approvals.

22.6 Compliance Officer or Focal Point

Recommended Good Practice

Not every organisation will have an independent compliance function, particularly smaller organisations. However, there should be a focal point or person responsible for following up on the application of policies, risk management, and internal communication regarding risk indicators.

Key Responsibilities

The compliance officer or focal point is responsible for:

- Following up implementation of internal policies.
- Preparing or updating the risk assessment.

- Monitoring the risk indicator and incident register.
- Supporting training for employees and volunteers.
- Reviewing unusual cases.
- Coordinating responses to supervisory requests.
- Following up corrective actions.
- Preparing short reports for management or the Board.
- Updating risk indicator lists.
- Integrating national risk indicators into procedures and training.
- Coordinating with finance, programmes, and volunteer teams.
- Recommending referral to the Ministry or competent authority where matt ers are unclear.

Important Note

The existence of a compliance officer does not exempt other parties from their responsibilities. The finance officer remains responsible for financial records, the volunteer coordinator for volunteers, and the programme officer for partners and beneficiaries.

22.7 Donations Officer or Fundraising Team

Legal Obligation / Recommended Good Practice

If the organisation collects, receives, or provides donations, there should be a clearly identified person or team responsible for managing this process.

Key Responsibilities

The donations officer or relevant team is responsible for:

- Verifying the organisation's legal status in relation to fundraising.
- Preparing permit or approval applications where required.
- Reviewing advertising and publicity materials.
- Ensuring that official channels only are used.
- Preventing the use of personal accounts.
- Linking each campaign to its purpose and permit.
- Coordinating with the finance officer on the donation register.
- Following up unusual donations.
- Preparing campaign reports.
- Maintaining the campaign file.
- Escalating any risk indicator relating to a donor, channel, or campaign.
- Ensuring that volunteers do not participate in fundraising without prior approval.

The Donation Regulation Law prohibits natural persons from collecting donations. Entities other than licensed entities may not establish, organise, or carry out any act aimed at collecting donations unless they have obtained a permit from the competent authority.

22.8 Programme and Project Officer

Recommended Good Practice

The programme and project officer is the party closest to activities, partners, and beneficiaries. This role is therefore essential in demonstrating that programmes \achieve their approved purpose.

Key Responsibilities

The programme officer is responsible for:

- Ensuring that the activity falls within the organisation's objectives and classification.
- Preparing the activity or project description.
- Identifying beneficiary categories.
- Establishing beneficiary selection criteria.
- Assessing partners or coordinating their assessment.
- Monitoring programme implementation.
- Collecting evidence of implementation.
- Preparing programme reports.
- Protecting beneficiary data and dignity.
- Escalating any risk indicator relating to a partner or beneficiary.
- Coordinating with the finance officer on budgets and expenditure.
- Coordinating with the volunteer coordinator where volunteers are used.

Examples of Evidence Retained by the Programme Officer

- Project plan.
- Beneficiary list or beneficiary category.
- Eligibility criteria.
- Implementation reports.
- Evidence of receipt or distribution.
- Photographic evidence where appropriate and with due regard to privacy.
- Partner assessment.
- Closing report.

22.9 Volunteer Coordinator

Legal Obligation / Recommended Good Practice

- If the organisation organises volunteering opportunities, there should be a clearly identified person responsible for managing volunteers and volunteering opportunities.

Key Responsibilities

The volunteer coordinator is responsible for:

- Verifying registration or licensing of the volunteering opportunity.
- Verifying volunteer registration in accordance with requirements.
- Ensuring acceptance of the Volunteer Charter.
- Defining volunteer tasks.
- Providing necessary briefing or training.
- Explaining the prohibition on fundraising without approval.
- Protecting volunteer data.
- Coordinating with programme teams regarding volunteer interaction with beneficiaries.
- Monitoring attendance and volunteer hours.

Recovering entrusted items or cards after completion of the task.

Recording any breach or risk indicator.

Escalating material breaches to management.

The Voluntary Work Law requires entities organising voluntary work to define volunteer tasks, qualify volunteers, provide the necessary requirements for them to perform the task, maintain the confidentiality of personal information, and ensure that registration requirements are met. Volunteers are also required to comply with instructions, the Volunteer Charter, and confidentiality obligations.

22.10 Employees

Recommended Good Practice

Every employee within the organisation is responsible for complying with the instructions relevant to their role and for reporting any risk indicator or breach they observe.

Employee Responsibilities

Employees are responsible for:

- Complying with policies and procedures.
- Not exceeding their authority.
- Maintaining records related to their work.
- Protecting donor, beneficiary, and volunteer data.
- Not using the organisation's name without authorisation.
- Not collecting or advertising donations except in accordance with authorisedpowers.

22.11 Volunteers

Legal Obligation / Recommended Good Practice

Volunteers represent the organisation while performing their tasks. Their responsibilities should therefore be clear and limited.

