

BET PLAY B.V

OPERATIONAL MANUAL

V 1.0

Table of Contents

Chapter 1 – Introduction and Document Governance 19

1.1 Welcome to the Bet Play B.V. Operational Manual 19

1.2 Purpose of the Manual 20

1.3 Scope 21

1.4 Proportionality..... 22

1.5 Supporting Documentation 23

1.6 Ownership and Approval 24

1.7 Review and Version Control 24

1.8 Document Control Table..... 25

Chapter 2 – Company Overview and Business Model..... 28

2.1 Company Overview 28

2.2 Corporate Details 28

2.3 Ownership Structure 29

2.4 Nature of the Business..... 30

2.5 Products and Services 31

2.6 Business Partner Profile..... 32

2.7 Commercial Model..... 33

2.8 Technology and Integration Model..... 33

2.9 Division of Responsibilities..... 34

2.10 Activities Outside the Company's Scope 36

2.11 Geographic and Jurisdictional Considerations 37

2.12 Operational Structure 38

2.13 Strategic Objectives 39

2.14 Changes to the Business Model 40

Chapter 3 – Corporate Governance and Organisational Structure 43

3.1 Corporate Governance Framework 43

3.2 Governance Principles 44

3.3 Organisational Structure 45

3.4 Director and Executive Oversight..... 45

3.5 Compliance Governance 46

3.6 AML/CFT/CPF Governance..... 47

3.7 Financial Governance 48

3.8 Account Management Governance 48

3.9 Delegation of Authority	49
3.10 Management Decision-Making	50
3.11 Management Meetings and Reporting	51
3.12 Reserved Matters and Escalation.....	51
3.13 Conflicts of Interest.....	52
3.14 Independence and Access to Information	53
3.15 Use and Oversight of External Service Providers.....	53
3.16 Succession and Temporary Absence Arrangements	54
3.17 Governance Records.....	55
3.18 Review of Governance Arrangements	55
Chapter 4 – Roles, Responsibilities and Key Functions	58
4.1 Purpose.....	58
4.2 General Responsibilities of Officers and Personnel.....	58
4.3 Director and Chief Executive Officer	59
4.3.1 Strategic and Corporate Responsibilities.....	60
4.3.2 Commercial Responsibilities	60
4.3.3 Regulatory and Compliance Responsibilities.....	61
4.3.4 Financial Responsibilities	61
4.3.5 Director Reporting and Records.....	61
4.4 Compliance Officer	62
4.4.1 Regulatory Compliance.....	62
4.4.2 Business-Partner Compliance	62
4.4.3 Compliance Monitoring.....	63
4.4.4 Compliance Advice and Escalation	64
4.5 Money Laundering Reporting Officer.....	64
4.5.1 AML/CFT/CPF Framework.....	65
4.5.2 Internal Reports and Suspicious Activity.....	65
4.5.3 Independence of the MLRO	66
4.6 Chief Financial Officer	66
4.6.1 Financial Administration	66
4.6.2 Invoicing and Revenue Controls	66
4.6.3 Payments and Expenditure	67
4.6.4 Reconciliation and Financial Reporting	67
4.6.5 Financial Escalation	67
4.7 Account Management Function	68

4.7.1 Prospective Business Partners	68
4.7.2 Existing Business Partners	69
4.7.3 Identification of Material Changes	69
4.7.4 Integration and Activation Coordination.....	69
4.7.5 Technical and Service Issues	71
4.8 External Advisers and Service Providers.....	71
4.9 Relationship with Babylon Gaming.....	72
4.9.1 Responsibilities of Bet Play B.V.	72
4.9.2 Responsibilities of Babylon Gaming and Upstream Providers	73
4.9.3 Escalation of Supplier Matters	73
4.10 Separation of Responsibilities and Checks	73
4.11 Responsibility and Approval Matrix	74
4.12 Authority Limitations	76
4.13 Reporting and Escalation Responsibilities	77
4.14 Competence and Suitability	78
4.15 Induction and Ongoing Training	78
4.16 Performance and Effectiveness Review	79
4.17 Role Descriptions and Appointment Records	80
4.18 Review of Roles and Responsibilities.....	80
Chapter 5 – Business Risk Management Framework.....	83
5.1 Purpose.....	83
5.2 Scope	83
5.3 Risk-Management Principles	84
5.3.1 Risk-Based Approach	84
5.3.2 Accountability	84
5.3.3 Proportionality	84
5.3.4 Evidence-Based Decisions.....	85
5.3.5 Prevention and Early Escalation	85
5.3.6 Documentation	85
5.3.7 Continuous Review.....	85
5.4 Governance and Responsibilities	85
5.4.1 Director.....	85
5.4.2 Compliance Officer	86
5.4.3 MLRO	86

5.4.4 Chief Financial Officer87

5.4.5 Account Management.....87

5.4.6 All Personnel87

5.5 Risk Appetite88

5.6 Principal Risk Categories89

5.6.1 Strategic and Business Risk.....89

5.6.2 Regulatory and Licensing Risk89

5.6.3 Business-Partner Risk89

5.6.4 Product and Distribution Risk.....90

5.6.5 Third-Party and Supplier Risk90

5.6.6 Operational Risk.....91

5.6.7 Financial Risk.....91

5.6.8 Information-Security and Data-Protection Risk92

5.6.9 Business-Continuity Risk92

5.6.10 Legal and Contractual Risk.....92

5.6.11 Reputational Risk93

5.6.12 AML/CFT/CPF and Sanctions Risk93

5.7 Risk-Identification Process94

5.8 Risk-Assessment Methodology.....94

5.8.1 Likelihood Scale95

5.8.2 Impact Scale.....95

5.8.3 Risk Score96

5.9 Risk Evaluation and Treatment96

5.9.1 Avoid97

5.9.2 Reduce97

5.9.3 Transfer or Share97

5.9.4 Accept97

5.10 Risk Acceptance and Exceptions98

5.11 Risk Register.....98

5.12 Risk-Assessment Triggers.....99

5.13 New Product, Service, Market and Change Risk Assessment100

5.14 Business-Partner Risk Assessment100

5.15 Third-Party and Supplier Risk Management102

5.16 Concentration and Dependency Risk..... 102

5.17 Monitoring of Risks and Controls..... 103

5.18 Key Risk Indicators 104

5.19 Incident and Near-Miss Reporting..... 104

5.20 Escalation of Material Risks 105

5.21 Corrective-Action Management 106

5.22 Risk Reporting..... 106

5.23 Business-Wide Risk Assessment..... 107

5.24 Recordkeeping 108

5.25 Training and Awareness 109

5.26 Independent Review and Assurance..... 109

5.27 Review of the Risk-Management Framework 110

Chapter 6 – Regulatory Compliance Framework 113

6.1 Purpose..... 113

6.2 Scope 114

6.3 Regulatory Status and Permitted Activities 114

6.4 Compliance Principles 115

6.4.1 Lawfulness 115

6.4.2 Regulatory Accountability 115

6.4.3 Proportionality 115

6.4.4 Independence..... 116

6.4.5 Evidential Compliance 116

6.4.6 Timely Escalation 116

6.4.7 Continuous Compliance 116

6.5 Compliance Governance 116

6.6 Responsibilities of the Director 118

6.7 Responsibilities of the Compliance Officer 118

6.8 Responsibilities of the MLRO 119

6.9 Responsibilities of the CFO 120

6.10 Responsibilities of Account Management..... 120

6.11 Regulatory Obligations Register..... 121

6.12 Regulatory Horizon Scanning..... 122

6.13 Regulatory Change Management..... 122

6.14 Compliance Risk Assessment..... 123

6.15 Compliance Review of New Business Partners 124

6.16 Market and Jurisdictional Compliance	124
6.17 Licence Verification	125
6.18 Product and Content Compliance	125
6.19 Onward Distribution and Reseller Controls.....	126
6.20 Compliance Conditions and Restrictions	126
6.21 Compliance Monitoring Programme	127
6.22 Monitoring Methods	128
6.23 Classification of Compliance Findings.....	129
6.24 Regulatory Breach Identification	129
6.25 Breach Assessment and Response	130
6.26 Regulatory Notifications.....	130
6.27 Regulatory Submissions and Returns	131
6.28 Regulatory Correspondence and Requests.....	132
6.29 Regulatory Inspections, Audits and Interviews	132
6.30 Internal Escalation	133
6.31 Suspension and Termination Controls	133
6.32 Corrective and Preventive Action	134
6.33 Compliance Reporting	134
6.34 Compliance Meetings.....	135
6.35 Conflicts of Interest.....	136
6.36 Speak-Up and Non-Retaliation	136
6.37 Outsourced Compliance Support	137
6.38 Compliance Training	137
6.39 Compliance Records	138
6.40 Compliance Management Information	138
6.41 Independent Compliance Review	139
6.42 Review of the Compliance Framework	140
Chapter 7 – Business-Partner Onboarding and Due Diligence	142
7.1 Purpose.....	142
7.2 Scope	143
7.3 Business-Partner Acceptance Principles.....	143
7.3.1 No Activation Before Approval	143
7.3.2 Risk-Based Due Diligence	143
7.3.3 Evidential Verification	144
7.3.4 Transparency	144

7.3.5 Regulatory and Contractual Compatibility	144
7.3.6 Continuing Suitability	145
7.4 Prohibited Relationships	145
7.5 Roles and Responsibilities	146
7.5.1 Director.....	146
7.5.2 Compliance Officer	146
7.5.3 MLRO	146
7.5.4 CFO	147
7.5.5 Account Management.....	147
7.5.6 Babylon Gaming and Other Providers	148
7.6 Initial Business Proposal	148
7.7 Onboarding Risk Screening.....	149
7.8 Standard Due-Diligence Requirements	151
7.9 Verification of Legal Identity	152
7.10 Identification of Ownership and Control.....	153
7.11 Ultimate Beneficial Owner Due Diligence.....	153
7.12 Directors, Key Persons and Authorised Representatives	154
7.13 Licence and Regulatory Verification	154
7.14 Brands, Domains and Websites	155
7.15 Market and Jurisdictional Assessment	156
7.16 Distribution Model and Downstream Parties	156
7.17 Regulatory and Enforcement History.....	157
7.18 Adverse-Media and Reputation Review.....	158
7.19 Sanctions and PEP Screening	158
7.20 Source of Funds and Source of Wealth	159
7.21 Financial Standing and Credit Risk.....	160
7.22 Bank Accounts and Payment Instructions	161
7.23 Information Security and Data Protection Review	161
7.24 Business-Partner Risk Assessment	162
7.25 Risk Classification.....	163
7.26 Enhanced Due Diligence	163
7.27 Reliance on Third-Party Due Diligence	164
7.28 Incomplete or Inconsistent Information	164
7.29 Compliance Approval	165
7.30 Management Approval	165

7.31 Conditional Approval	166
7.32 Contract Execution	166
7.33 Pre-Activation Checklist	167
7.34 Technical and Operational Activation.....	168
7.35 Business-Partner File	168
7.36 Ongoing Monitoring.....	169
7.37 Periodic Review	170
7.38 Event-Driven Review	170
7.39 Change Notification Obligations	171
7.40 Screening Refresh	171
7.41 Monitoring of Licences, Domains and Markets.....	172
7.42 Warning Indicators.....	172
7.43 Business-Partner Complaints and Disputes.....	173
7.44 Restriction and Suspension.....	173
7.45 Rejection and Termination	174
7.46 Reinstatement.....	175
7.47 Exceptions.....	175
7.48 Recordkeeping and Retention	176
7.49 Data Protection and Confidentiality.....	176
7.50 Training.....	177
7.51 Quality Assurance and Monitoring	177
7.52 Management Information	178
7.53 Independent Review	178
7.54 Review of the Onboarding Framework	179
Chapter 8 – Business-Partner Complaints and Dispute Resolution	181
8.1 Purpose.....	181
8.2 B2B Operating Context	181
8.3 Scope.....	182
8.4 Applicable Framework.....	182
8.5 Complaint-Handling Principles	182
8.5.1 Accessibility	182
8.5.2 Fairness.....	183
8.5.3 Promptness	183
8.5.4 Transparency.....	183
8.5.5 Proportionality	183

8.5.6 Confidentiality	183
8.5.7 Non-Retaliation	183
8.5.8 Evidence-Based Decisions.....	184
8.5.9 Continuous Improvement.....	184
8.6 Definitions	184
8.7 Roles and Responsibilities	184
8.7.1 Director	184
8.7.2 Compliance Officer	185
8.7.3 MLRO	185
8.7.4 Finance Function	185
8.7.5 Account Management	185
8.7.6 Technical and Operational Personnel.....	185
8.7.7 All Personnel	186
8.8 Complaint Channels.....	186
8.9 Distinguishing Support Requests from Complaints	186
8.10 Complaints Involving Babylon Gaming or Other Providers	186
8.11 Complaint Registration.....	187
8.12 Initial Assessment and Triage	187
8.13 Priority Classification.....	187
8.14 Acknowledgement.....	188
8.15 Verification of Authority.....	188
8.16 Investigation Planning	188
8.17 Evidence Collection and Preservation	188
8.18 Independence and Conflicts of Interest	189
8.19 Communication During Investigation	189
8.20 Resolution Timeframes	189
8.21 Technical and Content-Related Complaints.....	189
8.22 Game Malfunctions Escalated by Operators	190
8.23 Commercial and Invoicing Complaints.....	192
8.24 Complaints Alleging Fraud or Financial Crime.....	192
8.25 Information-Security and Data-Protection Complaints	192
8.26 Interim Measures	193
8.27 Complaint Outcome	193
8.28 Remedies and Corrective Action	193
8.29 Final Response	193

8.30 Internal Review 194

8.31 Contractual Dispute Resolution 194

8.32 Regulatory Complaints and Enquiries 194

8.33 Legal Proceedings and Settlement 194

8.34 Repeated or Abusive Communications 195

8.35 Complaint Records 195

8.36 Regulatory and Contractual Reporting 195

8.37 Root-Cause Analysis 195

8.38 Complaint Monitoring and Management Information 196

8.39 Connection with Business-Partner Oversight 196

8.40 Training 196

8.41 Quality Assurance 197

8.42 Key Controls 197

8.43 Exceptions 197

8.44 Review and Continuous Improvement 198

Chapter 9 – Information Security and Data Protection 200

9.1 Purpose 200

9.2 B2B Operating Context 200

9.3 Scope 200

9.4 Applicable Framework 201

9.5 Security and Privacy Principles 201

9.6 Information Classification 201

9.7 Roles and Responsibilities 201

9.8 Information Asset Inventory and Ownership 202

9.9 Risk Assessment 202

9.10 Identity and Access Management 202

9.11 Privileged Access 202

9.12 Authentication and Credentials 203

9.13 Acceptable Use and Endpoint Security 203

9.14 Network and Infrastructure Security 203

9.15 Encryption and Key Management 203

9.16 Secure Communications and Information Transfer 203

9.17 Logging and Monitoring 204

9.18 Vulnerability, Patch, and Configuration Management 204

9.19 Security Testing 204

9.20 Supplier and Babylon Gaming Security	204
9.21 Personal-Data Inventory and Privacy Roles	205
9.22 Data Minimisation and Pseudonymisation	205
9.23 Data-Subject Rights and Privacy Enquiries	205
9.24 Cross-Border Transfers and Disclosures	205
9.25 Retention and Secure Disposal	206
9.26 Backups	206
9.27 Security and Personal-Data Incidents	206
9.28 Records of Processing and Security Evidence	206
9.29 Monitoring and Management Information	206
9.30 Training and Awareness	207
9.31 Key Controls	207
9.32 Exceptions	207
9.33 Review and Continuous Improvement	207
Chapter 10 – IT Operations, Incident Management and Business Continuity	209
10.1 Purpose	209
10.2 Scope and B2B Context	209
10.3 Governance Principles	209
10.4 Roles and Responsibilities	209
10.5 IT Service and Dependency Inventory	210
10.6 Routine IT Operations	210
10.7 Event Monitoring and Alerting	210
10.8 Incident Definition and Classification	211
10.9 Incident Reporting and Intake	211
10.10 Initial Response	212
10.11 Containment	212
10.12 Technical Investigation and Evidence	212
10.13 Babylon Gaming and Provider Coordination	212
10.14 Communications	212
10.15 Business-Partner Notification	213
10.16 Regulatory and Other External Reporting	213
10.17 Security and Personal-Data Incidents	213
10.18 Game and Content Incidents	213
10.19 Recovery and Service Restoration	214
10.20 Closure	214

10.21 Root-Cause Analysis and Lessons Learned	214
10.22 Business Impact Analysis.....	214
10.23 Business Continuity Plans	215
10.24 Disaster Recovery	215
10.25 Backup and Restoration Testing	215
10.26 Continuity Activation and Crisis Management.....	215
10.27 Testing and Exercises	216
10.28 Change Freeze and Emergency Change.....	216
10.29 Records.....	216
10.30 Monitoring and Management Information	216
10.31 Training	216
10.32 Key Controls	216
10.33 Exceptions	217
10.34 Review and Continuous Improvement	217
Chapter 11 – Business Partner Support Operations	219
11.1 Purpose	219
11.2 B2B-Only Scope	219
11.3 Support Services	219
11.4 Principles.....	219
11.5 Roles and Responsibilities	220
11.6 Approved Channels and Hours	220
11.7 Partner and Contact Authentication.....	220
11.8 Ticket Registration	220
11.9 Classification	221
11.10 Priority and Service Targets	221
11.11 Acknowledgement and Ownership.....	221
11.12 Information Gathering.....	221
11.13 Standard Troubleshooting.....	222
11.14 Access and Credential Requests.....	222
11.15 Integration Support	222
11.16 Game and Content Queries	222
11.17 Player-Originated Malfunction Escalations	222
11.18 Complaints and Disputes	223
11.19 Incident Escalation	223
11.20 Security and Privacy Escalation	223

11.21 Change Requests	223
11.22 Babylon Gaming and Provider Escalation	223
11.23 Communications and Updates.....	224
11.24 Workarounds.....	224
11.25 Resolution and Closure.....	224
11.26 Reopening and Recurrence.....	224
11.27 Knowledge Management	224
11.28 Service-Level Management	225
11.29 Quality Assurance	225
11.30 Records and Management Information.....	225
11.31 Training	225
11.32 Key Controls	225
11.33 Exceptions	226
11.34 Review and Continuous Improvement	226
Chapter 12 – Product, Content and Business Development.....	228
12.1 Purpose.....	228
12.2 B2B Operating Model	228
12.3 Scope.....	228
12.4 Principles.....	228
12.5 Roles and Responsibilities	229
12.6 Product and Content Inventory	229
12.7 Product Strategy and Roadmap	229
12.8 Product Proposal and Business Case	229
12.9 Stage-Gate Approval.....	229
12.10 Regulatory and Market Assessment	230
12.11 Content Due Diligence	230
12.12 Product Requirements.....	230
12.13 Game Integrity and Fairness Evidence	230
12.14 Certification and Testing Laboratories	231
12.15 Responsible-Gaming and Player-Protection Dependencies.....	231
12.16 Security and Privacy by Design.....	231
12.17 Intellectual Property and Branding.....	231
12.18 Localisation and Market Presentation.....	231
12.19 Opportunity Qualification	232
12.20 Prospective-Partner Due Diligence	232

12.21 Proposals and Commercial Communications 232

12.22 Contracting Handover 232

12.23 Distribution Controls 232

12.24 Launch Readiness 233

12.25 Controlled Launch and Early-Life Support..... 233

12.26 Marketing and Product Claims 233

12.27 Demonstrations and Test Environments 233

12.28 Product Changes 233

12.29 Product Incidents and Malfunctions 234

12.30 Post-Launch Monitoring..... 234

12.31 Product Review and Retirement..... 234

12.32 Conflicts of Interest and Incentives 234

12.33 Records and Management Information 234

12.34 Training 235

12.35 Key Controls 235

12.36 Exceptions 235

12.37 Review and Continuous Improvement 235

Chapter 13 – Technology and Development Operations..... 237

13.1 Purpose 237

13.2 Scope and Operating Model 237

13.3 Principles..... 237

13.4 Roles and Responsibilities 237

13.5 Technology Inventory and Ownership 238

13.6 Development Lifecycle 238

13.7 Requirements and Traceability 238

13.8 Architecture and Design Review 238

13.9 Secure Development..... 238

13.10 Source-Code and Repository Controls..... 239

13.11 Third-Party Components and Supply Chain 239

13.12 Development, Test, and Production Separation..... 239

13.13 Change Classification 239

13.14 Change Request..... 239

13.15 Risk and Impact Assessment 240

13.16 Code Review..... 240

13.17 Testing Strategy 240

13.18 Gaming Content Testing and Certification 240

13.19 Defect Management 241

13.20 Build and Pipeline Security..... 241

13.21 Release Planning 241

13.22 Release Approval..... 241

13.23 Deployment 241

13.24 Post-Deployment Validation and Monitoring 242

13.25 Emergency Changes 242

13.26 Rollback and Recovery 242

13.27 Configuration Management..... 242

13.28 Database and Data Changes 242

13.29 API and Integration Management 243

13.30 Provider Development and Deliverables 243

13.31 Technical Documentation 243

13.32 Access to Production 243

13.33 Monitoring and Observability 243

13.34 Incident, Complaint, and Support Linkage 244

13.35 Maintenance and Technical Debt..... 244

13.36 Decommissioning 244

13.37 Records and Metrics 244

13.38 Quality Assurance and Independent Review..... 244

13.39 Training..... 245

13.40 Key Controls 245

13.41 Exceptions..... 245

13.42 Review and Continuous Improvement 245

Chapter 14 – Commercial Billing, Finance and Accounting Operations 247

14.1 Purpose 247

14.2 B2B Financial Operating Model..... 247

14.3 Scope 248

14.4 Applicable Framework..... 249

14.5 Core Financial-Control Principles 249

14.6 Roles and Responsibilities 250

14.6.1 Director 250

14.6.2 Finance Function 250

14.6.3 Compliance Officer 251

14.6.4 MLRO 251

14.6.5 Account Management and Commercial Personnel 251

14.6.6 All Personnel 251

14.7 Delegated Financial Authority..... 252

14.8 Segregation of Duties 252

14.9 Contract-to-Billing Control..... 253

14.10 Billing Source Data 253

14.11 Revenue-Share and Usage-Based Calculations 254

14.12 Invoice Preparation and Review..... 254

14.13 Invoice Issuance and Delivery 255

14.14 Credit Notes, Rebates, Refunds, and Adjustments 255

14.15 Accounts Receivable 255

14.16 Credit Risk and Overdue Debt..... 256

14.17 Billing Disputes 256

14.18 Supplier Onboarding and Master Data 256

14.19 Supplier Invoice Validation 257

14.20 Payment Preparation, Approval, and Release 257

14.21 Bank-Account and Beneficiary Changes..... 258

14.22 Corporate Bank-Account Controls..... 258

14.23 Incoming Receipts 259

14.24 Reconciliations 259

14.25 Babylon Gaming and Other Provider Dependencies..... 259

14.26 Foreign Currency..... 260

14.27 Taxes, Licence Fees, and Statutory Payments..... 260

14.28 Expenses and Reimbursements 260

14.29 Intercompany and Related-Party Transactions..... 261

14.30 Prohibited and Restricted Practices..... 261

14.31 Fraud Prevention and Payment Diversion 262

14.32 AML/CFT/CPF and Sanctions Escalation 262

14.33 Errors, Failed Payments, and Exceptions 263

14.34 Emergency Payments 263

14.35 Cash-Flow and Liquidity Monitoring 264

14.36 Financial Close and Accounting Entries 264

14.37 Management Information 264

14.38 Recordkeeping and Audit Trail..... 265

14.39 Information Security and Access..... 266

14.40 Business Continuity 266

14.41 Monitoring and Quality Assurance 266

14.42 Key Controls 267

14.43 Exceptions..... 268

14.44 Training..... 268

14.45 Accounting Policies and Standards 269

14.46 Chart of Accounts and Ledger Governance 269

14.47 Revenue Recognition 269

14.48 Accruals, Prepayments, Estimates, and Provisions 269

14.49 Fixed Assets and Intangible Assets 270

14.50 Period-End and Year-End Close..... 270

14.51 Journal Entries..... 270

14.52 Financial Statements and Management Accounts..... 270

14.53 Budgeting, Forecasting, and Variance Analysis 271

14.54 Going Concern and Capital Adequacy 271

14.55 External Accountants, Audit, and Tax Compliance..... 271

14.56 Review and Continuous Improvement 272

Operational Manual Closing Statement..... 273

Introduction

1

Chapter 1 – Introduction and Document Governance

1.1 Welcome to the Bet Play B.V. Operational Manual

This Manual provides a structured description of the governance arrangements, organisational responsibilities, operational procedures, and internal controls maintained by Bet Play B.V. in connection with its activities as a Business-to-Business (“B2B”) gaming-content distributor.

It explains how the Company manages and oversees its commercial activities, business-partner relationships, gaming-content distribution arrangements, regulatory responsibilities, financial operations, operational risks, and reliance on third-party suppliers.

The Manual serves as a central reference for the Company’s Director, officers, employees, contractors, auditors, regulators, business partners, and other authorised stakeholders. It is intended to provide a clear and accurate understanding of Bet Play B.V.’s operating model, the allocation of responsibilities within the Company, and the controls used to support lawful, reliable, and properly supervised operations.

Bet Play B.V. operates a focused and proportionate business model. The Company does not develop proprietary casino games or operate its own gaming platform. It obtains access to Evolution gaming content through its commercial relationship with Babylon Gaming and distributes access to that content to approved third-party gaming operators and gaming resellers.

The underlying games, platform functionality, hosting environment, and principal technical infrastructure are provided and maintained by the relevant upstream suppliers. Bet Play B.V.’s activities are therefore primarily concentrated on:

- Business-partner identification and onboarding.
- Commercial and contractual relationship management.
- Distribution of approved gaming content.
- Coordination of business-partner integrations.
- Compliance and risk oversight.
- Financial administration and invoicing.
- First-line business-partner support.

- Escalation of technical or operational matters to Babylon Gaming or the relevant responsible party.

The procedures and controls described in this Manual have been designed to reflect the nature, scale, and complexity of the Company's activities. Although Bet Play B.V. relies on third-party technology, gaming content, and related services, the Company recognises that it remains responsible for maintaining appropriate oversight of its licensed activities and ensuring that its supplier arrangements are managed consistently with applicable legal, regulatory, and contractual requirements.

1.2 Purpose of the Manual

The purpose of this Manual is to establish a clear, consistent, and proportionate framework for the management and oversight of Bet Play B.V.'s operations. It explains how the Company organises its activities, allocates responsibilities, manages commercial relationships, oversees operational and regulatory risks, and maintains appropriate internal controls.

This Manual has been prepared with reference to Article 5.9 of the National Ordinance on Games of Chance (Landsverordening op de Kansspelen or "LOK"), the conditions attached to the Company's supplier licence, and other applicable requirements and guidance issued by the Curaçao Gaming Authority ("CGA").

In particular, the Manual is intended to:

- Describe the Company's business model and the scope of its licensed B2B activities.
- Define the roles and responsibilities of the Director, Compliance Officer and Money Laundering Reporting Officer ("MLRO"), Chief Financial Officer ("CFO"), Account Management function, and other relevant personnel.
- Explain how prospective business partners are assessed, approved, contracted, and onboarded.
- Describe how the Company distributes gaming content obtained through Babylon Gaming.
- Explain how business-partner integrations, operational matters, and technical issues are coordinated and escalated.
- Establish appropriate controls for regulatory compliance, financial administration, risk management, information security, and record retention.
- Define the Company's arrangements for overseeing suppliers, contractors, and other third-party service providers.

- Support consistent decision-making, clear accountability, and appropriate management oversight.
- Provide employees, management, auditors, regulators, and other authorised stakeholders with an accurate understanding of the Company's operating and control environment.
- Promote the secure, reliable, transparent, and properly supervised conduct of the Company's B2B gaming-content distribution activities.

The Manual should be read together with the Company's applicable policies, procedures, commercial agreements, risk assessments, registers, and operational records. These supporting documents contain more detailed requirements for particular functions and activities.

Where any provision of this Manual conflicts with applicable legislation, a licence condition, or a binding instruction issued by the CGA, the applicable legal or regulatory requirement shall take precedence. The Manual must then be reviewed and amended as soon as reasonably practicable.

1.3 Scope

This Manual applies to Bet Play B.V. and to all Directors, officers, employees, contractors, consultants, and other persons performing activities on behalf of the Company.

Its requirements apply to the Company's principal activities, including:

- Corporate governance and management oversight.
- Regulatory compliance and licence management.
- Business development and commercial approval.
- Business-partner onboarding and due diligence.
- Contract preparation, review, approval, and retention.
- Account management and ongoing business-partner communication.
- Distribution of gaming content obtained through Babylon Gaming.
- Coordination of business-partner integrations.
- First-line commercial and operational support.
- Escalation of technical, content-related, or service-availability matters.

- Financial administration, invoicing, reconciliation, and reporting.
- Business-partner and supplier risk management.
- Information security and data protection.
- Staff competence, awareness, and training.
- Business continuity and operational resilience.
- Regulatory reporting and cooperation with the CGA.

Bet Play B.V. does not develop or own the underlying games, operate a proprietary gaming platform, maintain the underlying game-hosting infrastructure, provide gambling services directly to players, accept wagers, manage player accounts, or hold player funds.

Where the Company engages an external service provider or relies on an upstream supplier, the relevant activity remains subject to appropriate contractual controls, monitoring, incident escalation, recordkeeping, and management oversight.

1.4 Proportionality

Bet Play B.V. applies its operational arrangements in a manner proportionate to the nature, scale, complexity, and risk profile of its business.

The Company maintains a streamlined organisational structure because it does not undertake game development, software engineering, platform hosting, direct player operations, player payment processing, or the management of player accounts. Its principal internal business functions are:

- Account Management.
- Compliance.
- Finance.

These functions operate under the overall direction and oversight of the Company's Director. Technical and development requirements relating to the underlying games and platform services are integrated into the services provided through Babylon Gaming and the relevant upstream gaming provider.

The Company's streamlined structure does not reduce its responsibility to maintain effective governance and appropriate internal controls. Responsibilities must be clearly assigned, material decisions must be documented, operational and regulatory risks must be identified and monitored, and significant matters must be escalated to the appropriate officer or service provider.

Where an activity is performed by an external party, Bet Play B.V. will identify and document, where applicable:

- The party responsible for performing the activity.
- The contractual basis and scope of the arrangement.
- The Company officer responsible for overseeing the relationship.
- The information required to monitor the service.
- The process for reporting and escalating incidents.
- The records that must be maintained.
- The steps available where the service does not meet contractual, operational, or regulatory requirements.

The Company will periodically consider whether its organisational arrangements, staffing, controls, and resources remain appropriate as the business develops or its risk profile changes.

1.5 Supporting Documentation

This Manual should be read together with the Company's supporting documentation, which may include:

- Compliance policies and procedures.
- AML/CFT/CPF policies and business risk assessments.
- Business-partner acceptance, due-diligence and risk assessment procedures.
- Information Security Policy.
- Data Protection and Privacy Policy.
- Business Continuity and Incident Management Plan.

The Operational Manual establishes the overarching framework governing the Company's activities. Supporting policies and procedures provide more detailed instructions for the performance of particular activities and the operation of individual controls.

Where a supporting policy or procedure establishes more detailed or stricter requirements than this Manual, the requirements of that supporting document must be followed, provided that they remain consistent with applicable legislation, licence conditions, and regulatory instructions.

1.6 Ownership and Approval

The Compliance Officer has primary responsibility for ensuring that Bet Play B.V. maintains an appropriate, accurate, and current Operational Manual. The Compliance Officer is also responsible for coordinating periodic reviews of the Manual, identifying amendments required as a result of regulatory or operational developments, and verifying that the document remains consistent with the Company's licence conditions, business model, and internal policies.

Relevant officers and function owners are responsible for reviewing the sections applicable to their activities and informing the Director and Compliance Officer whenever:

- A documented process no longer reflects the Company's actual operations.
- A new activity, service, or business relationship is introduced.
- Responsibilities, delegated authorities, or reporting lines change.
- A control weakness or procedural gap is identified.
- A regulatory amendment affects the Company.
- A material supplier, system, or contractual arrangement changes.
- An incident, audit, or regulatory review identifies a need for amendment.

The Manual and any material amendments must be reviewed and formally approved by the Director. Evidence of approval must be retained as part of the Company's governance records.

Updated versions must be communicated and made accessible to the officers, employees, contractors, and other personnel whose responsibilities are affected by the changes.

1.7 Review and Version Control

The Manual must be reviewed at least annually and additionally whenever a material change occurs.

An additional review may be required following:

- A change to the Company's licence or the scope of its licensed activities.
- A change in ownership, directorship, or key-person appointments.
- The appointment or replacement of a material supplier or service provider.

- The introduction of a new category of gaming content or B2B service.
- A material legislative or regulatory amendment.
- A significant operational, compliance, or information-security incident.
- A material audit, compliance-review, or regulatory finding.
- A significant change to the Company's organisational structure.
- A change affecting the gaming-content distribution chain.
- A material change to the Company's integration or support arrangements.

Each approved version of the Manual must identify:

- The version number.
- The effective date.
- The document owner.
- The signature for approval.
- The scheduled review date.
- A summary of material amendments.

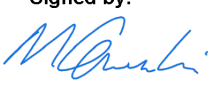
Superseded versions must be securely retained in accordance with the Company's document-retention arrangements. Only the latest approved version should be treated as the current Operational Manual.

1.8 Document Control Table

Document information	Details
Document title	Bet Play B.V. Operational Manual
Company registration number	147087
Document owner	Compliance Officer
Version	1.0
Effective date	1 June 2026
Next scheduled review	Twelve months after approval
Classification	Internal and confidential

Version History

Bet Play B.V

Version	Date	Summary of amendments	Prepared/reviewed by	Signature
1.0	June 1, 2026	Creation of Operational Manual	Compliance Officer	Signed by:  C844330A35F54B6...

Company Overview

2

Chapter 2 – Company Overview and Business Model

2.1 Company Overview

Bet Play B.V. is a company incorporated in Curaçao under registration number 147087 and operates pursuant to a Business-to-Business (“B2B”) supplier licence issued by the Curaçao Gaming Authority (“CGA”).

The Company operates as a distributor of online casino gaming content. Its principal activity is obtaining access to established third-party gaming content through its commercial relationship with Babylon Gaming and distributing access to that content to approved gaming operators and gaming resellers.

Bet Play B.V. does not develop proprietary casino games, operate its own gaming platform, or maintain the underlying systems through which the games are hosted and delivered. The Company's business model is deliberately focused on the commercial distribution and management of third-party gaming content.

The Company's principal operational functions are:

- Account Management.
- Compliance.
- Finance.

These functions operate under the overall direction and oversight of the Director and are supported, where necessary, by appropriately appointed officers, employees, contractors, advisers, and external service providers.

2.2 Corporate Details

Company information	Details
Legal name	Bet Play B.V.
Legal form	Private limited liability company
Country of incorporation	Curaçao
Registration number	147087
Registered address	Trompetbloemweg, 22 Willemstad, Curaçao

Company information	Details
Licence type	B2B Supplier Licence
Licensing authority	Curaçao Gaming Authority
Principal activity	Distribution of third-party online gaming content
Upstream distribution partner	Babylon Gaming
Principal gaming content	Evolution gaming content
Primary client types	Licensed gaming operators and approved gaming resellers

The Company's registered address, licence number, and any other formal particulars should be updated in this table following confirmation against its current corporate and licensing records.

2.3 Ownership Structure

Bet Play B.V. is privately owned. Its ownership and control arrangements are recorded in the Company's corporate registers and have been disclosed to the CGA as part of the applicable licensing process.

The Company maintains complete and current records concerning:

- Its shareholders and their respective ownership interests.
- Its ultimate beneficial owner or owners.
- Its directors and authorised representatives.
- The legal and natural persons exercising control over the Company.
- Any changes affecting its ownership, management, or control.
- Corporate approvals and supporting documentation relating to such changes.

The Compliance Officer is responsible for ensuring that material changes to the Company's ownership, control, governance arrangements, or management structure are assessed and notified to the CGA where required.

Detailed personal information relating to shareholders, ultimate beneficial owners, and officers is maintained securely in the Company's corporate and licensing records and is not reproduced unnecessarily within this Manual.

2.4 Nature of the Business

Bet Play B.V. conducts activities exclusively within the B2B gaming sector. It does not operate an online casino, contract directly with players, or provide gambling services to the public.

The Company obtains access to online casino games through Babylon Gaming, which provides the commercial and technical route through which the relevant gaming content is made available. Bet Play B.V. then distributes access to that content to approved third-party operators and gaming resellers under separate commercial agreements.

The Company's position within the distribution chain may be summarised as follows:

Evolution → Babylon Gaming → Bet Play B.V. → Approved gaming operators and gaming resellers

Within this arrangement:

- Evolution supplies and maintains the underlying gaming content and related game technology.
- Babylon Gaming provides Bet Play B.V. with access to that content and the supporting distribution services.
- Bet Play B.V. manages the commercial relationship with its approved B2B clients and coordinates their access to the available content.
- The licensed operator makes the games available to players through its own player-facing website or gaming platform.
- Where Bet Play B.V.'s client is another gaming reseller, that reseller distributes the content further only in accordance with the applicable contractual and regulatory arrangements.

Bet Play B.V. does not represent that it owns or develops the underlying games. The ownership of the gaming content, software, intellectual property, and related technical systems remains with the relevant rights holders and suppliers.

2.5 Products and Services

Bet Play B.V.'s products and services are limited to activities associated with the B2B distribution of third-party gaming content.

The Company's principal services include:

- Providing approved clients with commercial access to gaming content obtained through Babylon Gaming.
- Presenting the available content portfolio and applicable commercial terms to prospective and existing business partners.
- Conducting due diligence and obtaining internal approval before establishing a business relationship.
- Preparing, reviewing, and administering commercial agreements with operators and gaming resellers.
- Coordinating client onboarding and the activation of approved gaming content.
- Communicating relevant commercial, operational, and integration requirements to business partners.
- Liaising with Babylon Gaming regarding content availability, onboarding, integration, and service-related matters.
- Providing first-line commercial and operational assistance to clients.

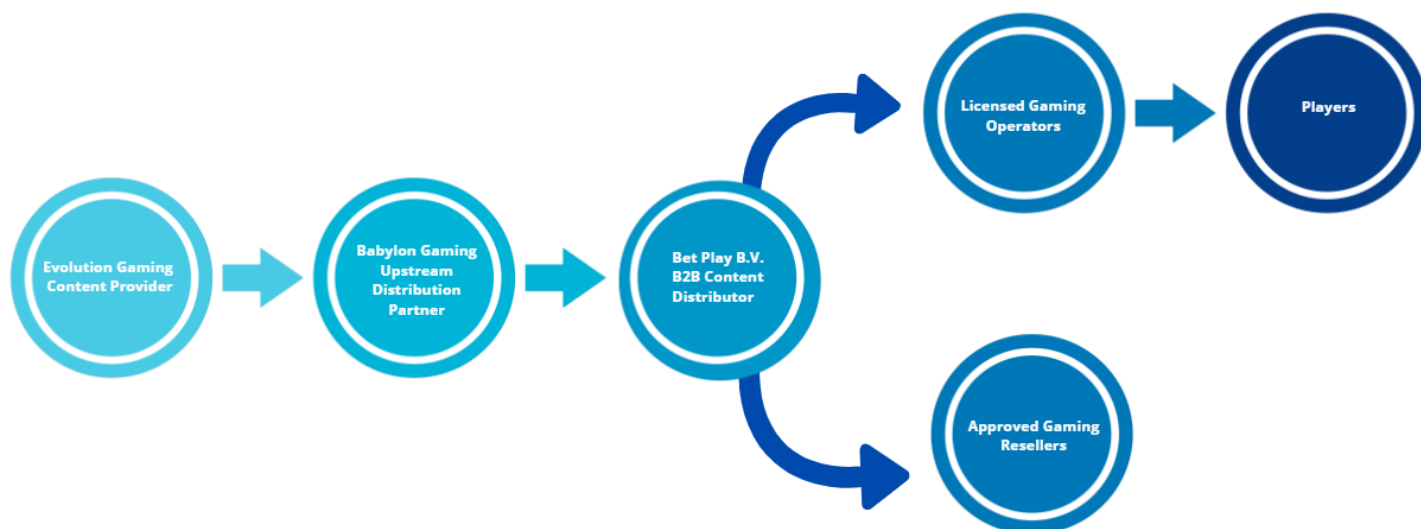


Figure 2.1 – Bet Play B.V. Gaming Content Distribution Model Bet Play B.V. obtains access to Evolution gaming content through Babylon Gaming and distributes that content to approved B2B clients. Bet Play B.V. does not contract directly with players or provide player-facing gambling services.

- Receiving, recording, and escalating technical or content-related issues to Babylon Gaming or another responsible service provider.
- Managing client accounts, invoicing, reconciliations, and ongoing commercial communications.
- Monitoring business relationships for continued compliance with contractual and regulatory requirements.

The exact gaming content available to a client may depend on supplier availability, contractual rights, technical compatibility, licensing restrictions, the client's operating jurisdictions, and any limitations imposed by the relevant content provider.

Bet Play B.V. does not guarantee that all content will be available in every market or through every business relationship.

2.6 Business Partner Profile

Bet Play B.V. provides its services only to approved business partners. These may include:

- Licensed online gaming operators.
- B2B gaming-content resellers.
- Gaming-content aggregators.
- Other appropriately authorised gaming businesses whose activities are compatible with the Company's licence and commercial arrangements.

Before entering into a business relationship, the Company assesses the prospective partner's identity, ownership, management, licensing status, business activities, target markets, reputation, sanctions exposure, and overall risk profile.

A prospective client must not be activated solely because it represents a commercial opportunity. The relationship must first be considered acceptable from regulatory, compliance, legal, operational, and financial perspectives.

Where the prospective client is a gaming reseller, Bet Play B.V. must obtain sufficient information to understand:

- The reseller's business model.
- The markets in which the content will be distributed.
- The types of downstream clients it serves.
- The controls applied when accepting downstream clients.
- Its licensing or authorisation status.
- Any contractual restrictions affecting further distribution.

- The intended use of the gaming content.

The detailed approval and due-diligence process is addressed in Chapter 7 of this Manual.

2.7 Commercial Model

Bet Play B.V. generates revenue through the commercial distribution of gaming content to its approved B2B clients.

The commercial arrangements applicable to each client are established in a written agreement and may be based on:

- A revenue-share arrangement.
- Fees calculated by reference to gaming activity.
- Fixed or minimum monthly charges.
- Setup, activation, or integration-related charges.
- Other agreed B2B commercial fees.

The specific pricing structure may vary depending on the client, expected activity, content package, markets, contractual arrangement, and upstream supplier terms.