- Volunteer Responsibilities
- Volunteers are responsible for:
- Complying with the Volunteer Charter.
- Performing only the tasks assigned to them.
- Complying with the instructions of the organising entity.
- Maintaining confidentiality of information.
- Respecting beneficiaries and their dignity.
- Not collecting donations except with prior approval from the Ministry and in accordance with approved procedures.
- Not using the organisation's name or logo outside the assigned task.
- Not publishing images or data without approval.
- Reporting any risks or breaches.
- Returning entrusted items, cards, or tools after completion of the task.

Volunteers and volunteer teams are prohibited from collecting donations, allowing donations to be collected, or advertising donations by any means except with prior approval from the Ministry.

22.12 Partners

Recommended Good Practice

A partner is not an internal part of the organisation, but it assumes specific responsibilities under the agreement, memorandum of understanding, or cooperation arrangement.

Partner Responsibilities

Agreements with partners should include clear obligations, such as:

- Implementing the activity in accordance with the agreed purpose.
- Using funds or resources only for the specified purpose.
- Providing financial and implementation reports.
- Retaining documents and evidence.
- Not transferring funds or resources to a third party without approval.
- Not using the organisation's name or logo without permission.
- Protecting beneficiary data.
- Reporting any issues or risk indicators.
- Allowing review or document requests when needed.
- Complying with relevant laws and instructions.

22.13 Key Responsibilities Matrix

The organisation should maintain a simple responsibility matrix showingthe main responsibilities of each internal party.

A simplified matrix may include the following areas:

Area	Board	Executive Management	Finance	Compliance / Focal Point	Programmes	Donations	Volunteer Coordinator
Policies	Approves	Implements	Provides input	Reviews / follows up	Applies	Applies	Applies
Risk assessment	Reviews	Oversees	Provides financial input	Prepares / updates	Provides operational input	Provides donation input	Provides volunteer input
Donations	Oversees material cases	Supervises	Records and reconciles	Reviews indicators	Coordinates where linked to programmes	Manages permits and channels	Ensures volunteers do not fundraise without approval
Partners	Approves higher-risk cases	Supervises	Reviews payment records	Reviews risk indicators	Manages and follows up	Coordinates where linked to campaigns	Coordinates where volunteers are involved
Volunteers	Receives material reports	Supervises	Records entrusted items where financial	Reviews risk indicators	Coordinates activity needs	Ensures no unauthorised fundraising	Manages registration and tasks
corrective actions	Oversees	Ensures	Maintains financial records	Follows up registers	Maintains programme records	Maintains campaign files	Maintains volunteer records
Risk indicators	Reviews material cases	Escalates	Escalates financial indicators	Maintains register	Escalates partner/ beneficiary indicators	Escalates donor/ campaign indicators	Escalates volunteer indicators
Corrective actions	Approves material actions	Implements	Implements financial actions	Tracks	Implements programme actions	Implements donation actions	Implements volunteer actions

22.14 Who Approves What?

Recommended Good Practice

The organisation should adopt a clear authority matrix.

A simplified authority matrix may include:

Decision	Suggested Approval Level
Core policies	Board of Directors
Authority matrix	Board of Directors
Annual budget	Board of Directors
Routine expenditure within budget	Executive management / authorised person
Significant expenditure	Executive management or Board, depending on value
Opening or changing bank accounts	Board / authorised authority
Change of authorised signatories	Board / authorised authority
Launching a fundraising campaign	Competent internal approval and official permit where required
Acceptance of routine low-risk donations	Donations officer / authorised team
Acceptance of large or higher-risk donations	Executive management / Board, depending on seriousness
Rejection or suspension of a high-risk donation	Executive management / Board where material
Approval of a partner	Programme management / executive management
Approval of higher-risk partner	Executive management / Board
Activity outside the State	Board and official approval where required
Volunteer opportunity	Volunteer coordinator / management, subject to registration or licensing where required
Material risk indicator	Executive management / Board
Corrective action plan for serious observation	Executive management / Board
Referral to Ministry or competent authority	Authorised focal point / management

22.15 Segregation of Duties

Recommended Good Practice

All stages of a sensitive process should not be concentrated in one person, especially in relation to finance, donations, and partners.

Examples of Required Segregation

Process	Request	Review	Approval	Execution	Reconciliation / Follow-Up
Payment	Programme / finance	Finance	Authorised person	Finance / bank signatory	Finance / reviewer
Donation campaign	Donations team	Compliance / finance	Management / competent authority where required	Donations team	Finance / management
Partner selection	Programme team	Compliance / management	Management / Board where higher risk	Programme team	Programme / finance
Volunteer opportunity	Volunteer coordinator	Programme / compliance	Management where required	Volunteer coordinator	Volunteer coordinator / management
Corrective action	Relevant unit	Compliance / management	Management / Board where material	Responsible unit	Compliance /Board wherematerial

In smaller organisations, full segregation may not always be possible. In such cases, compensating controls should be applied, such as post-review, dual approval, Board oversight, or external accountant review for sensitive transactions.