The Company does not receive wagers directly from players and does not hold or manage player balances. Amounts payable to Bet Play B.V. arise from its contractual relationships with its B2B clients and not from a direct relationship with individual players.

Account Management and Finance are responsible for ensuring that applicable commercial terms are documented, invoices and supporting calculations are reviewed, payments are reconciled, and material discrepancies are investigated.

2.8 Technology and Integration Model

Bet Play B.V. has not appointed a Chief Technology Officer because it does not develop proprietary games, operate its own gaming platform, or independently maintain the underlying technology used to host and deliver the gaming content it distributes.

The principal technology and development requirements relating to the underlying content are integrated into the services provided through Babylon Gaming and the relevant upstream gaming provider.

Bet Play B.V.'s technology-related responsibilities are limited to the level reasonably required to manage and oversee its distribution activities. These responsibilities include:

- Coordinating the onboarding and integration process between the business partner and Babylon Gaming.
- Communicating integration requirements and required documentation.
- Monitoring the progress of integrations.
- Assisting with routine commercial and operational queries.
- Recording reported technical issues.
- Escalating technical incidents to Babylon Gaming or the appropriate service provider.
- Communicating material updates and resolutions to affected business partners.
- Retaining appropriate records of significant integrations and incidents.
- Monitoring the performance of the supplier relationship from a commercial and operational perspective.

Bet Play B.V. does not independently access, develop, or modify:

- Game source code.
- Game logic or mathematical models.
- Random-number-generation systems.
- Return-to-player configurations.
- Game servers or hosting environments.
- Supplier-controlled platform infrastructure.
- Core integration technology maintained by Babylon Gaming or Evolution.

Where a technical matter is outside the Company’s competence or authority, it must be promptly referred to Babylon Gaming or the responsible upstream provider.

2.9 Division of Responsibilities

Bet Play B.V.’s responsibilities must be clearly distinguished from those of Babylon Gaming, the underlying gaming provider, and the licensed operator.

Activity	Principal responsible party
Development of the underlying games	Evolution or relevant gaming provider
Ownership and maintenance of game software	Evolution or relevant gaming provider

Hosting and technical delivery of gaming content	Upstream provider through the relevant supplier arrangements
Provision of content to Bet Play B.V.	Babylon Gaming
Commercial distribution to Bet Play's clients	Bet Play B.V.
Business-partner due diligence and approval	Bet Play B.V.
Contract and account management	Bet Play B.V.
Coordination of client activation and integration	Bet Play B.V. with Babylon Gaming
Resolution of underlying game or platform defects	Babylon Gaming and/or the relevant upstream provider
First-line communication with Bet Play's clients	Bet Play B.V.
Player registration and account management	Licensed operator
Player identity verification and AML controls	Licensed operator
Acceptance of wagers	Licensed operator
Player deposits, withdrawals, and balances	Licensed operator
Responsible gaming measures	Licensed operator
Player complaints and communications	Licensed operator
Player-facing terms and conditions	Licensed operator

The allocation of operational activities to another party does not remove Bet Play B.V.'s responsibility to oversee its own licensed activities, manage its contractual relationships, and respond appropriately to matters that may affect its regulatory obligations.

2.10 Activities Outside the Company's Scope

Bet Play B.V. does not:

- Develop proprietary casino games or gaming software.
- Operate or maintain a proprietary gaming platform.
- Own or maintain the underlying game-hosting infrastructure.
- Alter or control game logic, RNGs, RTP settings, or game outcomes.
- Certify or independently test the underlying games.
- Operate a player-facing gambling website.
- Register or manage player accounts.
- Accept wagers directly from players.
- Process player deposits or withdrawals.
- Hold or safeguard player funds.
- Perform player customer due diligence on behalf of operators unless expressly agreed and legally permitted.
- Make decisions concerning player affordability, responsible gaming interventions, account suspension, or self-exclusion.
- Provide direct customer support to players.
- Determine the player-facing terms under which an operator offers the games.
- Conduct marketing directly to players as part of its ordinary B2B distribution activities.

These activities remain the responsibility of the relevant operator, gaming provider, or other party identified in the applicable contractual arrangement.

If the Company intends to introduce a materially different product or service, the Director and Compliance Officer must assess the proposed change before implementation. This assessment must consider whether the activity falls within the Company's licence, whether regulatory approval or notification is required, and whether additional personnel, systems, policies, or controls are necessary.

Activities performed by Bet Play B.V.	Activities outside Bet Play B.V.'s scope
Business-partner onboarding	Game development

Due diligence and approval	Game hosting
Commercial account management	Modification of game logic, RNG or RTP
Content-distribution coordination	Player registration and KYC
Integration coordination	Acceptance of wagers
First-line partner assistance	Player payment processing
Invoicing and reconciliation	Holding player funds
Compliance and risk oversight	Responsible gaming interventions
Supplier and incident escalation	Direct player support

Figure 2.2 – Operational Scope and Responsibility Boundaries

Bet Play B.V.'s responsibilities are limited to the commercial distribution and oversight of third-party gaming content. Player-facing and underlying game-technology activities remain with the relevant operator and upstream providers

2.11 Geographic and Jurisdictional Considerations

Bet Play B.V. may establish relationships with business partners operating in different jurisdictions, subject to its licence conditions, upstream supplier restrictions, contractual rights, and internal risk-appetite requirements.

The Company does not assume that gaming content may be distributed in a jurisdiction solely because a prospective client requests access to it. Before approving a business relationship or market, the Company must consider, as applicable:

- The client’s licensing or authorisation status.
- The legality of the proposed activities in the relevant jurisdiction.
- Any restrictions imposed by the CGA.
- Any restrictions imposed by Babylon Gaming or the underlying gaming provider.
- Sanctions and AML/CFT/CPF risks.
- Regulatory warnings, enforcement actions, or blacklisting concerns.
- The client’s target markets and prohibited jurisdictions.
- Whether further distribution by a gaming reseller is permitted.

- Any content-specific or territorial limitations.
- The reputational and commercial risks associated with the relationship.

Where the legality or acceptability of a proposed market or distribution arrangement is uncertain, the matter must be referred to the Compliance Officer and, where appropriate, external legal or regulatory advice must be obtained before proceeding.

2.12 Operational Structure

The Company maintains a proportionate operational structure reflecting the limited and specialised nature of its activities.

Its principal internal functions are:

Account Management

Account Management is responsible for managing prospective and existing business relationships, coordinating onboarding, maintaining regular client communication, communicating commercial and operational requirements, and facilitating the escalation of service-related matters.

Compliance

The Compliance function is responsible for regulatory compliance, business-partner due diligence, risk assessments, policy governance, licence oversight, AML/CFT/CPF controls applicable to the Company, regulatory reporting, and staff awareness.

Finance

The Finance function is responsible for accounting, budgeting, financial reporting, invoicing, reconciliations, treasury administration, audit coordination, and the operation of appropriate financial controls.

These functions report through the Company's established governance structure and remain subject to the oversight of the Director. Further information concerning governance, reporting lines, and the responsibilities of individual officers is provided in Chapters 3 and 4.

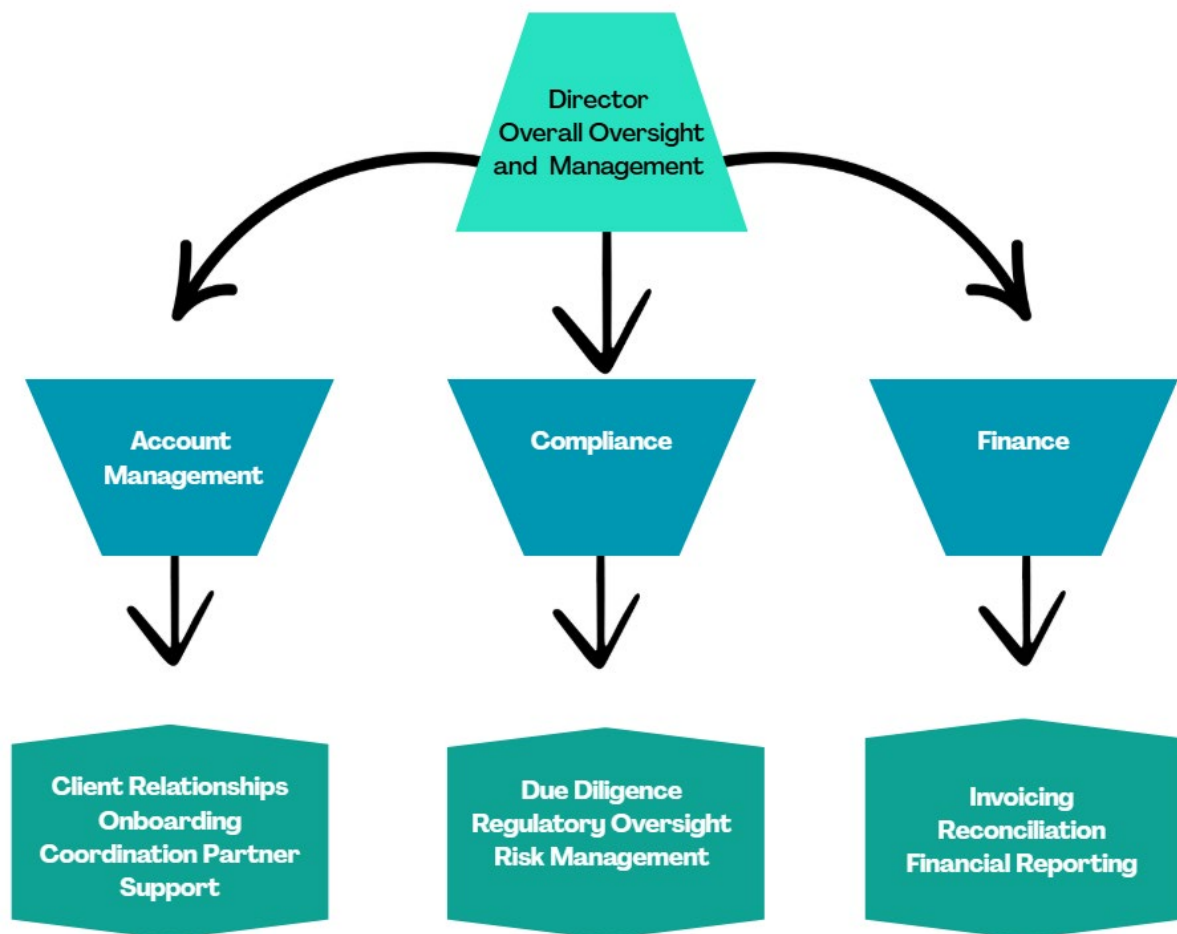


Figure 2.3 – Bet Play B.V. Operational Structure

Bet Play B.V. maintains a proportionate organisational structure consisting of Account Management, Compliance, and Finance under the overall direction and oversight of the Director.

2.13 Strategic Objectives

Bet Play B.V.'s principal objective is to provide approved B2B clients with dependable and commercially efficient access to established online casino gaming content through properly managed distribution arrangements.

In pursuing this objective, the Company seeks to:

- Maintain a commercially relevant portfolio of third-party gaming content.
- Establish sustainable relationships with suitable operators and gaming resellers.
- Conduct appropriate due diligence before entering into business relationships.

- Maintain clear and effective commercial agreements.
- Coordinate business-partner onboarding and integrations efficiently.
- Provide responsive first-line commercial and operational assistance.
- Maintain effective communication with Babylon Gaming.
- Escalate technical and service-related matters promptly.
- Operate in accordance with its licence and applicable regulatory requirements.
- Maintain proportionate governance, compliance, risk-management, and financial controls.
- Monitor the risks arising from reliance on upstream suppliers.
- Pursue controlled growth consistent with the Company's available resources and risk appetite.

The Company reviews its objectives, client portfolio, supplier relationships, operational capacity, and risk profile periodically to ensure that its business continues to operate on a sustainable and properly controlled basis.

2.14 Changes to the Business Model

Any proposed material change to the Company's business model must be reviewed before implementation.

Material changes may include:

- Distributing content from a new gaming provider.
- Appointing or replacing a principal upstream distribution partner.
- Introducing proprietary technology or platform services.
- Expanding into a materially different category of B2B gaming activity.
- Commencing direct technical hosting or software-development activities.
- Entering new markets presenting significant regulatory or sanctions risks.
- Introducing direct player-facing services.
- Processing or holding player funds.
- Materially changing the Company's revenue or contractual model.

The Director must ensure that the Compliance Officer and other relevant officers are consulted before such a change is approved. The review must determine whether the proposed activity:

- Falls within the scope of the Company's licence.
- Requires prior approval or notification to the CGA.

- Is permitted under the Company's supplier and commercial agreements.
- Requires additional policies, systems, personnel, expertise, or controls.
- Creates new operational, financial, regulatory, technical, or reputational risks.
- Requires amendments to this Manual or other governance documentation.

No material change should be implemented until the required internal approvals, contractual arrangements, risk assessments, and regulatory steps have been completed.

Corporate Governance & Organisational Structure

3

Chapter 3 – Corporate Governance and Organisational Structure

3.1 Corporate Governance Framework

Bet Play B.V. maintains a proportionate corporate governance framework appropriate to the nature, scale, and complexity of its activities as a Business-to-Business (“B2B”) gaming-content distributor.

The governance framework is designed to ensure that:

- The Company is directed and managed responsibly.
- Strategic and material operational decisions are subject to appropriate oversight.
- Responsibilities and reporting lines are clearly established.
- Regulatory, financial, operational, and commercial risks are properly considered.
- Conflicts of interest are identified and managed.
- Material decisions and approvals are appropriately documented.
- The Company maintains sufficient oversight of activities performed by external service providers and upstream suppliers.
- Appropriate information is made available to the Curaçao Gaming Authority (“CGA”) and other authorised parties when required.

The Director retains ultimate responsibility for the management, direction, and regulatory compliance of the Company. Operational responsibilities may be delegated to appointed officers, employees, contractors, or external service providers; however, such delegation does not remove the Director’s responsibility to maintain effective oversight.

The Company’s principal governance and operational functions are:

- Executive management.
- Account Management.
- Compliance.
- Finance.

The underlying technology, game development, hosting, and technical infrastructure supporting the distributed gaming content are provided through Babylon Gaming and the relevant upstream gaming provider. Bet Play B.V. therefore does not maintain a separate internal technology or game-development department.

3.2 Governance Principles

The Company's governance arrangements are based on the following principles:

Accountability

Each Director, officer, employee, contractor, and function owner is accountable for the proper performance of the responsibilities assigned to them.

Clear Allocation of Responsibilities

Responsibilities must be allocated clearly and communicated to the persons concerned. Material activities must have an identifiable owner responsible for their performance, monitoring, and escalation.

Appropriate Oversight

The Director must receive sufficient information to oversee the Company's operations, financial position, compliance status, business relationships, and material risks.

Proportionality

Governance arrangements are maintained in a manner proportionate to the Company's focused business model and operational risk profile.

Independence of Control Functions

The Compliance Officer and Money Laundering Reporting Officer ("MLRO") must be able to perform their duties objectively and raise matters directly with the Director without improper commercial influence.

Documented Decision-Making

Material business, compliance, financial, and supplier-related decisions must be documented in sufficient detail to demonstrate the basis of the decision, the persons involved, and any conditions or follow-up actions.

Regulatory Cooperation

The Company must cooperate openly and promptly with the CGA and other competent authorities, subject to applicable legal and confidentiality requirements.

Oversight of Third Parties

Reliance on Babylon Gaming or another external service provider does not remove the Company's responsibility to oversee its own licensed activities and manage the risks arising from the arrangement.

3.3 Organisational Structure

Bet Play B.V. maintains a streamlined organisational structure reflecting its limited and specialised role as a distributor of third-party gaming content.

The Company is governed by its Director, who is supported by the Compliance Officer and MLRO, Chief Financial Officer (“CFO”), and the Account Management function.

The organisational structure is as follows:



Figure 3.1 – Bet Play B.V. Governance and Organisational Structure

The Director retains overall responsibility for the Company. Account Management, Compliance, and Finance operate under the Director’s oversight and may be supported by appropriately appointed external advisers and service providers.

This structure may be expanded or amended where required by the growth of the business, changes in regulatory requirements, or the introduction of new products, services, markets, or material risks.

3.4 Director and Executive Oversight

The Director is responsible for the overall governance, strategic direction, and management of Bet Play B.V.

The Director's governance responsibilities include:

- Establishing the Company's strategic and commercial objectives.
- Ensuring that the Company operates within the scope of its licence.
- Approving material business relationships and contractual arrangements.
- Overseeing operational and financial performance.
- Ensuring that appropriate policies, procedures, controls, and resources are maintained.
- Reviewing material compliance, risk, financial, and operational matters.
- Ensuring that significant issues are addressed and appropriately escalated.
- Approving material changes to the Company's activities or organisational structure.
- Overseeing the Company's relationship with Babylon Gaming and other significant service providers.
- Ensuring that required notifications and reports are made to the CGA.
- Promoting an appropriate culture of compliance, accountability, and responsible business conduct.

The Director may delegate specific responsibilities where appropriate. Delegated responsibilities must be clearly defined, assigned to a competent person, and subject to ongoing oversight.

Matters of material regulatory, financial, legal, commercial, or reputational significance must remain subject to the Director's review and approval.

3.5 Compliance Governance

The Compliance function provides oversight of the Company's adherence to applicable legal, regulatory, licensing, and internal requirements.

The Compliance Officer is responsible for supporting the Director by:

- Monitoring the Company's regulatory obligations.
- Advising on the compliance implications of proposed activities and business relationships.
- Coordinating business-partner due diligence and risk assessments.
- Monitoring the Company's compliance framework and internal policies.
- Maintaining relevant compliance records and registers.
- Identifying and escalating actual or potential regulatory breaches.
- Coordinating regulatory reporting and correspondence.

- Supporting internal reviews and external audits.
- Monitoring relevant legislative and regulatory developments.
- Promoting compliance awareness among personnel.
- Reporting material compliance matters directly to the Director.

The Compliance Officer must be provided with access to the information, records, personnel, and management support reasonably required to perform the role effectively.

Commercial considerations must not prevent or delay the escalation of a material compliance concern.

3.6 AML/CFT/CPF Governance

The MLRO is responsible for overseeing the Company's framework for preventing money laundering, terrorist financing, and proliferation financing to the extent applicable to its activities.

Although Bet Play B.V. does not accept wagers, maintain player accounts, process player deposits or withdrawals, or hold player funds, it may be exposed to financial-crime risks through its business partners, commercial transactions, ownership structures, operating jurisdictions, and payment arrangements.

The MLRO's governance responsibilities include:

- Overseeing the Company's AML/CFT/CPF framework.
- Supporting the preparation and maintenance of the business risk assessment.
- Ensuring that appropriate due diligence is conducted on business partners and other relevant counterparties.
- Reviewing elevated-risk relationships and transactions.
- Assessing internal reports concerning unusual or suspicious activity.
- Determining whether an external report is required to a competent authority.
- Maintaining appropriate confidentiality in relation to internal and external reports.
- Ensuring that applicable records are retained.
- Supporting relevant staff awareness and training.
- Reporting material AML/CFT/CPF matters directly to the Director.

Where the Compliance Officer and MLRO positions are held by the same person, the responsibilities attached to each function remain separately identifiable and must be performed with appropriate independence and authority.

3.7 Financial Governance

The Finance function is overseen by the CFO and is responsible for maintaining appropriate financial administration, reporting, and internal controls.

The Company's financial governance arrangements are intended to ensure that:

- Financial transactions are properly authorised and recorded.
- Revenue and expenses are supported by appropriate documentation.
- Client invoices are accurate and consistent with contractual arrangements.
- Receipts and outstanding balances are monitored.
- Payments are subject to appropriate review and approval.
- Bank accounts and accounting records are reconciled.
- Financial performance and liquidity are monitored.
- Tax, accounting, audit, and regulatory obligations are addressed.
- Material financial irregularities or discrepancies are escalated.
- Financial records are retained securely and remain available for inspection.

The CFO reports material financial matters to the Director, including significant overdue balances, unusual transactions, liquidity concerns, material accounting discrepancies, and matters that may affect the Company's continued financial stability.

The Director retains ultimate oversight of the Company's financial affairs and approves material expenditure, banking arrangements, financial commitments, and other significant financial decisions.

3.8 Account Management Governance

Account Management is responsible for managing the Company's commercial relationships with prospective and existing business partners.

Its governance responsibilities include:

- Acting as the principal point of contact for assigned business partners.
- Coordinating prospective-client information gathering and onboarding.

- Referring prospective partners to Compliance for due diligence and approval.
- Ensuring that services are not activated before the required approvals and agreements are in place.
- Communicating commercial and operational requirements.
- Coordinating integration and activation activities with Babylon Gaming.
- Maintaining appropriate records of significant client communications.
- Monitoring the ongoing commercial relationship.
- Identifying material changes in a client's business, ownership, licensing status, or markets.
- Escalating complaints, incidents, technical matters, contractual concerns, and compliance issues.
- Coordinating internal communication between the client, Compliance, Finance, and management.

Account Management does not have authority to override a compliance decision or activate a client that has not completed the required approval process.

Where Account Management becomes aware of information that may affect the acceptability of a business partner, the matter must be reported promptly to the Compliance Officer.

3.9 Delegation of Authority

The Director may delegate operational responsibilities to the Compliance Officer, MLRO, CFO, Account Management personnel, or another competent person.

Any material delegation should specify:

- The responsibility or authority being delegated.
- The person or function receiving the delegation.
- The scope and limits of the authority.
- Any financial or approval threshold.
- The duration of the delegation, where applicable.
- The reporting and escalation requirements.
- The matters reserved for the Director.
- The arrangements applicable during absence or unavailability.

Delegation does not transfer the Director's ultimate responsibility for overseeing the Company.

The following matters must remain subject to approval by the Director unless a formally documented governance arrangement provides otherwise:

- Material changes to the Company's business model.
- Entry into significant supplier or distribution arrangements.
- Approval of material business-partner relationships.
- Entry into new high-risk jurisdictions or markets.
- Material contractual commitments.
- Material expenditure or financial commitments.
- Opening or closing Company bank accounts.
- Appointment or removal of key officers.
- Material regulatory notifications or submissions.
- Responses to significant regulatory findings.
- Approval of material policies and amendments to this Manual.
- Suspension or termination of a significant business relationship.
- Actions arising from material compliance, financial, or operational incidents.

3.10 Management Decision-Making

The Company's governance structure must support timely, informed, and appropriately documented decision-making.

Material decisions should take account of:

- The Company's licensed activities.
- Applicable legal and regulatory requirements.
- The Company's risk appetite.
- Commercial and financial implications.
- Compliance and reputational risks.
- Contractual obligations and supplier restrictions.
- Operational capacity and available resources.
- Information-security and data-protection implications.
- The interests of the Company and its legitimate stakeholders.

Depending on the nature of the matter, the Director may consult the Compliance Officer, MLRO, CFO, Account Management, external legal advisers, auditors, accountants, or other subject-matter experts before making a decision.

Decisions requiring formal documentation may be recorded through:

- Written Director resolutions.
- Management meeting minutes.
- Approval forms.
- Compliance assessments.
- Risk assessments.
- Contract approval records.
- Written email approvals.
- Entries in the relevant internal register.

The level of documentation should be proportionate to the significance and risk of the decision.

3.1.1 Management Meetings and Reporting

Management oversight may be conducted through scheduled meetings, written reports, direct consultations, or a combination of these methods.

Management reviews should address relevant matters such as:

- Business development and commercial performance.
- New and pending business-partner applications.
- Existing business-partner risks and material changes.
- Compliance monitoring and regulatory developments.
- AML/CFT/CPF matters.
- Financial performance, cash flow, and outstanding receivables.
- Material incidents, complaints, and service interruptions.
- Supplier performance and issues involving Babylon Gaming.
- Audit findings and corrective actions.
- Staffing, resources, training, and operational capacity.
- Material changes proposed to the Company's products or services.

The frequency and format of management reporting may be adapted to the volume and complexity of the Company's activities. However, urgent or material matters must be escalated immediately and must not be deferred until the next scheduled meeting.

Records of material discussions, decisions, assigned actions, responsible persons, and completion dates must be retained.

3.1.2 Reserved Matters and Escalation

The Company applies an escalation framework to ensure that material matters reach the appropriate decision-maker promptly.

Immediate escalation to the Director and, where relevant, the Compliance Officer or MLRO is required where a matter involves:

- A suspected breach of legislation or a licence condition.
- A request, inquiry, or formal communication from the CGA.
- Suspected money laundering, terrorist financing, proliferation financing, fraud, or sanctions exposure.
- A material information-security or personal-data incident.
- A significant or prolonged interruption affecting distributed gaming content.
- A material dispute with Babylon Gaming or another significant supplier.
- A material contractual breach by a business partner.
- Use of gaming content in an unauthorised or restricted jurisdiction.
- A significant financial irregularity or unexplained transaction.
- A threat to the Company's financial stability or continued operations.
- A significant complaint, legal claim, or enforcement matter.
- A material reputational risk.
- A conflict of interest affecting an important decision.

The person receiving the escalation must assess the matter, determine the required response, assign responsibility for follow-up, and ensure that the decision and actions taken are documented.

3.13 Conflicts of Interest

Directors, officers, employees, contractors, and advisers acting for the Company must avoid situations in which personal, financial, commercial, or other interests improperly influence—or appear to influence—the performance of their duties.

A person must disclose any actual, potential, or perceived conflict of interest concerning:

- A prospective or existing business partner.
- Babylon Gaming or another supplier.
- A proposed contract or commercial arrangement.
- A payment or financial transaction.
- The appointment of an employee, contractor, or adviser.

- A regulatory, compliance, or risk-management decision.
- Any entity in which the person or a connected party holds an interest.

Disclosures must be made promptly to the Director or, where the Director is affected, recorded and addressed through an appropriate independent review or governance process.

Depending on the circumstances, the Company may:

- Require the affected person to withdraw from discussions or decisions.
- Assign the matter to another competent person.
- Obtain independent legal, compliance, or financial advice.
- Decline or terminate the proposed arrangement.
- Document safeguards permitting the activity to continue.
- Notify the CGA where required.

Conflicts and the measures taken to manage them must be documented and retained.

3.14 Independence and Access to Information

The Compliance Officer, MLRO, and CFO must have access to the records and information reasonably required to perform their duties.

They must be permitted to:

- Raise concerns directly with the Director.
- Obtain information from relevant personnel and service providers.
- Review records within the scope of their responsibilities.
- Recommend corrective or preventive action.
- Escalate unresolved or material concerns.
- Communicate with regulators, auditors, banks, or professional advisers where authorised or legally required.

No person may conceal relevant information, obstruct a review, retaliate against a person who raises a legitimate concern, or improperly influence the outcome of a compliance, AML, risk, or financial assessment.

3.15 Use and Oversight of External Service Providers

Bet Play B.V. may engage external advisers, contractors, accountants, auditors, legal professionals, compliance specialists, or other service providers where specialist knowledge or additional operational support is required.

Before appointing a material service provider, the Company should consider:

- The provider's identity, ownership, competence, and reputation.
- Its experience and professional qualifications.
- The scope and criticality of the proposed service.
- Confidentiality and data-protection requirements.
- Potential conflicts of interest.
- Business-continuity arrangements.
- Regulatory access and audit rights, where applicable.
- The provider's ability to meet contractual and regulatory requirements.

Each material external arrangement must have an appointed internal owner responsible for overseeing performance and escalating concerns.

The Company must retain sufficient knowledge and control to understand the service being provided, assess whether it remains appropriate, and respond effectively if the provider fails to perform.

3.16 Succession and Temporary Absence Arrangements

The Company must maintain reasonable arrangements to ensure continuity where a Director, officer, or other person responsible for a critical function is temporarily unavailable.

These arrangements may include:

- Designating an appropriately competent alternate.
- Temporarily reallocating responsibilities.
- Engaging an approved external service provider.
- Providing secure access to essential records and contact information.
- Documenting pending matters and required follow-up actions.
- Informing relevant personnel and external parties of temporary reporting arrangements.
- Notifying the CGA where an absence or replacement affects a licensed or approved position and notification is required.

Temporary delegations must be clearly documented and must not assign regulated or specialist responsibilities to a person who lacks the necessary competence, authority, or approval.

3.17 Governance Records

The Company maintains records sufficient to demonstrate the operation of its governance arrangements.

These may include:

- Corporate registers and constitutional documents.
- Director and shareholder resolutions.
- Management meeting minutes.
- Organisational charts.
- Job descriptions and appointment records.
- Delegated-authority records.
- Conflict-of-interest declarations.
- Material approval records.
- Management and compliance reports.
- Risk assessments and decision records.
- Regulatory correspondence and submissions.
- External adviser and service-provider agreements.

Governance records must be accurate, appropriately protected, accessible to authorised persons, and retained in accordance with applicable legal, regulatory, and internal record-retention requirements.

3.18 Review of Governance Arrangements

The Director and Compliance Officer must periodically assess whether the Company's governance arrangements remain appropriate and effective.

The review should consider:

- Changes in the Company's activities or business model.
- Growth in the number or complexity of business relationships.
- Changes to Babylon Gaming or other material supplier arrangements.
- Regulatory developments or changes to licence conditions.
- Audit findings, compliance reviews, and identified control weaknesses.
- Significant incidents, breaches, or disputes.
- Changes in personnel or reporting lines.

- The adequacy of resources, competence, and segregation of responsibilities.
- Whether additional management or specialist functions are required.

Any material weakness or gap must be documented, assigned to an appropriate person, and addressed within a reasonable period according to its seriousness and regulatory significance.

Roles, Responsibilities and Key Functions

4

Chapter 4 – Roles, Responsibilities and Key Functions

4.1 Purpose

This chapter defines the roles, responsibilities, authority, reporting lines, and accountability of the persons and functions responsible for managing Bet Play B.V.

Clear allocation of responsibilities is intended to ensure that:

- Each material activity has an identifiable owner.
- Personnel understand the scope and limitations of their authority.
- Commercial, compliance, financial, and operational matters are appropriately reviewed.
- Material risks and concerns are escalated promptly.
- Conflicting responsibilities are identified and managed.
- The Company maintains effective oversight of activities performed by Babylon Gaming and other external service providers.
- Appropriate continuity arrangements are maintained during temporary absences.
- The Director receives sufficient information to oversee the Company's licensed activities.

The Company's principal roles and functions are:

- Director and Chief Executive Officer.
- Compliance Officer.
- Money Laundering Reporting Officer.
- Chief Financial Officer.
- Account Management.
- External advisers and service providers.

Where one person performs more than one role, the responsibilities and decisions associated with each role must remain clearly identifiable.

4.2 General Responsibilities of Officers and Personnel

All Directors, officers, employees, contractors, and other persons acting on behalf of Bet Play B.V. are expected to:

- Perform their responsibilities honestly, diligently, and competently.
- Act within the scope of their authority.
- Comply with applicable legislation, licence conditions, internal policies, and lawful management instructions.
- Protect confidential, commercially sensitive, and personal information.
- Identify and disclose actual, potential, or perceived conflicts of interest.
- Maintain complete and accurate records relevant to their responsibilities.
- Cooperate with internal reviews, external audits, and regulatory inquiries.
- Complete required training and maintain appropriate knowledge of their responsibilities.
- Report actual or suspected breaches, incidents, errors, irregularities, and control weaknesses.
- Escalate matters that exceed their authority or competence.
- Avoid making commitments on behalf of the Company without appropriate approval.
- Support a culture of compliance, accountability, and responsible business conduct.

No person may disregard a compliance, AML/CFT/CPF, financial-control, or information-security requirement solely to expedite a commercial relationship or transaction.

4.3 Director and Chief Executive Officer

The Director and Chief Executive Officer is responsible for the overall direction, governance, management, and performance of Bet Play B.V.

The Director retains ultimate responsibility for ensuring that the Company operates:

- Within the scope of its B2B supplier licence.
- In accordance with applicable legal and regulatory requirements.
- Consistently with its approved business model.
- Within its risk appetite and available operational resources.
- Under appropriate governance, compliance, financial, and operational controls.

Delegation of an activity to another officer, employee, contractor, or external provider does not remove the Director's responsibility to maintain appropriate oversight.

4.3.1 Strategic and Corporate Responsibilities

The Director is responsible for:

- Establishing and approving the Company's strategy and objectives.
- Overseeing the implementation of the approved business model.
- Ensuring that the Company maintains appropriate financial, human, and operational resources.
- Approving material changes to the Company's products, services, markets, or distribution arrangements.
- Overseeing the Company's corporate and licensing obligations.
- Ensuring that the CGA is notified of relevant changes where required.
- Approving appointments to key management or control functions.
- Ensuring that ownership, control, and governance records remain accurate and current.
- Reviewing the Company's operational capacity as its business develops.
- Promoting appropriate standards of integrity, accountability, and regulatory compliance.

4.3.2 Commercial Responsibilities

The Director's commercial responsibilities include:

- Approving material business-partner relationships.
- Approving material contracts and commercial commitments.
- Establishing or approving commercial parameters and pricing principles.
- Reviewing significant departures from standard contractual terms.
- Overseeing the Company's relationship with Babylon Gaming.
- Approving the appointment or replacement of material suppliers.
- Reviewing significant commercial disputes or contractual breaches.
- Approving the suspension or termination of material business relationships.
- Ensuring that commercial growth remains consistent with the Company's licence, resources, contractual rights, and risk appetite.

The Director must consider compliance, legal, financial, operational, technical, and reputational risks before approving a material relationship or commitment.

4.3.3 Regulatory and Compliance Responsibilities

The Director is responsible for:

- Ensuring that an appropriate compliance framework is established and maintained.
- Providing the Compliance Officer and MLRO with sufficient authority, access, and resources.
- Reviewing material compliance and AML/CFT/CPF matters.
- Ensuring that identified breaches and control weaknesses are addressed.
- Approving material regulatory notifications and submissions.
- Ensuring cooperation with the CGA and other competent authorities.
- Reviewing significant audit or regulatory findings.
- Approving corrective-action plans and monitoring their completion.
- Ensuring that commercial considerations do not improperly override regulatory requirements.

4.3.4 Financial Responsibilities

The Director's financial responsibilities include:

- Overseeing the Company's financial position and sustainability.
- Approving budgets and material expenditure.
- Approving significant payments and financial commitments in accordance with established authority limits.
- Approving the opening or closure of Company bank accounts.
- Reviewing material financial reports and cash-flow information.
- Ensuring that appropriate accounting, reconciliation, and financial-control arrangements are maintained.
- Addressing significant overdue balances, discrepancies, unusual transactions, or liquidity concerns.
- Ensuring that applicable tax, accounting, audit, and regulatory financial obligations are addressed.

4.3.5 Director Reporting and Records

Material decisions taken by the Director must be documented through an appropriate record, which may include:

- A written Director resolution.
- Management meeting minutes.
- A contract or business-partner approval form.
- A written risk-acceptance decision.
- An email approval.
- An entry in the relevant governance or compliance register.

The record should identify the decision, the information considered, any conditions imposed, the responsible person, and any required follow-up action.

4.4 Compliance Officer

The Compliance Officer is responsible for coordinating and overseeing the Company's compliance with applicable legislation, CGA requirements, licence conditions, internal policies, and relevant contractual obligations.

The Compliance Officer operates as a control function and must be permitted to raise concerns directly with the Director.

4.4.1 Regulatory Compliance

The Compliance Officer is responsible for:

- Identifying and maintaining an overview of the Company's regulatory obligations.
- Monitoring relevant legislative, regulatory, and licensing developments.
- Assessing the effect of regulatory changes on the Company.
- Advising management on the compliance implications of proposed activities.
- Coordinating required amendments to policies, procedures, and this Manual.
- Maintaining appropriate compliance calendars, registers, and records.
- Coordinating regulatory reporting and correspondence.
- Supporting licence applications, renewals, amendments, and notifications.
- Monitoring completion of regulatory commitments and corrective actions.
- Supporting inspections, audits, and regulatory reviews.
- Escalating actual or suspected breaches to the Director.

4.4.2 Business-Partner Compliance

In relation to prospective and existing business partners, the Compliance Officer is responsible for:

- Coordinating business-partner due diligence.
- Verifying that required information and documentation have been obtained.
- Assessing ownership, control, licensing, jurisdictional, sanctions, reputational, and financial-crime risks.
- Assigning or recommending an appropriate risk classification.
- Identifying enhanced due-diligence requirements.
- Assessing the intended markets and distribution model.
- Reviewing whether further distribution by a reseller is acceptable.
- Documenting the compliance recommendation or decision.
- Establishing conditions applicable to an approved relationship.
- Conducting or coordinating periodic and event-driven reviews.
- Monitoring material changes affecting approved partners.
- Recommending the restriction, suspension, or termination of relationships where necessary.

The Compliance Officer may refuse to recommend approval where the required due diligence has not been completed or the identified risks are outside the Company's risk appetite.

4.4.3 Compliance Monitoring

The Compliance Officer coordinates proportionate monitoring of the Company's compliance framework. This may include reviewing:

- Business-partner files and approvals.
- Licensing and corporate records.
- Contractual and jurisdictional restrictions.
- Compliance with onboarding conditions.
- Material complaints, incidents, and breaches.
- Supplier and outsourcing arrangements.
- Training completion.
- Regulatory reporting deadlines.
- Completion of corrective actions.
- The accuracy and implementation of relevant policies and procedures.

Monitoring findings must be documented and material weaknesses escalated to the Director.

4.4.4 Compliance Advice and Escalation

The Compliance Officer must be consulted where a matter involves:

- A proposed new product, service, market, or material supplier.
- An uncertain licensing or regulatory position.
- A prospective business partner presenting elevated risk.
- A proposed exception to an established compliance requirement.
- Suspected unauthorised use or distribution of gaming content.
- A potential breach of legislation or a licence condition.
- A regulatory inquiry, inspection, or information request.
- A material complaint or dispute with regulatory implications.
- A significant change to a business partner's ownership, licence, markets, or activities.

Where the Compliance Officer considers that a proposed activity is unlawful, outside the Company's licence, or presents an unacceptable regulatory risk, the matter must not proceed unless the concern has been resolved through appropriate legal or regulatory clarification.

4.5 Money Laundering Reporting Officer

The MLRO is responsible for overseeing the Company's AML/CFT/CPF arrangements to the extent applicable to Bet Play B.V.'s B2B activities.

Bet Play B.V. does not maintain player accounts, accept wagers, process player deposits or withdrawals, or hold player funds. Its financial-crime exposure arises primarily through:

- Business partners and their ownership structures.
- Commercial payments and settlement arrangements.
- Operating and target jurisdictions.
- Suppliers and other contractual counterparties.
- Unusual or unexplained business activity.
- Sanctions and adverse-media exposure.
- Attempts to misuse the Company's content-distribution relationships.

4.5.1 AML/CFT/CPF Framework

The MLRO is responsible for:

- Maintaining oversight of the Company's AML/CFT/CPF framework.
- Coordinating the preparation and review of the business risk assessment.
- Ensuring that applicable due-diligence requirements are reflected in internal procedures.
- Supporting risk-based classification of business partners and relevant counterparties.
- Reviewing higher-risk relationships and proposed risk exceptions.
- Monitoring changes in applicable sanctions and financial-crime risks.
- Ensuring that relevant personnel receive appropriate AML/CFT/CPF awareness training.
- Maintaining appropriate internal-reporting arrangements.
- Advising the Director on material financial-crime risks.
- Retaining relevant AML/CFT/CPF records securely.

4.5.2 Internal Reports and Suspicious Activity

Any officer, employee, contractor, or other person acting for the Company who identifies suspicious or unusual activity must report it promptly to the MLRO.

The MLRO is responsible for:

- Receiving and assessing internal reports.
- Obtaining additional information where necessary and legally permissible.
- Documenting the assessment and decision.
- Determining whether an external report is required.
- Making external reports to the competent authority where legally required.
- Protecting the confidentiality of reports and related information.
- Preventing unauthorised disclosure or tipping-off.
- Advising management on any operational measures that may lawfully be taken.

The MLRO must be able to make a required external report without seeking commercial approval. The Director may be informed only to the extent legally permissible and without compromising the confidentiality of the reporting process.

4.5.3 Independence of the MLRO

The MLRO must:

- Have direct access to the Director.
- Have access to relevant business-partner, contractual, and financial information.
- Be free from improper commercial interference.
- Be able to obtain professional advice where necessary.
- Maintain the confidentiality of sensitive AML/CFT/CPF information.
- Have sufficient competence and authority to perform the role.

Where the same person acts as both Compliance Officer and MLRO, decisions and records relating to suspicious activity must remain subject to the specific confidentiality requirements applicable to the MLRO function.

4.6 Chief Financial Officer

The CFO is responsible for overseeing the Company's financial administration, accounting, reporting, and internal financial controls.

4.6.1 Financial Administration

The CFO's responsibilities include:

- Maintaining complete and accurate accounting records.
- Coordinating bookkeeping and accounting services.
- Preparing or overseeing management accounts and financial reports.
- Monitoring income, expenditure, cash flow, and liquidity.
- Supporting the preparation and monitoring of budgets.
- Maintaining appropriate records of financial commitments.
- Coordinating tax filings, statutory accounts, and external audits.
- Ensuring that financial records remain available for authorised review.

4.6.2 Invoicing and Revenue Controls

In relation to client invoicing, the CFO is responsible for:

- Ensuring that invoices reflect the applicable contractual terms.
- Reviewing supporting revenue or activity reports.
- Confirming applicable revenue-share percentages, fixed fees, minimum charges, and other agreed amounts.
- Ensuring that invoice adjustments and credit notes are appropriately authorised.

- Monitoring issued invoices and outstanding receivables.
- Investigating material discrepancies or disputes.
- Reconciling amounts received against issued invoices.
- Escalating significant overdue balances to the Director and Account Management.

Account Management may support the validation of commercial information, but Finance retains responsibility for financial recording and reconciliation.

4.6.3 Payments and Expenditure

The CFO is responsible for:

- Verifying that payments are supported by appropriate invoices or documentation.
- Confirming that expenditure has been approved by an authorised person.
- Applying established payment-approval limits.
- Maintaining appropriate separation between payment preparation and approval where operationally practicable.
- Verifying supplier banking details and material changes to payment instructions.
- Monitoring unusual, duplicate, or potentially erroneous payments.
- Retaining evidence of payment review and approval.
- Escalating suspicious or unexplained transactions to the Director and MLRO.

4.6.4 Reconciliation and Financial Reporting

The CFO coordinates:

- Bank reconciliations.
- Client account reconciliations.
- Supplier and upstream-provider reconciliations.
- Revenue and fee reconciliations.
- Review of outstanding receivables and liabilities.
- Investigation and resolution of material variances.
- Periodic reporting to the Director.

Material unresolved discrepancies must be documented and escalated.

4.6.5 Financial Escalation

The CFO must report promptly to the Director where a matter involves:

- A material accounting discrepancy.