22.16 Internal Governance, Risk, and Compliance Committee

Recommended Good Practice

In larger or more active organisations, an internal governance, risk, and compliance committee may be established. It does not need to be complex, but it can help coordinate responsibilities among teams.

Suggested Functions

The committee may:

- Review the risk assessment.
- Follow up risk indicators.
- Review unusual donations.
- Review higher-risk partners.
- Follow up corrective actions.
- Review training.
- Prepare reports for management or the Board.
- Recommend referral to the competent authority where needed.

Suggested Composition

The committee may include:

- A representative of executive management.
- The finance officer.
- The compliance officer or focal point.
- The programme officer.
- The donations officer.
- The volunteer coordinator, where needed.

22.17 Focal Point with the Ministry or Competent Authority

Supervisory Requirement / Recommended Good Practice

The organisation should identify a focal point responsible for coordinating with the Ministry or competent authority in relation to data requests, updates, inspection, or enquiries.

The organisation should identify a focal point responsible for coordinating with the Ministry or competent authority in relation to data requests, updates, inspection, or enquiries.

Responsibilities of the Focal Point

The focal point is responsible for:

- Receiving official correspondence.
- Recording requests and deadlines.
- Coordinating the internal collection of information.
- Reviewing consistency of responses.
- Retaining copies of correspondence.
- Following up open requests.
- Escalating important matters to management.
- Avoiding the submission of unverified or unapproved information.
- Ensuring referral to the competent authority where matters are unclear.

22.18 Focal Point with the Bank

Recommended Good Practice

The organisation should also identify a focal point with the bank to ensure

consistency of information and timely responses to information update requests or

banking enquiries.

Responsibilities

The banking focal point is responsible for:

Maintaining the bank file.

Updating authorised signatory information.

Coordinating responses to bank requests.

Ensuring that information is consistent with the organisation's records.

Escalating any restriction or sensitive request.

Coordinating with the finance officer and management.

Retaining banking correspondence.

22.19 Managing Absence or Changes in Key Persons

Recommended Good Practice

The organisation should not depend on one person who knows everything. Absence or departure of a key person may lead to loss of knowledge or disruption of work.

Proposed Controls

The organisation should ensure:

- Records are kept in an institutional system, not personally held.
- There is a backup person for each sensitive role.
- Formal handover takes place when staff change.
- Access rights are updated.
- Authorised persons and focal points are updated when changes occur.
- More than one person is trained on core procedures.
- Passwords and files are managed in accordance with secure policies.

22.20 Accountability and Follow-Up

Recommended Good Practice

Defining responsibilities has no value without follow-up. There should therefore be a periodic mechanism to review whether responsibilities are being implemented.

Follow-Up Tools

The organisation may use:

- Periodic meetings.
- Short reports.
- Checklists.
- Sample file reviews.
- Follow-up of risk indicators.
- Follow-up of corrective actions.
- Reports to the Board of Directors.
- Performance evaluation linked to compliance, where appropriate.

22.21 Common Mistakes in the Allocation of Responsibilities

Common mistakes that should be avoided include:

- Not identifying who has approval authority.
- Leaving donations to the media team without financial or legal coordination.
- Leaving volunteers without a clear supervisor.
- Not having a focal point with the competent authority.
- Leaving the bank account under the control of one person only.
- Not having backups for key employees.
- Not documenting rejection or escalation decisions.
- Not presenting material observations to the Board.
- Assuming that the compliance officer alone is responsible for everything.
- Not training partners or volunteers on the limits of their roles.

22.22 Self-Assessment Questions for Roles and Responsibilities

The organisation may use the following questions:

- Do we have a written authority matrix?
- Does the Board understand its oversight responsibilities?
- Does executive management know what must be escalated?
- Does the finance officer review records and escalate discrepancies?
- Is there a compliance or risk focal point?
- Is there a clearly identified person responsible for donations?
- Is there a clearly identified person responsible for volunteers?
- Does the programme officer retain implementation and beneficiary evidence?
- Do we know who communicates with the Ministry or competent authority?
- Do we know who communicates with the bank?
- Do we have backups for sensitive roles?
- Is there segregation between request, approval, and payment?
- Are material indicators presented to the Board?
- Is the person responsible for each corrective action documented?
- Do volunteers and partners understand the limits of their roles?

22.23 Chapter Summary

Clear roles and responsibilities are the foundation for the practical implementation of this Manual. An organisation that does not define who is responsible for decisions, implementation, review, escalation, and follow-up will find it difficult to demonstrate governance and effectiveness, even if it has good policies.

The key rules of this chapter can be summarised as follows:

- Compliance is a shared responsibility, but it requires clear allocation.
- The Board of Directors is responsible for oversight, approval, and follow-up.
- Executive management is responsible for practical implementation.
- The finance officer protects records, funds, and reports.
- The compliance officer or focal point coordinates risks and escalation.
- Donations teams are responsible for permits, channels, and records.
- Programme teams are responsible for partners, beneficiaries, and evidence of implementation.
- The volunteer coordinator is responsible for organising volunteers and defining the limits of their roles.
- Employees and volunteers are responsible for compliance and reporting.
- Partners should comply with the obligations set out in agreements.
- Sensitive processes require segregation of duties.
- There should be a clear focal point with the Ministry or competent authority and with the bank.
- Every material decision and follow-up responsibility should be documented.

By applying these principles, the organisation becomes better able to implement controls, conduct oversight, escalate issues, and demonstrate effectiveness before the Ministry, the competent authority, or any assessment body.

Map of Legal Obligations and Good Practices

23

Map of Legal Obligations and Good Practices

23.1 Purpose of this Chapter

This chapter aims to provide a practical map that helps Non-Profit Organisations distinguish between legal obligations, regulatory or supervisory requirements, recommended good practices, FATF expectations, and matters that may require confirmation from the Ministry or the competent authority.

This distinction is important because it prevents confusion between mandatory legal requirements and guidance-based practices. It also helps organisations understand their priorities, organise their files, and determine what must be complied with immediately and what should be adopted to strengthen governance, transparency, risk management, and effectiveness.

23.2 How to Read this Map

For the purposes of this chapter, the following classifications are used:

Classification	Meaning
Legal Obligation	A requirement set out in a law, decree-law, executive regulation, or binding decision.
Regulatory / Supervisory Requirement	A requirement or practice linked to the supervision of the Ministry or competent authority, or to licensing, inspection, follow-up, or reporting procedures.
Recommended Good Practice	A practice that may not be expressly stated as a specific standalone obligation, but helps the organisation strengthen governance, compliance, transparency, risk management, and effectiveness.
FATF Expectation	A principle or direction based on the FATF Standards or international best practices, particularly Recommendation 8 and Immediate Outcome 10.
Requires Confirmation	A matter that should be confirmed with the Ministry or competent authority due to differences in application, lack of clarity, or the need for detailed instructions.

This map should not be treated as a substitute for the applicable laws, regulations, decisions, permits, circulars, or instructions. It is an operational tool to help organisations understand and organise their obligations.

23.3 Map of Obligations Related to Licensing, Declaration, and Classification

Subject	Classification	Requirement or Practice	Reference / Note
Practising public benefit activities	Legal Obligation	Public benefit activities may not be practised unless the relevant licensing, declaration, registration, and approval requirements have been satisfied.	Federal Decree-Law No. (50) of 2023 and related regulations.
Licence and declaration	Legal Obligation	The organisation must maintain its licence, declaration, and legal status in accordance with the applicable requirements.	Core legal status requirement.
Registration in the relevant register	Legal Obligation / Supervisory Requirement	The organisation's information must be recorded and updated in the relevant register maintained by the Ministry or competent authority.	Updates should be made when material changes occur.
Classification	Regulatory / Supervisory Requirement	The organisation should understand its approved classification and ensure that its activities are consistent with that classification.	Classification Guide for Public Benefit Organisations.
Activities outside the approved scope	Requires Confirmation	Any activity not clearly covered by the organisation's objectives, classification, or licence should be verified with the Ministry or competent authority before implementation.	Prevents acting outside the approved scope.

23.4 Map of Obligations Related to Governance and Management

Subject	Classification	Requirement or Practice	Reference / Note
Governance and sound administration	Legal Obligation	Public Benefit Organisations must follow rules of governance and sound administration.	Federal Decree-Law No. (50) of 2023.
Internal regulations	Legal Obligation	The organisation should maintain internal regulations covering procurement, financial affairs, human resources, disciplinary measures, and a professional code of conduct.	Core governance requirement.
Board oversight	Recommended Good Practice / Legal Obligation where applicable	The Board should oversee policies, risks, budgets, accounts, major activities, and corrective actions.	Evidence of effectiveness.
Authority matrix	Recommended Good Practice	The organisation should define who approves key decisions, payments, donations, partners, activities, and escalations.	Supports accountability.
Conflict of interest	Recommended Good Practice / Legal Obligation where applicable	Conflicts of interest should be disclosed, recorded, and managed.	Protects integrity of decisions.
Segregation of duties	Recommended Good Practice	Sensitive processes should not be managed entirely by one person.	Particularly important for payments, donations, and partner relationships.