- An unauthorised or potentially fraudulent payment.
- A significant overdue balance.
- A material deterioration in cash flow or liquidity.
- A tax, audit, or statutory reporting concern.
- An unusual transaction or payment arrangement.
- A financial matter that may affect the Company's licence or continued operations.
- A suspected breach of financial controls.
- A request to make or receive payment through an unrelated third party.

Where appropriate, the MLRO and Compliance Officer must also be notified.

4.7 Account Management Function

Account Management is responsible for managing the Company's relationships with prospective and existing business partners.

Account Management serves as the principal coordination point between the business partner, the Director, Compliance, Finance, and Babylon Gaming.

4.7.1 Prospective Business Partners

For prospective relationships, Account Management is responsible for:

- Receiving and documenting commercial inquiries.
- Obtaining preliminary information about the prospective partner.
- Understanding the proposed business model, products, markets, and distribution arrangements.
- Providing the prospective partner with approved information about available gaming content.
- Explaining the Company's onboarding and due-diligence requirements.
- Referring the prospective partner to Compliance for review.
- Coordinating requests for outstanding information.
- Supporting the preparation and negotiation of commercial terms.
- Ensuring that the partner is not activated before approval and execution of the required agreement.
- Maintaining records of material communications and agreed actions.

Account Management must not make representations concerning regulatory approval, content availability, integration completion, or market access unless the relevant matter has been confirmed by the responsible function or supplier.

4.7.2 Existing Business Partners

For existing relationships, Account Management is responsible for:

- Acting as the business partner's principal commercial contact.
- Maintaining regular and professional communication.
- Monitoring the status and needs of assigned accounts.
- Coordinating requests for additional content or services.
- Communicating relevant supplier, content, or operational updates.
- Supporting the resolution of invoice or contractual queries.
- Recording material complaints, service issues, and disputes.
- Escalating technical matters to Babylon Gaming.
- Monitoring completion of agreed actions.
- Identifying opportunities for appropriate commercial development.
- Supporting periodic and event-driven reviews of the relationship.

4.7.3 Identification of Material Changes

Account Management must inform Compliance promptly where it becomes aware of:

- A change in the business partner's ownership or control.
- A change in Directors or key management.
- A suspension, expiry, restriction, or revocation of a licence.
- Entry into a new or higher-risk market.
- Further distribution through an undisclosed reseller or downstream client.
- A material change to the partner's business model.
- Adverse media, enforcement action, or regulatory warning.
- Use of gaming content in an unauthorised territory.
- Unusual or unexplained changes in gaming or payment activity.
- A refusal or repeated failure to provide requested information.
- Any conduct that may create a regulatory, legal, financial, or reputational risk.

Account Management must not independently determine that such information is immaterial where it may affect the partner's approval or risk classification.

4.7.4 Integration and Activation Coordination

Account Management coordinates the commercial and operational aspects of business-partner integration by:

- Confirming that required internal approvals have been completed.

- Confirming that the relevant agreement has been executed.
- Coordinating information and documentation required by Babylon Gaming.
- Communicating integration instructions and operational requirements.
- Monitoring the status of the integration.

Prospective Business-Partner Onboarding and Integration Workflow

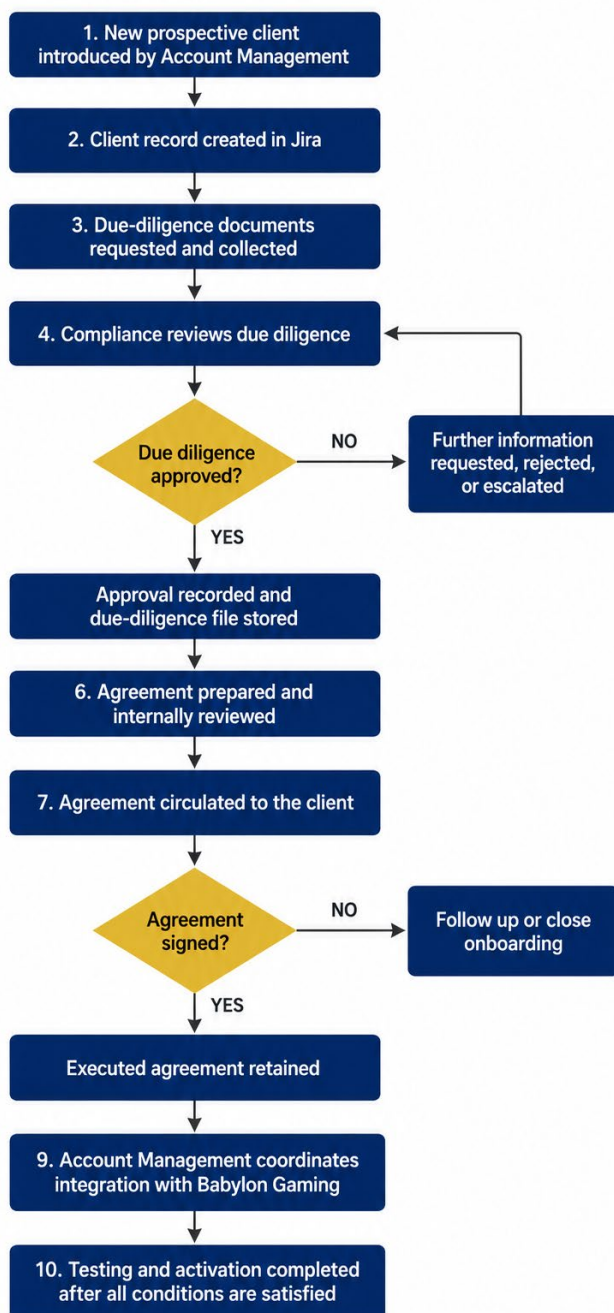


Figure 4.1 – Prospective Business-Partner Onboarding and Integration Workflow

- Coordinating testing or activation communications between the relevant parties.

- Confirming that outstanding compliance or contractual conditions have been addressed.

- Maintaining records of significant integration milestones.

- Escalating delays, errors, or technical issues to the responsible party.

Account Management does not independently modify the underlying game technology, supplier platform, or integration infrastructure.

4.7.5 Technical and Service Issues

When a business partner reports a technical or content-related issue, Account Management is responsible for:

- Recording the issue and the time it was reported.
- Obtaining sufficient information to understand its nature and impact.
- Determining whether the issue can be addressed through approved guidance.
- Referring technical matters to Babylon Gaming or the relevant service provider.
- Monitoring the status of the escalation.
- Providing appropriate updates to the affected business partner.
- Escalating prolonged or material incidents internally.
- Retaining records of significant communications and resolutions.

Account Management must not provide unsupported technical explanations or make commitments concerning resolution times unless these have been confirmed by the responsible provider.

4.8 External Advisers and Service Providers

Bet Play B.V. may appoint external parties to provide specialist or supporting services, including:

- Legal advice.
- Regulatory and compliance support.
- Accounting and tax services.
- External audit.
- Corporate administration.
- Information-security advice.
- Data-protection advice.
- Training.
- Technical or integration support.
- Business-continuity support.

External providers are responsible for performing the services defined in their agreements competently, securely, and within the agreed scope.

The appointed internal owner of each material relationship is responsible for:

- Confirming the scope of the service.
- Providing only the information necessary for the assignment.
- Monitoring delivery and performance.
- Reviewing material outputs or recommendations.
- Escalating service failures or conflicts of interest.
- Ensuring that confidentiality and data-protection obligations are observed.
- Maintaining relevant agreements, reports, and correspondence.
- Periodically assessing whether the arrangement remains appropriate.

The use of an external adviser does not transfer the Director's or relevant officer's responsibility for the final decision.

4.9 Relationship with Babylon Gaming

Babylon Gaming is the Company's principal upstream distribution partner and provides the commercial and technical route through which Bet Play B.V. obtains access to the relevant gaming content.

Bet Play B.V. is responsible for managing and overseeing this relationship from a commercial, operational, contractual, and regulatory perspective.

4.9.1 Responsibilities of Bet Play B.V.

The Company's responsibilities include:

- Maintaining an appropriate written agreement with Babylon Gaming.
- Understanding the scope and limitations of the services provided.
- Complying with applicable content, market, and distribution restrictions.
- Providing accurate information concerning proposed business partners.
- Coordinating approved client onboarding and activation.
- Monitoring material service issues and incidents.
- Escalating business-partner reports to Babylon Gaming where necessary.
- Reviewing invoices, statements, or activity reports received through the arrangement.
- Monitoring material changes affecting the service.
- Retaining significant contractual and operational records.
- Assessing the regulatory impact of material failures or changes.

4.9.2 Responsibilities of Babylon Gaming and Upstream Providers

Subject to the applicable agreements, Babylon Gaming and the relevant upstream providers are responsible for matters such as:

- Providing access to the available gaming content.
- Maintaining the relevant supplier-side delivery arrangements.
- Communicating technical and integration requirements.
- Supporting technical activation.
- Investigating underlying game, platform, or content-delivery issues.
- Communicating material service or content changes.
- Applying provider-controlled territorial or content restrictions.
- Maintaining the technology falling within their respective control.

The precise allocation of responsibilities is governed by the applicable agreements and must not be inferred solely from this Manual.

4.9.3 Escalation of Supplier Matters

The following matters must be escalated to the Director and other relevant officers:

- A significant or prolonged service interruption.
- A material breach of contract.
- A material change to the available content or services.
- An unauthorised distribution concern.
- A data-protection or information-security incident.
- A regulatory inquiry relating to the distribution arrangement.
- A significant invoice or reconciliation dispute.
- A matter affecting the Company's ability to meet its obligations.
- A proposed termination or material amendment of the relationship.

4.10 Separation of Responsibilities and Checks

The Company applies proportionate separation of responsibilities to reduce the risk of error, unauthorised activity, and conflicts of interest.

Where operationally practicable:

- Account Management initiates and coordinates commercial relationships.

- Compliance conducts or coordinates due diligence and provides compliance approval or recommendations.
- The Director approves material relationships and contractual commitments.
- Finance verifies invoicing, receipts, and payments.
- Technical matters are referred to Babylon Gaming or the responsible provider.
- The MLRO independently assesses suspicious-activity reports.

A person must not use one responsibility to bypass the controls associated with another function.

Because the Company maintains a streamlined structure, complete segregation may not always be practicable. In such cases, compensating controls may include:

- Secondary review by the Director.
- Written approval by another authorised officer.
- Independent review by an external adviser.
- Periodic retrospective checks.
- Documented reconciliations.
- Enhanced recordkeeping.
- Restricted access rights.
- Clear financial approval thresholds.

Any material limitation in segregation of duties must be assessed and addressed proportionately.

4.1 1 Responsibility and Approval Matrix

The following matrix summarises the principal allocation of responsibilities. It must be adapted if the Company’s actual appointments or delegated authorities change.

Activity	Account Management	Compliance Officer / MLRO	CFO	Director
Initial commercial inquiry	Lead	Informed where relevant	—	Informed where material

Collection of onboarding information	Coordinate	Review	—	—
Business-partner due diligence	Support	Lead	Support on financial matters	Oversight
Risk classification	Provide information	Lead	Consulted where relevant	Approve material or high-risk cases
Commercial terms	Prepare and coordinate	Review regulatory implications	Review financial implications	Approve material terms
Contract approval	Coordinate	Compliance review	Financial review	Final approval
Client activation	Coordinate	Confirm compliance clearance	Confirm financial setup where required	Approve material relationships
Integration coordination	Lead	Monitor regulatory conditions	—	Oversight
Technical issue escalation	Lead	Informed if material	—	Informed if material
Client invoicing	Support validation	—	Lead	Oversight
Receipt and payment reconciliation	Support queries	Review unusual matters	Lead	Oversight
Regulatory reporting	Provide information	Prepare or coordinate	Provide financial information	Approve where required

Suspicious-activity assessment	Report concerns	MLRO decision	Report concerns	Informed only where legally permissible
Supplier oversight	Support operational monitoring	Compliance monitoring	Financial monitoring	Overall oversight
Material incident response	Coordinate client communication	Assess regulatory impact	Assess financial impact	Direct and approve response
Suspension or termination	Provide commercial information	Recommend where compliance-related	Assess financial implications	Final approval
Policy and Manual approval	Consulted	Prepare and review	Review relevant sections	Final approval

A dash indicates that the function does not ordinarily lead the activity but may still be consulted where relevant.

4.12 Authority Limitations

No officer, employee, contractor, or other person acting for Bet Play B.V. may, without appropriate authority:

- Approve a business partner that has not completed required due diligence.
- Override a compliance or MLRO decision.
- Commit the Company to material contractual obligations.
- Agree to distribute gaming content in an unauthorised or restricted jurisdiction.
- Modify standard contractual terms materially.
- Open, close, or change control over a Company bank account.
- Approve a payment outside their delegated limit.
- Change payment details without the required verification.
- Make a regulatory submission on behalf of the Company unless authorised.

- Represent that the Company owns, develops, hosts, or controls the underlying games.
- Guarantee content availability, technical performance, or resolution times without confirmation.
- Disclose confidential or personal information without a lawful basis and appropriate authority.
- Engage a material external service provider without approval.
- Suspend or terminate a material relationship without the required decision.

Where a person is uncertain whether they have authority, the matter must be referred to the Director or relevant function owner before action is taken.

4.1.3 Reporting and Escalation Responsibilities

All personnel are responsible for escalating matters that exceed their authority, competence, or ordinary responsibilities.

Immediate Escalation

Immediate escalation is required where a matter involves:

- A suspected breach of legislation or a licence condition.
- A formal communication from the CGA.
- Suspected money laundering, fraud, sanctions exposure, or other financial crime.
- An unauthorised distribution or prohibited-jurisdiction concern.
- A material information-security or personal-data incident.
- A significant or prolonged interruption of services.
- A material contractual dispute or supplier failure.
- A significant financial irregularity.
- A threat to the Company's liquidity or continued operations.
- A legal claim, enforcement action, or material reputational issue.

Routine Escalation

Routine operational matters should be reported through the normal reporting line and recorded in the relevant system, register, correspondence file, or management report.

The person receiving an escalation is responsible for:

- Acknowledging and assessing the matter.
- Determining its seriousness and potential impact.
- Involving the appropriate functions.
- Assigning responsibility for follow-up.
- Establishing required actions and timeframes.
- Determining whether external notification is required.
- Ensuring that the matter and its resolution are documented.

4.14 Competence and Suitability

Persons appointed to management, compliance, AML/CFT/CPF, financial, or other material functions must possess competence and experience proportionate to their responsibilities.

The Company should consider:

- Relevant professional experience.
- Knowledge of the gaming industry.
- Understanding of applicable regulatory requirements.
- Qualifications or professional certifications.
- Integrity and professional reputation.
- Ability to exercise independent judgement.
- Capacity and availability to perform the role.
- Conflicts of interest.
- Any regulatory approval or suitability requirement.
- Ongoing training and professional development needs.

Appointment records should include sufficient information to demonstrate why the person was considered suitable for the role.

Where an appointed person requires additional knowledge in a particular area, the Company may provide training, obtain external advice, or implement additional oversight.

4.15 Induction and Ongoing Training

Personnel must receive induction and ongoing training appropriate to their roles.

Training may cover:

- The Company's business model and licence scope.

- The Operational Manual and relevant internal policies.
- Business-partner onboarding and due diligence.
- AML/CFT/CPF and sanctions awareness.
- Regulatory reporting and breach escalation.
- Conflicts of interest.
- Information security and data protection.
- Incident reporting and business continuity.
- Financial controls and fraud prevention.
- Contractual and jurisdictional restrictions.
- Recordkeeping and confidentiality.
- Changes to applicable legislation or CGA requirements.

Role-specific training should be provided where a person has responsibilities requiring specialist knowledge.

Training records must identify:

- The participant.
- The subject of the training.
- The date completed.
- The training provider or source.
- Any assessment undertaken.
- Any follow-up training required.

4.16 Performance and Effectiveness Review

The Director must periodically consider whether the Company's officers and functions are performing their responsibilities effectively.

The review may consider:

- Completion of assigned responsibilities.
- Accuracy and timeliness of work.
- Quality of reporting and recordkeeping.
- Compliance with internal policies and authority limits.
- Effectiveness of escalation.
- Completion of required training.
- Audit, monitoring, or regulatory findings.
- Workload and available resources.

- Conflicts of interest or independence concerns.
- The need for additional personnel, expertise, or support.

Material performance or resource deficiencies must be documented and addressed through training, revised procedures, additional supervision, reassignment of responsibilities, external support, or appointment of additional personnel.

4.17 Role Descriptions and Appointment Records

The Company must maintain current role descriptions for its material functions.

Each role description should identify:

- The title of the position or function.
- The principal responsibilities.
- The reporting line.
- The scope of decision-making authority.
- Reserved or prohibited activities.
- Required competence and experience.
- Regulatory approval or notification requirements.
- Escalation obligations.
- Temporary absence arrangements.
- Any additional responsibilities arising from another role.

Appointment records should include, where applicable:

- The appointment date.
- Evidence of approval.
- Curriculum vitae and qualifications.
- Suitability or due-diligence documentation.
- Regulatory approval or notification records.
- Employment, consultancy, or service agreement.
- Conflict-of-interest declaration.
- Training and continuing-development records.
- Records of resignation, removal, or replacement.

4.18 Review of Roles and Responsibilities

The Director and Compliance Officer must review the allocation of roles and responsibilities at least annually and whenever a material change occurs.

A review must also be considered following:

- Appointment, departure, or prolonged absence of a key officer.
- Material growth in the number of business partners.
- Expansion into new markets or services.
- A change in the relationship with Babylon Gaming.
- A material regulatory amendment.
- An audit or regulatory finding.
- A significant operational, compliance, financial, or security incident.
- Identification of an actual or potential conflict of interest.
- Evidence that a function lacks sufficient capacity, authority, or competence.
- Introduction of proprietary technology or materially expanded technical responsibilities.

Any resulting change must be documented and reflected, where relevant, in:

- The organisational chart.
- Role descriptions.
- Delegated authorities.
- Internal policies and procedures.
- Regulatory records and notifications.
- This Operational Manual.

The Company must ensure that its documented allocation of responsibilities continues to reflect its actual operating arrangements.

Business Risk Management Framework

5

Chapter 5 – Business Risk Management Framework

5.1 Purpose

This chapter establishes the framework used by Bet Play B.V. to identify, assess, manage, monitor, and report risks arising from its licensed B2B gaming-supplier activities.

The framework is intended to ensure that:

- Material risks are identified before decisions are made.
- Risk is considered consistently across the Company.
- Controls are proportionate to the likelihood and potential impact of each risk.
- Responsibilities for managing risks are clearly allocated.
- Material risks and control weaknesses are escalated promptly.
- Commercial objectives remain consistent with the Company's licence, contractual rights, risk appetite, and operational capacity.
- The Company maintains effective oversight of risks associated with Babylon Gaming and other external service providers.
- Risk assessments and management decisions are properly documented.
- Emerging risks and material changes are identified and addressed.

This chapter covers the Company's general business, regulatory, operational, financial, technological, third-party, and reputational risks.

Detailed financial-crime risk requirements are governed by the Company's separate AML/CFT Policy. Where an identified risk involves money laundering, terrorist financing, proliferation financing, sanctions, fraud, or suspicious activity, the matter must also be addressed under that policy and referred to the MLRO where appropriate.

5.2 Scope

The risk-management framework applies to:

- The Director.
- The Compliance Officer.

- The MLRO.
- The CFO.
- Account Management.
- Employees and contractors acting for the Company.
- Material external advisers and service providers.
- Prospective and existing business-partner relationships.
- The Company's relationship with Babylon Gaming.
- Proposed products, content, services, markets, and distribution arrangements.
- Financial, contractual, regulatory, and operational decisions.
- Material changes, incidents, complaints, breaches, and control weaknesses.

Risk management is an ongoing responsibility and is not limited to the completion of a formal annual assessment.

5.3 Risk-Management Principles

Bet Play B.V. applies the following principles:

5.3.1 Risk-Based Approach

The nature and extent of controls must be proportionate to the risk presented. Relationships or activities presenting higher risk require greater scrutiny, stronger controls, more senior approval, and more frequent monitoring.

5.3.2 Accountability

Each material risk must have an identifiable owner responsible for ensuring that it is assessed, controlled, monitored, and escalated appropriately.

5.3.3 Proportionality

The Company's risk arrangements must reflect the scale, nature, complexity, and actual responsibilities of its operations.

The Company must not represent that it performs technical, hosting, game-development, or monitoring controls where these are performed by Babylon Gaming or another upstream provider. However, it must understand the allocation of responsibility and maintain appropriate oversight of material outsourced or supplier-controlled risks.

5.3.4 Evidence-Based Decisions

Risk decisions must be based on sufficiently reliable information. Where material information is missing, inconsistent, outdated, or unverifiable, the matter must not be treated as low risk solely because no adverse information has been identified.

5.3.5 Prevention and Early Escalation

Risks should be addressed at the earliest reasonable stage. Personnel must escalate matters before committing the Company to a relationship, market, payment, contract, or activity that may exceed its risk appetite or authority.

5.3.6 Documentation

Material assessments, decisions, conditions, exceptions, incidents, and remedial actions must be documented sufficiently to demonstrate:

- What was assessed.
- What information was considered.
- Who conducted and approved the assessment.
- The identified risks and controls.
- The resulting risk rating.
- Any conditions or limitations imposed.
- The date of the decision.
- The required review or follow-up date.

5.3.7 Continuous Review

Risk assessments must be reviewed when relevant circumstances change. Approval at onboarding does not establish that a relationship or activity remains acceptable indefinitely.