23.5 Map of Financial Obligations and Bank Accounts

Subject	Classification	Requirement or Practice	Reference / Note
Bank accounts	Legal Obligation	Accounts should be opened in the organisation's official name and in accordance with the applicable legal requirements.	Federal Decree-Law No. (50) of 2023.
Notification of account details	Legal Obligation	The competent authority should be notified of bank account details and changes where required.	Within the applicable timeframe.
Personal accounts	Recommended Good Practice / Legal Obligation where applicable	Organisational funds and donations should not be received, held, or transferred through personal accounts.	High-risk financial indicator.
Cash controls	Recommended Good Practice / Legal Obligation where applicable	Cash should be recorded, controlled, deposited into official accounts, and reconciled.	Reduces loss and misuse.
Financial records	Legal Obligation	Financial and accounting records should be maintained and retained in accordance with applicable requirements.	Usually no less than ten years for financial and accounting records.
Investment	Legal Obligation	Investment of funds exceeding the organisation's needs requires approval from the competent authority and must follow applicable controls.	Not an unrestricted commercial activity.

23.6 Map of Obligations Related to Donations

Subject	Classification	Requirement or Practice	Reference / Note
Collection of donations	Legal Obligation	Donations may be collected only by licensed entities or authorised entities with the required permit.	Donation Regulation Law and Executive Regulation.
Natural persons	Legal Obligation	Natural persons may not collect donations outside licensed or authorised channels.	Core prohibition.
Fundraising permit	Legal Obligation	A permit or approval must be obtained where required before launching, advertising, or implementing a fundraising campaign.	Applies to authorised entities and relevant campaigns.
Advertising donations	Legal Obligation	Donation-related advertising must comply with the permit, approval, and applicable rules.	Includes digital and social media content.
Donation records	Legal Obligation	Donations should be recorded, including proceeds, sources, purpose, expenditure, and beneficiary entities where applicable.	Donation-related accounting records should be retained for no less than ten years.
Use of donations	Legal Obligation	Donations must be used for the purpose for which they were collected or approved.	Protects donors' funds.
Administrative and operational expenses	Legal Obligation	Deduction of such expenses from donations is permitted only where allowed and approved under applicable controls.	Requires clarity and documentation.

23.7 Map of Obligations Related to Donors and Sources of Funding

Subject	Classification	Requirement or Practice	Reference / Note
Donor due diligence	Recommended Good Practice / Legal Obligation where applicable	Donor information and review should be proportionate to the level of risk.	Risk-based approach.
Small low-risk donations	Recommended Good Practice	Basic recording may be sufficient where donations are small, low risk, and received through official channels.	Avoids unnecessary burden.
Large or unusual donations	Recommended Good Practice	Large, unusual, repeated, conditional, anonymous, or unclear donations should be reviewed before acceptance.	May require escalation.
Conditional donations	Recommended Good Practice / Legal Obligation where applicable	Conditional donations should be accepted only where the condition is lawful, clear, documented, and consistent with approved purposes.	Unclear conditions require caution.
Anonymous donations	Recommended Good Practice / Legal Obligation where applicable	Large anonymous donations should not be accepted without appropriate verification.	Particularly where conditional or repeated.
Virtual assets or crypto-assets	Requires Confirmation	The organisation should not accept donations through virtual assets or crypto-assets unless permitted and confirmed by the competent authority and relevant regulators.	Higher-risk and non-traditional channel.

23.8 Map of Obligations Related to Partners and Beneficiaries

Subject	Classification	Requirement or Practice	Reference / Note
Partner due diligence	Recommended Good Practice	Partners should be verified according to risk, including legal status, purpose, authority, and ability to implement.	Important for funds and implementation.
Written agreements	Recommended Good Practice	Material partnerships should be documented through contracts or memoranda of understanding.	Particularly where funds, resources, data, or beneficiaries are involved.
Partner reports	Recommended Good Practice	Partners should provide reports and evidence of implementation.	Supports traceability and effectiveness.
Transfers to partners	Recommended Good Practice / Legal Obligation where applicable	Transfers should be made to official accounts and supported by documents.	Avoid personal or third-party accounts.
Beneficiary selection	Recommended Good Practice	Beneficiaries should be selected based on clear criteria and documented reasons.	Prevents favouritism or misuse.
Beneficiary data	Recommended Good Practice / Legal Obligation where applicable	Beneficiary data and dignity should be protected.	Avoid unnecessary disclosure.
Final beneficiary evidence	Recommended Good Practice	The organisation should retain evidence that assistance or services reached the intended purpose or beneficiary category.	Proportionate to risk and value.

23.9 Map of Obligations Related to Voluntary Work

Subject	Classification	Requirement or Practice	Reference / Note
Registration and licensing of voluntary work	Legal Obligation	Voluntary work and volunteering opportunities should be registered or licensed where required.	Voluntary Work Law and Executive Regulation.
Volunteer registration	Legal Obligation	Volunteers and volunteer teams should be registered in accordance with applicable requirements.	Where required.
Volunteer Charter	Legal Obligation	Volunteers should accept and comply with the Volunteer Charter.	Core requirement.
Volunteer tasks	Legal Obligation / Recommended Good Practice	The organisation should clearly define volunteer tasks, limits, and responsibilities.	Prevents misuse of role.
Prohibition on fundraising by volunteers	Legal Obligation	Volunteers and volunteer teams may not collect, allow the collection of, or advertise donations except with prior approval from the Ministry.	Critical control.
Volunteer data and confidentiality	Legal Obligation / Recommended Good Practice	Personal and operational information accessed by volunteers should be protected.	Includes beneficiary data.
Volunteer breaches	Recommended Good Practice	Breaches should be recorded, reviewed, and escalated where necessary.	Supports accountability.

23.10 Map of Obligations Related to Activities Outside the State

Subject	Classification	Requirement or Practice	Reference / Note
Activities outside the State	Requires Confirmation / Legal Obligation where applicable	External activities should not be implemented without verifying official requirements and obtaining required approvals.	Depending on the nature of the activity.
Foreign partners	Recommended Good Practice	Foreign partners should be subject to due diligence proportionate to risk.	Legal status, authority, account, reporting.
External transfers	Recommended Good Practice / Legal Obligation where applicable	External transfers should use formal financial channels and be linked to clear purpose and approvals.	Avoid informal channels.
In-kind assistance outside the State	Requires Confirmation	External in-kind assistance should comply with applicable requirements and be documented.	May require coordination with relevant authorities.
Volunteers outside the State	Requires Confirmation / Legal Obligation where applicable	Volunteering opportunities outside the State require verification of applicable requirements and approvals.	Voluntary Work Law and Executive Regulation.
Cross-border crowdfunding	Requires Confirmation	Cross-border platforms or crowdfunding should not be used unless permitted and approved.	Higher-risk channel.
Virtual assets in cross-border activities	Requires Confirmation	Virtual assets or crypto-assets should not be used without clear official confirmation.	Higher-risk and regulatory sensitivity.

23.11 Map of Obligations Related to Media and Institutional Communication

Subject	Classification	Requirement or Practice	Reference / Note
Official communication channels	Recommended Good Practice	The organisation should identify and control its official communication channels.	Website, social media, media statements.
Approval of public messages	Recommended Good Practice	Public content should be reviewed and approved before publication.	Particularly donation-related content.
Donation-related content	Legal Obligation where applicable	Donation appeals, links, and campaign messages should comply with permit and approval requirements.	May constitute fundraising.
Use of name and logo	Recommended Good Practice / Legal Obligation where applicable	Use of the organisation's name or logo should be authorised and controlled.	Applies to volunteers and partners.
Beneficiary images and stories	Recommended Good Practice / Legal Obligation where applicable	Beneficiary images and stories should be used lawfully, respectfully, and with safeguards.	Dignity and data protection.
Impersonation and fake links	Recommended Good Practice	Unauthorised pages, fake accounts, and donation links should be recorded and addressed promptly.	May require notification.

23.12 Map of Obligations Related to Records and Reports

Subject	Classification	Requirement or Practice	Reference / Note
Administrative records	Legal Obligation / Recommended Good Practice	Administrative records should generally be retained for no less than five years unless a longer period applies.	According to applicable requirements.
Financial and accounting records	Legal Obligation	Financial and accounting records should generally be retained for no less than ten years unless a longer period applies.	Includes supporting documents.
Donation-related accounting records	Legal Obligation	Donation-related accounting records should be retained for no less than ten years.	Donation Regulation Executive Regulation.
Reports to competent authority	Legal Obligation / Supervisory Requirement	Reports should be submitted when required by law, permit, approval, inspection, or supervisory request.	Must be accurate and supported.
Risk and incident register	Recommended Good Practice	Risk indicators, incidents, breaches, and corrective actions should be recorded.	Evidence of effectiveness.
Conflict of interest register	Recommended Good Practice	Conflicts should be recorded and managed.	Supports governance.
Electronic records	Recommended Good Practice	Electronic records should be secure, backed up, and protected from unauthorised alteration.	Supports retrieval and review.

23.13 Map of Obligations Related to Supervision and Inspection

Subject	Classification	Requirement or Practice	Reference / Note
Cooperation with supervision	Legal Obligation / Supervisory Requirement	The organisation should cooperate with the Ministry or competent authority and respond to requests.	Inspection and follow-up framework.
Data requests	Supervisory Requirement	Requests should be answered accurately, completely, and within the required timeframe.	Keep copy of response and evidence.
Inspection readiness	Recommended Good Practice	The organisation should maintain organised records and evidence on an ongoing basis.	Not only when inspection is announced.
Supervisory observations	Supervisory Requirement	Observations should be recorded, classified, and followed up.	Evidence of corrective action.
Corrective action plans	Supervisory Requirement / Recommended Good Practice	Corrective actions should identify the root cause, responsible person, deadline, and closure evidence.	Prevents recurrence.
Immediate escalation	Recommended Good Practice / Legal Obligation where applicable	Serious indicators or potential violations should be escalated promptly.	May require referral to competent authority.