5.4 Governance and Responsibilities

5.4.1 Director

The Director has ultimate responsibility for the Company's risk-management framework.

The Director is responsible for:

- Approving the Company's risk appetite.
- Ensuring that appropriate risk-management arrangements are maintained.
- Reviewing material and high-risk matters.

- Approving material risk acceptance and exceptions.
- Ensuring that sufficient resources are available to manage identified risks.
- Reviewing significant incidents, breaches, and control weaknesses.
- Approving material remedial measures.
- Ensuring that regulatory notifications are made where required.
- Determining whether a material relationship or activity should be restricted, suspended, or terminated.

5.4.2 Compliance Officer

The Compliance Officer coordinates the Company's general regulatory and compliance-risk framework and is responsible for:

- Identifying material regulatory and licensing risks.
- Supporting or conducting formal risk assessments.
- Reviewing compliance risks associated with prospective business partners.
- Assessing proposed markets, products, services, and distribution arrangements.
- Monitoring regulatory developments.
- Maintaining relevant risk and compliance records.
- Monitoring the implementation of agreed controls.
- Escalating material risks and control weaknesses to the Director.
- Recommending restrictions, conditions, corrective actions, suspension, or termination.

5.4.3 MLRO

The MLRO is responsible for risks relating to:

- Money laundering.
- Terrorist financing.
- Proliferation financing.
- Sanctions.
- Suspicious transactions or business activity.
- Financial-crime indicators involving business partners and counterparties.

The MLRO applies the methodology and controls established in the Company's AML/CFT Policy. Confidential suspicious-activity assessments must not be entered

into a general risk register where this would compromise applicable confidentiality requirements.

5.4.4 Chief Financial Officer

The CFO is responsible for identifying and monitoring financial risks, including:

- Liquidity and cash-flow risk.
- Revenue concentration.
- Credit and receivables risk.
- Invoice and reconciliation discrepancies.
- Payment and banking risks.
- Tax, accounting, and audit risks.
- Unusual or unauthorised financial activity.
- Financial exposure arising from contractual arrangements.

5.4.5 Account Management

Account Management is responsible for identifying and reporting risks arising during the prospective and ongoing business-partner relationship.

Account Management must:

- Obtain accurate information concerning the proposed relationship.
- Identify intended markets and distribution arrangements.
- Report material changes concerning the business partner.
- Avoid making commitments before the required approvals are obtained.
- Monitor operational and commercial issues affecting assigned accounts.
- Escalate complaints, contractual breaches, unauthorised distribution, service issues, adverse information, and unexplained changes.
- Support implementation of risk conditions imposed by Compliance or the Director.

5.4.6 All Personnel

Every person acting for the Company is responsible for:

- Remaining alert to risks within their activities.
- Complying with established controls.
- Reporting incidents, errors, breaches, and control weaknesses.
- Escalating matters outside their authority or competence.
- Providing complete and accurate information for risk assessments.
- Cooperating with reviews and remedial actions.

5.5 Risk Appetite

The Company's risk appetite defines the nature and level of risk it is prepared to accept in pursuit of its legitimate business objectives.

Bet Play B.V. maintains no appetite for:

- Deliberate or knowing breaches of legislation or licence conditions.
- Distribution of gaming content outside the Company's contractual or regulatory authority.
- Business relationships involving unidentified or unverifiable ownership.
- Relationships involving prohibited persons, entities, or jurisdictions.
- Circumvention of sanctions or regulatory restrictions.
- Unauthorised onward distribution of gaming content.
- Misrepresentation to the CGA, banks, auditors, suppliers, or business partners.
- Concealment of material incidents or regulatory matters.
- Use of Company relationships for money laundering, terrorist financing, proliferation financing, fraud, or other unlawful activity.
- Improper interference with the Compliance Officer or MLRO.
- Activation of a partner before required due diligence, contractual, and internal approvals are completed.
- Use of third-party payment arrangements without adequate explanation, verification, and approval.
- Material compromises to the confidentiality, integrity, or availability of Company information.

The Company may accept a controlled degree of commercial, operational, financial, supplier, and technological risk where:

- The activity is lawful and within the scope of the licence.
- The risk is understood and documented.
- Appropriate controls are implemented.
- Responsibility for the risk is assigned.
- Any necessary senior approval is obtained.
- The residual risk is consistent with the Company's risk appetite.

A risk outside the Company's approved appetite must be avoided, reduced, transferred, or submitted to the Director for a formally documented decision. A risk must not be accepted where doing so would result in unlawful activity or breach a licence condition.

5.6 Principal Risk Categories

5.6.1 Strategic and Business Risk

Strategic and business risks may arise from:

- An unsuitable or unsustainable business model.
- Excessive reliance on a single supplier, partner, market, or revenue source.
- Expansion exceeding the Company's resources or operational capacity.
- Material changes in market conditions.
- Failure to adapt to regulatory or industry developments.
- Inadequate management information.
- Entry into activities outside the Company's approved licence scope.
- Commercial commitments that cannot be supported operationally.

5.6.2 Regulatory and Licensing Risk

Regulatory and licensing risks include:

- Breach of applicable legislation or CGA requirements.
- Operation outside the scope of the B2B supplier licence.
- Failure to make a required notification or submission.
- Inaccurate or incomplete regulatory information.
- Failure to implement regulatory amendments.
- Use of content in an unauthorised or restricted jurisdiction.
- Relationships with inadequately licensed or unsuitable business partners.
- Failure to retain records required for regulatory review.
- Material changes to the Company's operations without appropriate assessment or approval.

5.6.3 Business-Partner Risk

Business-partner risk may arise from:

- Unclear, complex, or opaque ownership.
- Unverified beneficial owners or controllers.
- Inadequate licensing or regulatory status.
- Operation in prohibited or higher-risk jurisdictions.
- Adverse media or regulatory enforcement.
- Financial instability.
- Inaccurate or misleading information.
- Undisclosed resellers or downstream distribution.

- Unauthorised use of the Company's content.
- Refusal or failure to cooperate with ongoing due diligence.
- Unusual payments or third-party settlement arrangements.
- A business model inconsistent with the Company's licence or contractual authority.

The assessment and approval of business partners must be conducted in accordance with Chapter 7 and the Company's AML/CFT Policy.

5.6.4 Product and Distribution Risk

Product and distribution risks include:

- Distribution of content not covered by the applicable agreement.
- Content being made available in an unauthorised market.
- Incorrect classification or description of gaming content.
- Failure to communicate provider restrictions.
- Activation before applicable approvals are completed.
- Undisclosed onward distribution.
- Inaccurate representations regarding ownership, hosting, development, testing, or control of games.
- Dependence on supplier information that is incomplete or outdated.
- Failure to assess a material change to the product or distribution model.

5.6.5 Third-Party and Supplier Risk

Third-party risk arises where the Company depends on Babylon Gaming or another provider for a material service or control.

Relevant risks include:

- Service interruption or failure.
- Inadequate performance.
- Loss of access to gaming content.
- Contractual breach.
- Inadequate incident reporting.
- Material changes to content availability or delivery arrangements.
- Information-security or data-protection incidents.
- Financial failure of a material provider.
- Loss of a required licence, certification, or authorisation.
- Inadequate business-continuity arrangements.
- Concentration of critical services with a single provider.

- Insufficient regulatory access, information, or audit rights.

Bet Play B.V. must not assume that outsourcing or reliance on a supplier transfers its regulatory responsibility.

5.6.6 Operational Risk

Operational risks may arise from:

- Inadequate or unclear procedures.
- Human error.
- Insufficient staffing or competence.
- Failure to escalate a material issue.
- Incomplete or inaccurate records.
- Unauthorised activity.
- Inadequate separation of responsibilities.
- Failure of internal communication.
- Dependency on a key person.
- Missed deadlines or contractual obligations.
- Weaknesses in onboarding, invoicing, reconciliation, or incident management.
- Failure to implement or evidence an agreed control.

5.6.7 Financial Risk

Financial risks include:

- Insufficient liquidity or working capital.
- Excessive concentration of revenue.
- Late or uncollectable receivables.
- Inaccurate invoicing.
- Reconciliation discrepancies.
- Unauthorised or duplicate payments.
- Changes to payment instructions or banking details.
- Fraud or attempted fraud.
- Tax or accounting failures.
- Unusual third-party payment arrangements.
- Currency or settlement risk.
- Disputes with business partners or suppliers.
- Financial exposure arising from termination of a material relationship.

5.6.8 Information-Security and Data-Protection Risk

These risks include:

- Unauthorised access to Company systems or records.
- Loss, alteration, or unauthorised disclosure of information.
- Phishing, malware, social engineering, or credential compromise.
- Excessive or inappropriate access rights.
- Inadequate security controls at a service provider.
- Loss or theft of equipment.
- Insufficient backup or recovery arrangements.
- Personal-data processing without an appropriate basis.
- Failure to respond appropriately to a security or personal-data incident.
- Failure to retain or delete records in accordance with applicable requirements.

The Company's detailed information-security and data-protection arrangements are addressed in Chapter 9.

5.6.9 Business-Continuity Risk

Business-continuity risks include:

- Prolonged loss of a material service.
- Unavailability of Babylon Gaming or another critical provider.
- Loss of access to key records or communications.
- Absence of a critical officer or employee.
- Cybersecurity incidents.
- Natural disasters or infrastructure failures.
- Inability to communicate with business partners.
- Failure of banking or financial services.
- Regulatory action affecting continued operations.
- Insufficient recovery arrangements.

Detailed incident-management and business-continuity arrangements are addressed in Chapter 10.

5.6.10 Legal and Contractual Risk

Legal and contractual risks include:

- Agreements that do not reflect the actual operating model.
- Unclear allocation of responsibilities.

- Commitments exceeding the Company's authority or operational capability.
- Inadequate termination, audit, confidentiality, or data-protection provisions.
- Conflicts between upstream and downstream obligations.
- Failure to comply with market or content restrictions.
- Use of unapproved contractual amendments.
- Unresolved disputes or breaches.
- Failure to retain executed agreements and supporting records.

5.6.11 Reputational Risk

Reputational risk may arise from:

- Association with unsuitable business partners.
- Regulatory enforcement or public criticism.
- Misleading commercial representations.
- Poor handling of complaints or incidents.
- Unauthorised distribution of content.
- Material supplier failures.
- Data breaches or security incidents.
- Financial disputes or unpaid obligations.
- Unethical behaviour by Directors, officers, personnel, or representatives.
- Failure to respond transparently and appropriately to a material issue.

5.6.12 AML/CFT/CPF and Sanctions Risk

The Company's exposure to money laundering, terrorist financing, proliferation financing, and sanctions risk arises principally through:

- The identity and ownership of business partners.
- The source and destination of commercial payments.
- Target and operating jurisdictions.
- Unusual or unexplained business structures.
- Third-party payments.
- Adverse media or regulatory findings.
- Attempts to disguise the identity or activities of a counterparty.
- Use of the distribution relationship for unlawful purposes.

These risks must be assessed and managed under the Company's AML/CFT Policy and referred to the MLRO where appropriate.

5.7 Risk-Identification Process

Risks may be identified through:

- Business-wide risk assessments.
- Business-partner onboarding and reviews.
- Proposed new products, services, or markets.
- Contract and supplier reviews.
- Compliance monitoring.
- Financial reconciliations.
- Management reporting.
- Internal or external audits.
- Regulatory communications.
- Complaints, disputes, and legal claims.
- Operational or security incidents.
- Employee or contractor reports.
- Adverse media and sanctions screening.
- Changes to legislation or licence conditions.
- Changes in ownership, control, personnel, technology, or service providers.
- Business-continuity exercises.
- Analysis of previous errors, failures, or near misses.

A person identifying a risk must provide sufficient information to allow the responsible owner to assess it.

5.8 Risk-Assessment Methodology

The Company assesses risk by considering:

1. The likelihood that the risk will occur.
2. The potential impact if it occurs.
3. The controls currently in place.
4. The effectiveness of those controls.
5. The remaining or residual risk.
6. Whether further action or senior approval is required.

Assessments must distinguish between:

- Inherent risk: the level of risk before considering controls.

- Control effectiveness: the extent to which existing controls reduce the risk.
- Residual risk: the level of risk remaining after controls are applied.

5.8.1 Likelihood Scale

Rating	Classification	General description
1	Rare	The event is exceptional and is not reasonably expected under ordinary circumstances.
2	Unlikely	The event could occur but is not expected to arise frequently.
3	Possible	The event may occur in some circumstances or has occurred occasionally.
4	Likely	The event is expected to occur or has occurred repeatedly.
5	Almost Certain	The event is occurring, is imminent, or is expected to occur frequently.

5.8.2 Impact Scale

Rating	Classification	General description
1	Insignificant	Limited effect, readily corrected, with no material regulatory, financial, operational, or reputational consequence.
2	Minor	Localised disruption or weakness requiring routine management action.
3	Moderate	Material operational, financial, contractual, or compliance consequence requiring management involvement.
4	Major	Serious breach, loss, disruption, regulatory concern, or reputational damage requiring immediate senior action.
5	Severe	Potential threat to the licence, financial viability, continued operations, or regulatory standing of the Company.

When determining impact, the assessor should consider:

- Regulatory and licensing consequences.
- Financial loss or liability.
- Operational interruption.
- Harm to business partners or other affected parties.
- Contractual consequences.
- Information-security and data-protection effects.
- Reputational damage.
- Duration and reversibility.
- Whether the matter could affect the Company's continued operations.

5.8.3 Risk Score

The risk score is calculated as:

Risk score = Likelihood × Impact

Score	Risk level	Required response
1–4	Low	Manage through routine controls and periodic monitoring.
5–9	Moderate	Assign an owner and implement proportionate controls; monitor regularly.
10–16	High	Prompt management attention, documented treatment plan, and Director oversight required.
17–25	Critical	Immediate escalation; activity must not commence or continue without lawful resolution and formal Director decision.

A numerical score supports consistency but does not replace professional judgement. A matter may be assigned a higher classification where its regulatory, financial-crime, licensing, or reputational significance warrants this.

5.9 Risk Evaluation and Treatment

After a risk has been assessed, the Company must determine the appropriate response.

Available treatments include:

5.9.1 Avoid

The Company may decide not to begin or continue the activity where the risk is unlawful, prohibited, outside the Company's appetite, or cannot be controlled adequately.

5.9.2 Reduce

The Company may implement additional controls to reduce the likelihood or impact of the risk.

These may include:

- Obtaining additional information.
- Conducting enhanced due diligence.
- Imposing contractual restrictions.
- Limiting markets, content, services, or access.
- Requiring senior approval.
- Increasing monitoring frequency.
- Requiring additional reporting.
- Introducing secondary review or reconciliation.
- Obtaining external legal, technical, compliance, or financial advice.
- Providing additional training.
- Improving documentation or access controls.
- Establishing incident or continuity measures.

5.9.3 Transfer or Share

Where appropriate, the Company may transfer or share elements of risk through:

- Contractual allocation.
- Insurance.
- Indemnities.
- Specialist external providers.
- Alternative service arrangements.

Transfer of risk does not remove the Company's regulatory responsibility or its obligation to oversee the arrangement.

5.9.4 Accept

A residual risk may be accepted where:

- The activity is lawful.
- The risk has been adequately assessed.

- Available controls are proportionate.
- The remaining exposure falls within the Company's risk appetite.
- The person accepting the risk has the necessary authority.
- The decision and rationale are documented.
- Monitoring and review arrangements are established.

5.10 Risk Acceptance and Exceptions

An exception arises where the Company proposes to depart from an established control, policy, procedure, standard term, or risk limit.

A request for an exception must state:

- The requirement from which departure is proposed.
- The reason for the exception.
- The period for which it is required.
- The risks created by the exception.
- The proposed compensating controls.
- The responsible owner.
- The required approval.
- The date by which the exception will be reviewed or closed.

Compliance requirements imposed by law, regulation, licence condition, or a competent authority cannot be waived through internal risk acceptance.

High or critical residual risks and material policy exceptions require the Director's written approval following consultation with the Compliance Officer and other relevant functions.

Where the matter concerns AML/CFT/CPF, sanctions, or suspicious activity, the MLRO must be involved and the separate requirements of the AML/CFT Policy must be followed.

5.11 Risk Register

The Company must maintain a central risk register proportionate to the nature and complexity of its activities.

The risk register should include:

- A unique reference number.

- The date the risk was identified.
- The risk category.
- A clear description of the risk.
- The potential causes and consequences.
- The inherent likelihood and impact.
- The existing controls.
- An assessment of control effectiveness.
- The residual likelihood and impact.
- The resulting risk classification.
- The risk owner.
- Required additional actions.
- Responsible persons.
- Target completion dates.
- Current status.
- The date and outcome of the most recent review.
- The next review date.
- Relevant approvals or escalation records.

Sensitive AML/CFT/CPF or suspicious-activity information must be maintained separately where necessary to preserve confidentiality.

5.12 Risk-Assessment Triggers

A formal or documented risk assessment must be considered before:

- Approving a new business partner.
- Entering a new jurisdiction or market.
- Introducing a material new product, service, or distribution model.
- Appointing or replacing a material service provider.
- Entering or materially amending a significant contract.
- Accepting a material departure from standard contractual terms.

- Activating a reseller or onward-distribution arrangement.
- Introducing a significant change to technology or information processing.
- Changing a material payment or settlement arrangement.
- Accepting a material risk exception.
- Making a significant change to the Company's business model.
- Resuming a relationship following suspension.
- Undertaking an activity that may affect the scope of the Company's licence.

A reassessment must also be conducted following a material incident, breach, audit finding, regulatory development, or change in relevant circumstances.

5.13 New Product, Service, Market and Change Risk Assessment

Before approving a material change, the responsible person must provide sufficient information concerning:

- The nature and purpose of the proposal.
- The parties involved.
- The proposed markets and jurisdictions.
- The intended clients and distribution arrangements.
- The applicable contractual rights and restrictions.
- The regulatory and licensing implications.
- The role of Babylon Gaming or another supplier.
- The financial model and expected exposure.
- Information-security and data-protection implications.
- Operational resources and competence required.
- Business-continuity implications.
- AML/CFT/CPF and sanctions considerations.
- The controls required before implementation.

The Compliance Officer must review the regulatory implications. The CFO must review material financial implications. The Director must approve material changes.

Implementation conditions must be documented and confirmed as completed before launch or activation.

5.14 Business-Partner Risk Assessment

Each prospective business partner must undergo a documented risk assessment before approval.

The assessment must consider, where relevant:

- Legal identity and registration.
- Ownership and control.
- Ultimate beneficial owners.
- Directors and key persons.
- Licensing and regulatory status.
- Nature of the business and proposed relationship.
- Target and operating markets.
- Distribution channels.
- Use of resellers or downstream clients.
- Reputation and adverse media.
- Regulatory or enforcement history.
- Sanctions and PEP exposure.
- Financial standing.
- Payment arrangements.
- Source and destination of funds where relevant.
- Expected activity and revenue.
- Quality and completeness of information provided.
- Compatibility with Babylon Gaming's requirements.
- Contractual and content restrictions.
- Any identified AML/CFT/CPF concerns.

The Company's AML/CFT Policy provides the detailed methodology for assigning the applicable financial-crime and business-partner risk classification.

A partner must not be activated until:

- Required due diligence has been completed.
- Material risks have been assessed.
- Compliance clearance has been recorded.
- The necessary management approval has been obtained.
- The applicable agreement has been executed.
- Required supplier or upstream-provider conditions have been satisfied.
- Any conditions imposed on the approval have been implemented.

5.15 Third-Party and Supplier Risk Management

Before appointing or materially relying on a third party, the Company should assess:

- The service to be provided.
- The importance and criticality of the service.
- The provider's identity, ownership, competence, and reputation.
- Applicable licences, certifications, or professional qualifications.
- Financial and operational stability.
- Information-security and data-protection arrangements.
- Business-continuity and recovery arrangements.
- Use of subcontractors.
- Contractual service levels.
- Incident and breach-notification obligations.
- Regulatory access and audit rights.
- Termination and transition arrangements.
- Conflicts of interest.
- Concentration and dependency risks.

Each material provider must have an internal relationship owner.

Material providers must be reviewed periodically and when:

- A serious service failure occurs.
- A material incident or breach is reported.
- Ownership or control changes.
- A relevant licence or certification changes.
- Material adverse information arises.
- The scope of the service changes.
- Contract renewal or material amendment is proposed.
- There is evidence that the provider may no longer meet the Company's requirements.

5.16 Concentration and Dependency Risk

The Company recognises that dependence on Babylon Gaming creates concentration risk because access to gaming content and related integration support is materially dependent on that relationship.

The Company must therefore:

- Maintain a current written agreement with Babylon Gaming.
- Understand the scope and limitations of the services provided.

- Identify critical points of dependency.
- Maintain appropriate contact and escalation arrangements.
- Monitor material service issues and contractual changes.
- Consider the impact of prolonged unavailability or termination.
- Retain sufficient records to manage the relationship.
- Assess whether contingency, transition, or alternative arrangements are reasonably available.
- Avoid representing that it controls services or technology that remain under Babylon Gaming's or an upstream provider's control.
- Escalate any matter that may materially affect the Company's ability to meet its obligations.

Concentration risk must be reviewed as part of the Company's business-continuity and strategic-risk assessments.