23.14 Map of Obligations Related to Training and Awareness

Subject	Classification	Requirement or Practice	Reference / Note
Training plan	Recommended Good Practice	The organisation should maintain a proportionate training plan.	Based on roles and risks.
Board training	Recommended Good Practice	Board members should understand oversight, governance, risk, and corrective actions.	Supports effectiveness.
Staff training	Recommended Good Practice	Staff should be trained on the policies relevant to their roles.	Finance, donations, programmes, records.
Volunteer training	Legal Obligation / Recommended Good Practice	Volunteers should understand their tasks, confidentiality, conduct, and prohibition on fundraising without approval.	Voluntary Work framework.
Training register	Recommended Good Practice	Training activities should be documented.	Topic, date, participants, materials.
Scenario-based training	Recommended Good Practice	Practical examples should be used to strengthen understanding.	Useful for risk indicators.

23.15 Map of Obligations Related to Risk Indicators and Escalation

Subject	Classification	Requirement or Practice	Reference / Note
Risk indicators	Recommended Good Practice / FATF Expectation	The organisation should identify and respond to indicators relating to donations, partners, volunteers, beneficiaries, finance, and records.	Supports risk-based approach.
Internal reporting	Recommended Good Practice	Staff and volunteers should know how to report concerns.	Good-faith reporting.
Incident register	Recommended Good Practice	Indicators and incidents should be recorded and closed with evidence.	Demonstrates effectiveness.
Immediate escalation	Recommended Good Practice / Legal Obligation where applicable	High-risk indicators should be escalated to management, Board, or competent authority as appropriate.	Especially funds, donations, partners, volunteers.
Corrective action	Recommended Good Practice	Repeated indicators should result in updated controls, training, or procedures.	Root cause treatment.
Referral to competent authority	Requires Confirmation / Legal Obligation where applicable	Where the correct action is unclear or the matter is serious, the organisation should refer to the Ministry or competent authority.	Document referral and response.

23.16 Map of FATF Recommendation 8 and Immediate Outcome 10 Requirements

FATF Area	Classification	Practical Meaning for the Organisation
Risk-based approach	FATF Expectation	The organisation should apply controls proportionate to its risks, rather than treating all cases the same.
Protection from terrorist financing abuse	FATF Expectation	The organisation should understand how its funds, activities, partners, beneficiaries, volunteers, or name could be misused.
Focused and proportionate measures	FATF Expectation	Controls should be stronger where risks are higher and simpler where risks are lower.
Avoiding disruption of legitimate activity	FATF Expectation	Controls should protect legitimate work and not impose unnecessary restrictions.
Identification of higher-risk exposure	FATF Expectation / National Supervisory Function	The State identifies the sub-set most exposed to risk; organisations should understand their own exposure.
Outreach and awareness	FATF Expectation / Supervisory Requirement	Organisations should benefit from guidance and training and reflect relevant risk indicators internally.
Effectiveness under IO.10	FATF Expectation	The organisation should be able to show practical evidence of implementation, not only written policies.
Evidence of practical implementation	Recommended Good Practice	Donation reviews, partner due diligence, volunteer controls, risk registers, corrective actions, and Board minutes are examples of effectiveness evidence.

23.17 Key Matters Requiring Confirmation from the Ministry or Competent Authority

The organisation should seek confirmation from the Ministry or competent authority where the requirement is unclear or where an activity may require prior approval.

Examples include:

- Whether a specific activity falls within the approved licence or classification.
- Whether a fundraising campaign requires a permit.
- Whether a digital donation channel is permitted.
- Whether a donation from outside the State may be accepted.
- Whether a conditional donation may be accepted.
- Whether a large or unusual donation should be suspended or reported.
- Whether a foreign partner may be used.
- Whether assistance may be provided outside the State.
- Whether a virtual asset or crypto-asset donation may be accepted.
- Whether volunteers may participate in a specific external activity.
- Whether specific beneficiary information may be shared with a bank, partner, or external party.
- Whether a material breach or risk indicator requires notification.
- Whether a corrective action plan is sufficient to close a supervisory observation.

The organisation should document the request for confirmation, the response received, and any action taken.