5.17 Monitoring of Risks and Controls

Risk monitoring may include:

- Review of the risk register.
- Compliance monitoring.
- Business-partner periodic reviews.
- Analysis of incidents and complaints.
- Supplier-performance reviews.
- Financial and reconciliation reporting.
- Review of overdue actions.
- Audit and assurance findings.
- Regulatory horizon scanning.
- Training and competence reviews.
- Testing of business-continuity arrangements.
- Review of access rights and information-security controls.
- Management review of key dependencies.
- Verification that approval conditions remain in place.

The frequency of monitoring must reflect the risk classification, with higher-risk matters subject to more frequent review.

Monitoring must assess both:

- Whether the control has been implemented.
- Whether the control is operating effectively.

5.18 Key Risk Indicators

Where useful and proportionate, the Company may use key risk indicators to identify changes in exposure.

Indicators may include:

- Number of high-risk business partners.
- Due-diligence files overdue for review.
- Unresolved compliance conditions.
- Partners operating in or seeking access to new markets.
- Undisclosed or unauthorised onward distribution.
- Significant service interruptions.
- Repeated technical or operational complaints.
- Material supplier incidents.
- Overdue receivables.
- Reconciliation discrepancies.
- Unusual or third-party payments.
- Policy exceptions.
- Open audit findings.
- Overdue corrective actions.
- Missed regulatory deadlines.
- Information-security incidents.
- Staff-training completion.
- Dependency on individual clients, suppliers, or personnel.

A key risk indicator exceeding an established threshold must be reviewed and escalated according to its significance.

5.19 Incident and Near-Miss Reporting

A risk event includes an incident, breach, failure, error, or circumstance in which a control did not operate as intended.

A near miss is an event that could have caused a material consequence but was detected or prevented before the consequence occurred.

Personnel must report material incidents and near misses promptly. The report should identify:

- What occurred.
- When and how it was identified.
- The affected relationship, service, record, or process.

- The immediate and potential impact.
- Actions already taken.
- Persons or providers involved.
- Whether the incident is continuing.
- Whether regulatory, contractual, financial, security, or AML/CFT/CPF implications may arise.

Material incidents must be assessed to determine:

- The root cause.
- Whether immediate containment is required.
- Whether the matter must be notified externally.
- Whether affected parties must be informed.
- What corrective and preventive actions are required.
- Whether the risk register or relevant procedures must be updated.
- Whether similar risks exist elsewhere in the Company.

5.20 Escalation of Material Risks

A risk must be escalated immediately to the Director and relevant control function where it involves:

- An actual or suspected regulatory breach.
- Activity outside the scope of the Company's licence.
- A request or formal communication from the CGA.
- A critical or unacceptable residual risk.
- Suspected money laundering, terrorist financing, proliferation financing, sanctions exposure, or fraud.
- Unauthorised distribution or use of gaming content.
- A serious business-partner suitability concern.
- A material information-security or personal-data incident.
- A significant or prolonged service interruption.
- A material failure by Babylon Gaming or another critical provider.
- A material financial irregularity or liquidity concern.
- A legal claim, enforcement action, or significant contractual dispute.
- A risk to the Company's continued operations.
- A material reputational threat.
- Concealment, falsification, or obstruction affecting a risk assessment or review.

The Director, in consultation with the relevant officers, must determine:

- Whether the affected activity should be paused.
- What immediate controls or containment measures are required.
- Whether external advice is necessary.
- Whether the CGA or another authority must be notified.
- Whether a business relationship should be restricted, suspended, or terminated.
- What remedial action and follow-up reporting are required.

5.21 Corrective-Action Management

Where a risk assessment, incident, audit, or monitoring review identifies a weakness, the Company must establish a corrective-action plan proportionate to its seriousness.

The plan should include:

- The identified weakness.
- The required corrective or preventive action.
- The responsible person.
- The target completion date.
- Any temporary controls.
- The priority and risk classification.
- Required evidence of completion.
- The person responsible for verifying completion.
- Any required reporting or approval.

An action must not be treated as completed solely because it has been assigned or because a revised document has been drafted. Completion must be supported by evidence that the required control has been implemented.

Overdue high-risk actions must be escalated to the Director.

5.22 Risk Reporting

The Director must receive risk information sufficient to oversee the Company's activities.

Risk reporting may include:

- The current risk profile.
- New and emerging risks.
- High and critical risks.
- Material changes in existing risks.
- Business-partner risk developments.
- Supplier and concentration risks.
- Incidents, breaches, complaints, and near misses.
- Regulatory developments.
- Financial and liquidity risks.
- Outstanding corrective actions.
- Approved policy exceptions.
- Audit and compliance-monitoring findings.
- Matters requiring a decision or additional resources.

Urgent or material risks must be reported immediately and must not be deferred until the next scheduled management report.

5.23 Business-Wide Risk Assessment

The Company must maintain a documented business-wide risk assessment addressing the principal risks arising from its operations.

The assessment should consider:

- The Company's corporate and ownership structure.
- The nature and scope of its licensed activities.
- Its products and services.
- Business partners and counterparties.
- Target and operating jurisdictions.
- Distribution channels.
- Babylon Gaming and other material providers.
- Revenue and supplier concentration.
- Financial and payment arrangements.
- Technology and information processing.
- Personnel, competence, and key-person dependencies.
- Regulatory and legal obligations.
- AML/CFT/CPF and sanctions exposure.
- Information security and data protection.

- Business continuity.
- Previous incidents, audit findings, and control weaknesses.
- Expected changes to the business.

The business-wide risk assessment must distinguish between risks arising from activities performed directly by Bet Play B.V. and risks arising from services performed by Babylon Gaming or another provider.

It must be reviewed:

- At least annually.
- Following a material change to the business model.
- Before entering a materially different market or activity.
- Following appointment or replacement of a critical provider.
- After a serious incident or breach.
- Following a material regulatory amendment.
- Where an audit or regulatory review identifies significant weaknesses.
- Whenever management determines that the existing assessment may no longer reflect the Company's risk exposure.

The AML/CFT/CPF component may be maintained within the separate AML/CFT Policy or business risk assessment, provided the assessments remain consistent and are reviewed together where relevant.

5.24 Recordkeeping

Risk-management records may include:

- Business-wide risk assessments.
- Risk registers.
- Business-partner risk assessments.
- New-product and change assessments.
- Supplier-risk assessments.
- Risk-acceptance and exception records.
- Incident and near-miss reports.
- Corrective-action plans.
- Monitoring and testing records.
- Management risk reports.
- Meeting minutes and approval records.

- Audit reports.
- Evidence of completed remedial actions.
- Relevant regulatory correspondence.
- Training records.

Records must be:

- Accurate and complete.
- Dated and attributable to the relevant assessor and approver.
- Protected against unauthorised access or alteration.
- Accessible to authorised persons.
- Retained in accordance with applicable legal, regulatory, contractual, and internal requirements.

5.25 Training and Awareness

Personnel must receive risk-management training appropriate to their responsibilities.

Training should address, where relevant:

- The Company's principal risk categories.
- Risk identification and escalation.
- The risk-assessment methodology.
- Business-partner risk indicators.
- Regulatory and jurisdictional restrictions.
- Supplier and outsourcing risks.
- Incident and near-miss reporting.
- Financial-control risks.
- Information-security and data-protection risks.
- AML/CFT/CPF and sanctions awareness.
- Recordkeeping requirements.
- Individual authority limits.
- Changes to the Company's risk appetite or procedures.

Risk-related training must be updated where material new risks, regulatory requirements, or control weaknesses are identified.

5.26 Independent Review and Assurance

The Company may obtain independent assurance from auditors, legal advisers, compliance professionals, information-security specialists, accountants, or other competent persons.

Independent review should be considered where:

- A risk is particularly complex or material.
- Internal expertise is insufficient.
- A significant conflict of interest exists.
- A serious incident or control failure has occurred.
- The CGA or another authority requests assurance.
- The Company introduces a materially new activity.
- Management requires confirmation that corrective actions are effective.
- The same person performs multiple roles affecting segregation of responsibilities.

The scope, findings, recommendations, management response, and completion of corrective actions must be documented.

5.27 Review of the Risk-Management Framework

The Director and Compliance Officer must review this framework at least annually and following any material change.

The review should consider:

- Whether the framework reflects the Company's actual activities.
- Whether risks are being identified and escalated promptly.
- Whether assessments are complete and consistent.
- Whether risk owners understand their responsibilities.
- Whether controls are operating effectively.
- Whether risk classifications remain appropriate.
- Whether corrective actions are completed on time.
- Whether the risk appetite remains suitable.
- Whether Babylon Gaming and other material dependencies are adequately addressed.
- Whether the framework remains consistent with the AML/CFT Policy and other internal documents.
- Whether changes to legislation, CGA requirements, or licence conditions require amendments.

- Whether additional resources, training, or independent assurance are required.

Material amendments must be approved by the Director and communicated to the relevant personnel.

Regulatory Compliance Framework

6

Chapter 6 – Regulatory Compliance Framework

6.1 Purpose

This chapter establishes the framework through which Bet Play B.V. manages and demonstrates compliance with the laws, regulations, licence conditions, regulatory directions, contractual restrictions, and internal standards applicable to its activities as a licensed B2B gaming supplier.

The framework is intended to ensure that:

- The Company conducts only activities permitted under its licence.
- Regulatory responsibilities are clearly identified and allocated.
- Compliance requirements are translated into operational controls.
- Regulatory developments are identified, assessed, and implemented promptly.
- Business partners, markets, products, and distribution arrangements are reviewed before approval.
- Material compliance concerns are escalated without delay.
- Breaches and control weaknesses are investigated and remediated.
- Required regulatory notifications and submissions are made accurately and on time.
- Compliance decisions and supporting evidence are properly documented.
- The Company maintains effective oversight of activities performed by Babylon Gaming and other service providers on its behalf or in support of its operations.

This chapter may be read together with the Company's:

- AML/CFT Policy.
- Business Risk Management Framework.
- Business-partner onboarding and due-diligence procedures.
- Outsourcing and supplier-management arrangements.
- Information-security and data-protection controls.
- Incident-management and business-continuity arrangements.
- Recordkeeping and document-retention requirements.

6.2 Scope

This framework applies to:

- The Director.
- The Compliance Officer.
- The MLRO.
- The CFO.
- Account Management.
- All employees and contractors.
- External compliance, legal, financial, technical, and regulatory advisers.
- Babylon Gaming and other material providers, to the extent relevant to the services they perform.
- Prospective and existing business partners.
- Products and gaming content distributed through the Company's arrangements.
- Markets and jurisdictions connected with the Company's activities.
- Commercial, contractual, financial, technical, and operational changes.
- Regulatory submissions, notifications, inspections, audits, and information requests.

Compliance is a continuing responsibility and must be considered throughout the lifecycle of every material relationship and activity.

6.3 Regulatory Status and Permitted Activities

Bet Play B.V. must operate strictly within the scope of the licence granted by the Curaçao Gaming Authority ("CGA") and any related permissions, conditions, limitations, or regulatory directions.

The Company operates as a B2B gaming supplier. Its activities principally involve the commercial distribution and facilitation of access to gaming content and related services made available through Babylon Gaming and relevant upstream providers.

The Company must not conduct or represent itself as conducting activities outside its regulatory and contractual authority.

In particular, unless separately authorised, Bet Play B.V. must not:

- Accept or register individual players.
- Hold or manage player funds.

- Determine or alter game outcomes.
- Operate a consumer-facing online casino.
- Issue gaming accounts directly to players.
- Process player withdrawals or deposits.
- Perform the regulated obligations of a B2C gaming operator.
- Claim ownership or operational control of technology belonging to Babylon Gaming or another provider.
- Distribute gaming content beyond the rights granted under its supplier arrangements.
- Permit onward distribution without the required contractual, compliance, and supplier approvals.
- Enter a jurisdiction in which its proposed activities would be unlawful or require an authorisation that has not been obtained.

Any uncertainty concerning the scope of permitted activities must be referred to the Compliance Officer before the activity proceeds.

6.4 Compliance Principles

6.4.1 Lawfulness

The Company must not pursue a commercial objective through unlawful conduct or conduct that breaches its licence conditions.

6.4.2 Regulatory Accountability

Reliance on Babylon Gaming, a consultant, business partner, or another external provider does not remove the Company's regulatory accountability.

The Company must understand:

- Which responsibilities it performs directly.
- Which responsibilities are performed by another party.
- How performance is monitored.
- How deficiencies are identified and escalated.
- What evidence is available to demonstrate compliance.

6.4.3 Proportionality

Compliance controls must reflect the nature, scale, complexity, and risk of the Company's activities. Higher-risk relationships or proposals require stronger controls, greater scrutiny, and more senior approval.

6.4.4 Independence

The Compliance Officer and MLRO must be able to perform their responsibilities without improper commercial or operational interference.

Compliance concerns must not be suppressed, delayed, or altered to secure a commercial outcome.

6.4.5 Evidential Compliance

The Company must be able to demonstrate that required controls were applied.

Verbal confirmation or informal understanding is insufficient where a regulatory obligation, approval, assessment, review, or material decision should be documented.

6.4.6 Timely Escalation

Personnel must escalate a compliance concern as soon as it becomes known. A concern must not be withheld until all facts are confirmed where delay could increase regulatory, financial, operational, or reputational exposure.

6.4.7 Continuous Compliance

Approval at the beginning of a relationship does not establish permanent acceptability. The Company must monitor relevant changes throughout the relationship.

6.5 Compliance Governance

The Company maintains a compliance structure based on:

- Oversight and final accountability by the Director.
- Coordination and monitoring by the Compliance Officer.
- Independent financial-crime responsibilities assigned to the MLRO.
- Financial oversight by the CFO.
- First-line identification and escalation by Account Management and other personnel.

- Specialist support from external advisers where required.
- Oversight of Babylon Gaming and other material providers.
- Documented reporting, escalation, and approval arrangements.

The allocation of responsibilities must remain consistent with Chapter 4 of this Manual and the Company's current organisational structure.

Where one person holds more than one function, each responsibility must remain separately identifiable and any conflict, capacity issue, or independence concern must be managed appropriately.

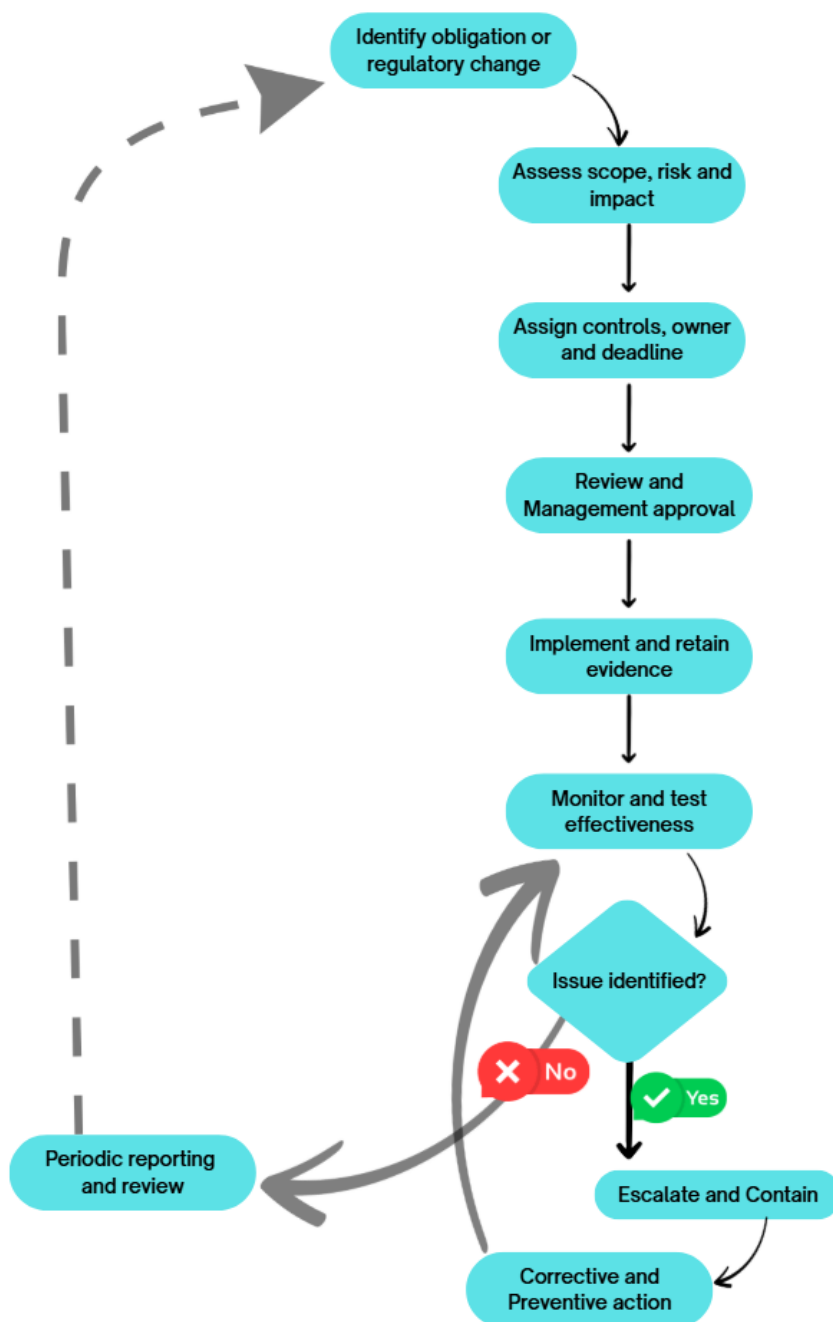


Figure 6.1 – Regulatory Compliance Management Lifecycle
 This diagram captures the central process running throughout the chapter: identifying requirements, assessing them, implementing controls, monitoring compliance, escalating deficiencies, and completing corrective action

6.6 Responsibilities of the Director

The Director has ultimate responsibility for ensuring that the Company maintains an effective regulatory compliance framework.

The Director is responsible for:

- Establishing an appropriate compliance culture.
- Ensuring that the Company operates within its licence scope.
- Approving material compliance policies and procedures.
- Ensuring the Compliance Officer and MLRO have sufficient authority, information, access, and resources.
- Reviewing material compliance risks and breaches.
- Approving entry into material new markets, services, and distribution arrangements.
- Approving high-risk business relationships where permitted.
- Determining whether a relationship or activity should be restricted, suspended, or terminated.
- Ensuring regulatory submissions and notifications receive appropriate oversight.
- Addressing material audit, regulatory, or monitoring findings.
- Ensuring that corrective actions are assigned and completed.
- Ensuring that the CGA is informed of reportable matters.
- Preventing improper interference with the Compliance Officer or MLRO.
- Obtaining external professional advice where the Company lacks sufficient internal expertise.

The Director must receive compliance information of sufficient quality and frequency to exercise effective oversight.

6.7 Responsibilities of the Compliance Officer

The Compliance Officer is responsible for coordinating the Company's regulatory compliance framework.

Responsibilities include:

- Maintaining awareness of applicable legal and regulatory requirements.
- Monitoring the Company's continued compliance with its licence.
- Advising the Director and personnel on regulatory matters.
- Reviewing the regulatory implications of proposed activities and changes.

- Supporting business-partner suitability and market reviews.
- Assessing compliance implications associated with contracts and distribution arrangements.
- Maintaining the regulatory obligations register.
- Coordinating the compliance-monitoring programme.
- Maintaining regulatory correspondence and submission records.
- Escalating actual or suspected breaches.
- Recommending corrective, preventive, or restrictive measures.
- Monitoring completion of agreed remedial actions.
- Supporting regulatory audits, inspections, and information requests.
- Reviewing whether material providers continue to satisfy applicable requirements.
- Providing or coordinating compliance training.
- Reporting material compliance matters to the Director.
- Liaising with the CGA where authorised or required.

The Compliance Officer must have timely access to:

- Corporate and licensing records.
- Business-partner files.
- Material agreements.
- Product and distribution information.
- Market and jurisdictional information.
- Financial and reconciliation information relevant to compliance.
- Incident and complaint records.
- Provider-performance information.
- Internal policies and procedures.
- Regulatory submissions and correspondence.
- Audit and monitoring records.

6.8 Responsibilities of the MLRO

The MLRO is responsible for the Company's AML/CFT/CPF, sanctions, and suspicious-activity arrangements in accordance with the separate AML/CFT Policy.

The MLRO's responsibilities include:

- Overseeing the financial-crime risk framework.
- Reviewing internal reports of suspicious activity.
- Determining whether an external report is required.
- Maintaining the confidentiality of suspicious-activity information.
- Overseeing sanctions, PEP, and relevant adverse-media controls.

- Advising on higher-risk business-partner relationships.
- Escalating material financial-crime risks to the Director where appropriate.
- Maintaining access to the information required to discharge the function.
- Liaising with the competent authorities where required.

Nothing in this chapter permits another person to direct the MLRO's decision concerning whether a suspicious-activity report should be submitted.

6.9 Responsibilities of the CFO

The CFO supports regulatory compliance by ensuring that appropriate financial controls and records are maintained.

Responsibilities include:

- Maintaining accurate accounting and financial records.
- Supporting regulatory financial reporting.
- Monitoring liquidity, receivables, and material financial exposure.
- Reviewing unusual payment or settlement arrangements.
- Escalating unexplained reconciliation discrepancies.
- Verifying changes to bank or payment instructions.
- Supporting the review of business-partner financial standing where relevant.
- Ensuring required taxes, fees, and licence-related payments are monitored.
- Supporting audits and regulatory requests.
- Reporting suspected financial irregularities to the Director, Compliance Officer, or MLRO, as appropriate.

6.10 Responsibilities of Account Management

Account Management forms part of the Company's first line of compliance control.