23.18 Practical Priorities for the Organisation

Based on the chapters of this Manual, the organisation should prioritise the following actions:

1. Confirm legal status, licence, declaration, and classification.

2. Ensure that actual activities are consistent with approved purposes.

3. Approve core internal policies and procedures.

4. Establish an authority matrix.

5. Maintain official bank accounts and prohibit personal accounts.

6. Maintain proper financial and accounting records.

7. Ensure that donation activities are licensed or authorised where required.

8. Maintain donation and fundraising campaign files.

9. Apply risk-based review to donors and donations.

10. Conduct due diligence on partners and beneficiary entities.

11. Protect final beneficiaries' dignity and data.

12. Organise voluntary work and prohibit unauthorised fundraising by volunteers.

13. Control the organisation's name, logo, media content, and digital channels.

14. Maintain records and reports for the required period.

15. Establish a risk indicator and incident register.

16. Train Board members, staff, and volunteers according to their roles.

17. Prepare for supervision and inspection through organised files.

18. Document corrective actions and closure evidence.

19. Maintain a banking file and respond promptly to bank requests.

20. Refer to the Ministry or competent authority where matters are unclear.

23.19 Practical Summary of the Chapter

This chapter provides a final operational map to help Non-Profit Organisations understand how the legal and supervisory framework, internal governance, FATF expectations, and recommended good practices fit together.

The key messages are:

- Not every item in this Manual has the same legal status.
- Legal obligations must be complied with.
- Supervisory requirements should be followed and documented.
- Recommended good practices help the organisation strengthen governance and demonstrate effectiveness.
- FATF expectations help explain why risk-based and proportionate controls matter.
- Matters that are unclear should be confirmed through the Ministry or competent authority.
- The organisation should focus on practical implementation, not only written documents.
- Evidence is essential: decisions, approvals, records, reports, registers, and corrective actions should be maintained and retrievable.
- The organisation should continuously update its controls based on risk indicators, supervisory observations, legal changes, and lessons learned.
- This map should be used as a living tool. It may be adapted into internal checklists, compliance calendars, inspection readiness files, training materials, or Board reporting templates.

General Conclusion of the Manual

This Manual has been prepared to support Non-Profit Organisations in the United Arab Emirates in understanding and applying the legal, regulatory, supervisory, and risk-based requirements relevant to their work.

The core message of the Manual is that protecting the sector from abuse should go hand in hand with enabling legitimate public benefit, charitable, humanitarian, social, cultural, educational, and voluntary work.

The Manual does not treat Non-Profit rganisations as inherently high risk. Rather, it recognises the importance of the sector and the need to protect it through proportionate, practical, and evidence-based controls.

Across its chapters, the Manual has explained the following:

- The legal and regulatory framework governing Non-Profit Organisations, donations, voluntary work, classification, supervision, and accountability.
- The relationship between the national framework and FATF Recommendation 8 and Immediate Outcome 10.
- The importance of understanding risks, particularly risks of terrorist financing abuse.
- The application of the risk-based approach.
- Governance, transparency, internal controls, and the role of the Board of Directors.
- Core internal policies and procedures.
- Donation regulation, donor due diligence, and protection of donors' funds.
- Financial management, bank accounts, records, and financial reports.
- Partners, beneficiary entities, and final beneficiaries.
- Voluntary work, volunteers, and volunteer teams.
- Transparency, record-keeping, reporting, and disclosure to the Ministry or competent authority.
- Supervision, inspection, follow-up, and corrective actions.
- Training, awareness, and capacity-building.
- Risk indicators, internal reporting, and escalation.
- Access to financial services and dealing with banks.
- Institutional communication, media, beneficiary images, and public messages.
- Activities outside the State and cross-border partnerships.
- Preparation for mutual evaluation and demonstrating effectiveness.
- Allocation of roles and responsibilities within the organisation.
- Mapping of legal obligations, supervisory requirements, FATF expectations, and good practices.

The success of this Manual depends on practical implementation. Policies, forms, registers, and templates are useful only when they guide real decisions, improve governance, strengthen transparency, and help prevent misuse.

Accordingly, each organisation should adapt the Manual to its legal form, size, activities, risk profile, resources, and approved classification. A small local organisation may apply simplified controls, while a larger organisation that collects donations, works with partners, operates outside the State, or deals with higher-risk activities should apply stronger controls and deeper documentation.

The following principles should guide implementation:

01 Understand the organisation's legal status and approved scope.

02 Apply controls that are proportionate to risk.

03 Use official financial and donation channels.

04 Document decisions and retain evidence.

05 Protect beneficiaries, donors, volunteers, and partners.

06 Control the organisation's name, logo, and public communications.

07 Identify and escalate risk indicators.

08 Cooperate with the Ministry and competent authority.

09 Train relevant persons according to their roles.

10 Review and improve controls continuously.

By applying these principles, Non-Profit Organisations can strengthen public trust, protect their resources, support national effectiveness, and c ontinue to perform their legitimate and valuable role in serving society.

This Manual should therefore be treated as a practical reference for daily governance, compliance, training, supervision readiness, and continuous improvement. It should be reviewed periodically and updated whenever there are changes in the legal framework, supervisory expectations, national risk understanding, or the organisation's activities and risk profile.