Account Managers must:

- Provide accurate information about prospective and existing business partners.
- Avoid making commitments before the required approvals are obtained.
- Ensure due-diligence requests are communicated and followed up.
- Identify proposed markets, domains, brands, distribution arrangements, and intended use of gaming content.
- Monitor material changes affecting assigned relationships.
- Escalate complaints, disputes, regulatory concerns, adverse information, and contractual breaches.
- Report suspected unauthorised onward distribution.

- Communicate applicable restrictions and approval conditions.
- Avoid describing Bet Play B.V.'s services or technical capabilities inaccurately.
- Cooperate with periodic reviews and compliance monitoring.
- Ensure that commercial urgency does not override compliance requirements.

Account Management may coordinate onboarding and activation but may not grant compliance clearance.

6.1.1 Regulatory Obligations Register

The Company must maintain a regulatory obligations register identifying the principal requirements applicable to its operations.

The register should include:

- The relevant law, regulation, licence condition, regulatory direction, or internal commitment.
- A summary of the requirement.
- The activity or function affected.
- The responsible owner.
- The control or procedure used to satisfy the requirement.
- The evidence retained.
- The applicable deadline or frequency.
- The date of the most recent review.
- Identified deficiencies or required actions.
- The next review date.

The register should cover, where applicable:

- Licence scope and conditions.
- Corporate and ownership requirements.
- Key-person appointments.
- Regulatory notifications.
- Business-partner suitability.
- AML/CFT/CPF and sanctions.
- Outsourcing and material provider oversight.
- Technical or certification requirements relevant to the Company.
- Information security and data protection.
- Regulatory fees and financial reporting.
- Recordkeeping and retention.
- Incident and breach reporting.
- Complaints relating to the Company's B2B services.

- Audit and assurance requirements.
- Changes requiring approval or notification.

The Compliance Officer must review the register at least annually and following a material regulatory amendment.

6.12 Regulatory Horizon Scanning

The Compliance Officer must maintain a reasonable process for identifying legal and regulatory developments that may affect the Company.

Relevant sources may include:

- CGA publications and direct communications.
- Curaçao legislation and official notices.
- Competent financial-intelligence and sanctions authorities.
- Regulatory publications in markets relevant to the Company.
- Professional legal and compliance updates.
- Industry associations.
- External legal or regulatory advisers.
- Notifications from Babylon Gaming or other material providers.
- Enforcement decisions and regulatory warnings relevant to the Company's activities.

A regulatory development must be assessed to determine:

- Whether it applies to the Company.
- Which relationships, products, markets, or procedures are affected.
- The implementation date.
- Whether regulatory clarification or external advice is required.
- Which documents, systems, contracts, or controls must change.
- Who is responsible for implementation.
- Whether personnel or business partners must be informed.
- Whether the CGA must be notified.
- What evidence will demonstrate completion.

6.13 Regulatory Change Management

Material regulatory changes must be documented and managed through an implementation plan.

The plan should identify:

- The relevant regulatory change.
- Its effective or transitional date.
- The gap between current and required arrangements.
- Required changes to policies, procedures, contracts, or controls.
- Responsible persons.
- Required resources or external support.
- Implementation deadlines.
- Training or communication requirements.
- Required testing or assurance.
- Evidence of completion.
- Any remaining risks or dependencies.

The Compliance Officer must monitor implementation and escalate overdue or inadequate actions to the Director.

A regulatory change must not be treated as implemented solely because an internal document has been amended. The Company must confirm that affected operational practices and controls have also changed.

6.14 Compliance Risk Assessment

Compliance risk assessments must be conducted in accordance with the methodology established in Chapter 5.

A compliance assessment should consider:

- Whether the activity falls within the Company's licence scope.
- Applicable legal and regulatory requirements.
- Relevant jurisdictions.
- Business-partner licensing and suitability.
- Product and content restrictions.
- Distribution and onward-distribution arrangements.
- Contractual rights and limitations.
- Responsibilities performed by Bet Play B.V.
- Responsibilities performed by Babylon Gaming or another provider.
- Required technical, regulatory, or game certifications.
- AML/CFT/CPF and sanctions exposure.
- Information-security and data-protection implications.
- Required notifications, consents, or approvals.
- Available resources and competence.
- Potential consequences of non-compliance.

Material uncertainty must be resolved before the relevant activity begins.

6.15 Compliance Review of New Business Partners

Before a prospective business partner is approved, the Compliance Officer must confirm that the applicable review has been completed.

The review must establish, where relevant:

- The identity and legal existence of the entity.
- Ownership and control.
- Ultimate beneficial owners.
- Directors and key persons.
- Regulatory and licensing status.
- The proposed nature of the relationship.
- Intended brands, domains, and markets.
- Proposed distribution arrangements.
- Whether resellers or downstream business partners will be involved.
- Whether the proposed use of content is contractually permitted.
- Whether any relevant sanctions, PEP, adverse-media, or enforcement concerns exist.
- Whether the relationship is compatible with the Company's risk appetite.
- Whether Babylon Gaming or another provider must approve the relationship.
- Whether conditions, restrictions, or enhanced monitoring are required.

The detailed due-diligence and onboarding process is addressed in Chapter 7 and the AML/CFT Policy.

6.16 Market and Jurisdictional Compliance

Before approving distribution into a new market, the Company must determine whether the proposed activity is lawful and permitted.

The assessment should consider:

- The location of the business partner.
- The markets in which gaming content will be made available.
- The licensing status of the business partner in those markets.
- Whether supplier licensing or registration is required.
- Whether the relevant games or game categories are permitted.
- Whether specific technical certification is required.
- Any advertising, localisation, or content restrictions relevant to the relationship.

- Applicable sanctions and prohibited-territory restrictions.
- Contractual restrictions imposed by Babylon Gaming or upstream providers.
- Regulatory warnings, blacklist entries, or enforcement history.
- Whether geolocation or access restrictions are required from the operator or technical provider.
- Whether local legal advice is necessary.

A business partner's representation that it may lawfully operate in a jurisdiction does not automatically replace the Company's own proportionate assessment.

Where legal or regulatory uncertainty is material, the Company must:

- Obtain additional evidence.
- Seek appropriate professional advice.
- Impose conditions or restrictions.
- Delay the proposed activity.
- Decline the market or relationship.

6.17 Licence Verification

Where a business partner is required to hold a licence or other authorisation, the Company must verify the status of that authorisation through a reliable source.

Verification should establish:

- The name of the licence holder.
- The licensing authority.
- The licence or authorisation number.
- The activities and brands covered.
- The authorised domains, where available.
- The effective and expiry dates, where applicable.
- Any material conditions or limitations.
- Whether the licence is active, suspended, revoked, or subject to enforcement.
- Whether the proposed arrangement falls within its scope.

Evidence of the verification must be retained.

Licence status must be reviewed periodically and following information suggesting that the licence may have changed.

6.18 Product and Content Compliance

Before gaming content is made available through a business-partner relationship, the Company must confirm, to the extent applicable to its role, that:

- The content falls within the relevant contractual rights.
- The provider has authorised its distribution.
- Required certifications or testing evidence are available.
- The intended market is permitted.
- The business partner is authorised to offer the relevant content.
- Relevant game restrictions have been communicated.
- The content is accurately described.
- Required technical or commercial conditions have been satisfied.
- Responsibilities for updates, suspension, and incident handling are understood.
- Any supplier conditions have been recorded.

Bet Play B.V. must not claim to have independently developed, tested, hosted, certified, or controlled games where those functions are performed by Babylon Gaming or another provider.

6.19 Onward Distribution and Reseller Controls

A business partner may not resell, sublicense, aggregate, or otherwise distribute the Company's content to another party unless the arrangement has been expressly approved.

Before approving onward distribution, the Company must assess:

- The identity and regulatory status of the downstream party.
- Ownership and control.
- Intended markets and domains.
- The contractual chain.
- Whether Babylon Gaming or an upstream provider permits the arrangement.
- Applicable due-diligence requirements.
- Responsibility for monitoring downstream use.
- Audit, information, suspension, and termination rights.
- Whether the arrangement creates additional licensing obligations.
- How unauthorised or prohibited distribution will be identified and addressed.

Undisclosed onward distribution constitutes a material compliance and contractual concern and must be escalated immediately.

6.20 Compliance Conditions and Restrictions

The Company may approve a relationship or activity subject to documented conditions.

Conditions may include:

- Restriction to specified jurisdictions.
- Restriction to approved brands or domains.
- Exclusion of particular games or content.
- Prohibition of onward distribution.
- Completion of additional due diligence.
- Provision of updated licensing evidence.
- Enhanced or more frequent monitoring.
- Prior approval for material changes.
- Specific reporting requirements.
- Technical or access restrictions.
- Additional contractual protections.
- Confirmation from Babylon Gaming or another provider.

The responsible relationship owner must understand the conditions and ensure they are communicated and implemented.

A relationship must not be activated until all pre-activation conditions have been satisfied.

6.21 Compliance Monitoring Programme

The Compliance Officer must maintain a risk-based compliance-monitoring programme.

The programme should identify:

- The area or obligation being reviewed.
- The regulatory or internal requirement.
- The purpose and scope of the review.
- The review frequency.
- The responsible reviewer.
- The sample or evidence required.
- The expected control.
- The method of testing.
- The findings and risk classification.
- Required corrective actions.
- The responsible action owner.
- Target completion dates.

- Follow-up and closure arrangements.

Monitoring may cover:

- Licence-scope compliance.
- Business-partner onboarding.
- Due-diligence completeness.
- Licensing and market verification.
- Contract execution.
- Approval conditions.
- Onward-distribution controls.
- Regulatory notifications and submissions.
- Babylon Gaming and supplier oversight.
- Financial and reconciliation controls.
- Incident and complaint handling.
- Information-security controls.
- Training completion.
- Recordkeeping.
- Policy review dates.
- Corrective-action completion.

6.22 Monitoring Methods

Compliance monitoring may include:

- File reviews.
- Sample testing.
- Interviews with responsible personnel.
- Review of contracts and approvals.
- Examination of domains, brands, and market activity.
- Review of management information.
- Inspection of regulatory and provider records.
- Review of incidents, complaints, and disputes.
- Verification of licence status.
- Review of invoices and financial records.
- Testing of escalation procedures.
- Confirmation that approval conditions remain effective.
- Review of provider reports and service performance.
- Follow-up of previous findings.

Monitoring must assess both the design and the practical operation of the relevant control.

6.23 Classification of Compliance Findings

Compliance findings should be classified according to their seriousness.

Classification	General description	Required response
Low	Minor administrative or documentation weakness with limited compliance impact.	Correct through routine action and monitor completion.
Moderate	Control weakness capable of creating a material issue if not corrected.	Assign corrective action, responsible owner, and deadline.
High	Material control failure, serious exposure, or likely breach requiring prompt senior attention.	Escalate to the Director and implement urgent remediation.
Critical	Actual or imminent serious breach, licence threat, prohibited activity, or unacceptable exposure.	Escalate immediately; pause or restrict the affected activity and consider regulatory notification.

Professional judgement must be applied. A finding may be escalated regardless of its numerical risk score where its nature or regulatory significance warrants this.

6.24 Regulatory Breach Identification

A regulatory breach or suspected breach may be identified through:

- Compliance monitoring.
- Internal reports.
- Business-partner reviews.
- Financial reconciliations.
- Complaints or disputes.
- Technical or security incidents.
- Provider notifications.
- Audit findings.
- Regulatory correspondence.
- Adverse media.

- Missed submissions or deadlines.
- Unauthorised market or content use.
- Changes in licence status.
- Inaccurate or incomplete regulatory information.
- Failure to implement an approval condition.
- Activity outside the Company's permitted licence scope.

Personnel must report an actual or suspected breach immediately to the Compliance Officer.

Where the matter concerns suspected financial crime, it must also be reported to the MLRO through the appropriate confidential channel.

6.25 Breach Assessment and Response

Following identification of an actual or suspected breach, the Compliance Officer must coordinate an initial assessment addressing:

- What occurred.
- When it began and whether it is continuing.
- How it was identified.
- The applicable requirement.
- The persons, business partners, markets, systems, or services affected.
- The actual and potential impact.
- Whether immediate containment is required.
- Whether the activity should be suspended.
- Whether evidence must be preserved.
- Whether external legal or technical advice is required.
- Whether the CGA or another authority must be notified.
- Whether a contractual notification is required.
- What corrective and preventive actions are necessary.

The Company must not conceal, minimise, or inaccurately describe a material breach.

6.26 Regulatory Notifications

The Company must notify the CGA and other competent authorities whenever required by law, regulation, licence condition, or regulatory direction.

Potentially notifiable matters may include:

- Changes in ownership or control.

- Changes involving Directors, key persons, or regulated functions.
- Material changes to the business model.
- Material outsourcing or critical supplier arrangements.
- Changes affecting licence scope.
- Serious regulatory breaches.
- Material security or data incidents.
- Significant operational disruption.
- Events affecting financial viability.
- Criminal, regulatory, or enforcement proceedings.
- Material changes in corporate information.
- Other events specified by the CGA.

Before a notification is submitted, the Company should confirm:

- The applicable notification requirement.
- The deadline.
- The required form and supporting evidence.
- The accuracy and completeness of the information.
- The appropriate internal approval.
- Whether follow-up reporting will be required.

Where a notification deadline is urgent, the Company must not delay solely because every detail is not yet available. An initial notification may be made and supplemented when appropriate.

6.27 Regulatory Submissions and Returns

The Company must maintain a schedule of required regulatory submissions, returns, declarations, fees, and licence-related deadlines.

The schedule should record:

- The submission or payment required.
- The responsible owner.
- The reporting period.
- The due date.
- The required reviewer or approver.
- Supporting information required.
- The date submitted or paid.
- Evidence of submission or payment.
- Any acknowledgement or follow-up.
- Any extension, correction, or resubmission.

Information submitted to the CGA must be:

- Accurate.
- Complete.
- Consistent with Company records.
- Supported by appropriate evidence.
- Reviewed by a competent person.
- Approved in accordance with the Company's authority arrangements.
- Retained with proof of submission.

Any material error identified after submission must be escalated promptly and corrected where necessary.

6.28 Regulatory Correspondence and Requests

All material correspondence from the CGA or another competent authority must be forwarded promptly to the Director and Compliance Officer.

The Company must:

- Record the date and method of receipt.
- Identify the response deadline.
- Assign responsibility for coordinating the response.
- Preserve all relevant evidence.
- Ensure the response is accurate and complete.
- Obtain appropriate internal and professional review.
- Submit the response within the required period.
- Retain the final response and evidence of submission.
- Monitor any resulting actions or commitments.

No person may alter, conceal, destroy, or fabricate information relevant to a regulatory request.

6.29 Regulatory Inspections, Audits and Interviews

The Company must cooperate fully and professionally with lawful regulatory inspections, audits, meetings, and interviews.

The Compliance Officer should coordinate:

- Identification of the scope and requested information.
- Collection and preservation of documents.
- Verification that records are complete and current.

- Scheduling of relevant personnel.
- Internal briefing on the process.
- Engagement of legal or specialist advisers where appropriate.
- Recording of questions, responses, and commitments.
- Follow-up actions and deadlines.

Personnel must answer regulatory questions honestly and within their knowledge. Where a person does not know or cannot verify an answer, this must be stated rather than guessed.

6.30 Internal Escalation

A compliance matter must be escalated immediately where it involves:

- An actual or suspected breach of law or licence condition.
- Activity outside the Company's authorised scope.
- A CGA inquiry, warning, or enforcement matter.
- A prohibited or unauthorised jurisdiction.
- A material business-partner suitability concern.
- Loss, suspension, or restriction of a relevant licence.
- Unauthorised onward distribution.
- A serious provider or supplier control failure.
- A material security or personal-data incident.
- Suspected fraud, sanctions exposure, or financial crime.
- Inaccurate information previously provided to a regulator.
- Failure to meet a material regulatory deadline.
- A conflict affecting the independence of a control function.
- Obstruction or concealment of a compliance concern.
- A matter capable of threatening the Company's licence or continued operations.

The Director, following advice from the Compliance Officer and other relevant officers, must determine the immediate response.

6.31 Suspension and Termination Controls

The Company must be able to restrict, suspend, or terminate a relationship or activity where continued operation creates unacceptable legal, regulatory, contractual, financial, or reputational risk.

Grounds may include:

- Loss or suspension of a required licence.

- Provision of false or misleading information.
- Refusal to provide required due-diligence information.
- Sanctions or serious financial-crime concerns.
- Unauthorised markets, domains, or onward distribution.
- Material contractual breach.
- Serious or repeated non-compliance.
- Regulatory enforcement.
- Failure to comply with approval conditions.
- Use of content outside authorised arrangements.
- Conduct capable of harming the Company's licence or reputation.

The decision and rationale must be documented.

Where immediate suspension is necessary, the Company must coordinate with Babylon Gaming or the relevant provider to the extent required to implement the restriction safely and effectively.

6.32 Corrective and Preventive Action

Compliance findings, breaches, audit observations, and regulatory concerns must be addressed through documented corrective and preventive action.

Each action should identify:

- The issue or deficiency.
- Its cause.
- The corrective action.
- Any preventive action.
- The responsible owner.
- The target date.
- Interim controls.
- Required evidence.
- The person responsible for verifying completion.
- Any reporting or approval requirement.

A finding may be closed only after sufficient evidence confirms that the required action has been implemented and is operating effectively.

6.33 Compliance Reporting

The Compliance Officer must provide the Director with periodic compliance reports proportionate to the Company's activities and risk profile.

Reports may include:

- Material regulatory developments.
- Licence and submission status.
- Business-partner onboarding and review information.
- Higher-risk or restricted relationships.
- Market and jurisdictional concerns.
- Compliance-monitoring findings.
- Incidents and suspected breaches.
- Regulatory correspondence.
- Supplier and Babylon Gaming oversight matters.
- Open corrective actions.
- Overdue actions.
- Training completion.
- Policy and procedure reviews.
- Matters requiring a decision, additional resources, or external advice.

Urgent matters must be reported immediately and must not wait for the next periodic report.

6.34 Compliance Meetings

Compliance matters may be reviewed through periodic management or compliance meetings.

The agenda may include:

- Regulatory developments.
- New and changing business-partner relationships.
- Market-entry proposals.
- Licence and certification matters.
- Provider and supplier issues.
- Compliance-monitoring results.
- Incidents, complaints, and disputes.
- Financial and reconciliation concerns.
- AML/CFT/CPF and sanctions matters, subject to confidentiality restrictions.
- Corrective-action progress.
- Training and resource requirements.
- Upcoming regulatory submissions and audits.

Material decisions, actions, responsible persons, and deadlines must be recorded.

Confidential suspicious-activity information must not be included in general meeting records where doing so would breach confidentiality requirements.

6.35 Conflicts of Interest

Actual or potential conflicts affecting a regulatory or compliance decision must be disclosed promptly.

A person must not independently approve a matter where they:

- Have a personal or financial interest.
- Were materially involved in creating the issue under review.
- Have a close relationship with the affected party.
- May benefit from approval.
- Cannot exercise objective judgement.

Appropriate measures may include:

- Disclosure and recording of the conflict.
- Reassignment of the review or decision.
- Independent secondary approval.
- External professional review.
- Exclusion from relevant discussions.
- Additional monitoring.

6.36 Speak-Up and Non-Retaliation

Personnel must be able to report suspected non-compliance, misconduct, concealment, or improper interference without retaliation.

Reports may be made to:

- The Compliance Officer.
- The MLRO, for financial-crime matters.
- The Director.
- An appropriate external adviser or authority where permitted or required.

Retaliation against a person who raises a genuine concern in good faith is prohibited.

Knowingly false or malicious reports may be addressed through appropriate disciplinary or contractual measures.

6.37 Outsourced Compliance Support

The Company may engage qualified external advisers to support:

- Regulatory interpretation.
- Policy development.
- Licence applications and changes.
- Business-partner reviews.
- Market-entry assessments.
- Compliance monitoring.
- Audits and independent assurance.
- Regulatory responses.
- Training.
- Remedial projects.

External support does not replace the Company's responsibility for compliance.

The Company must ensure that:

- The adviser is suitably competent.
- The scope of work is documented.
- Confidentiality is protected.
- Advice is reviewed and implemented appropriately.
- Decisions remain with the authorised Company officers.
- Records of material advice and resulting actions are retained.

6.38 Compliance Training

Personnel must receive compliance training appropriate to their responsibilities.

Training should cover, where relevant:

- The Company's licence scope.
- Individual responsibilities and authority limits.
- Business-partner onboarding.
- Market and jurisdictional restrictions.
- Product and distribution controls.
- Onward-distribution risks.
- Regulatory escalation.
- Breach and incident reporting.
- AML/CFT/CPF and sanctions awareness.
- Information security and data protection.
- Conflicts of interest.

- Recordkeeping.
- Regulatory changes.
- Consequences of non-compliance.

Training must be provided:

- During induction.
- Periodically thereafter.
- Following a material regulatory change.
- When an individual's responsibilities change.
- Where monitoring or an incident identifies a knowledge deficiency.

Completion records must be retained.

6.39 Compliance Records

The Company must maintain appropriate records demonstrating operation of the compliance framework.

Records may include:

- Regulatory obligations registers.
- Regulatory-change assessments.
- Compliance risk assessments.
- Business-partner approvals.
- Licence and market verifications.
- Compliance conditions and restrictions.
- Monitoring plans and testing records.
- Findings and corrective actions.
- Regulatory submissions and notifications.
- Correspondence with the CGA.
- Audit and inspection records.
- Compliance reports and meeting records.
- External legal and regulatory advice.
- Training records.
- Breach and incident assessments.
- Suspension and termination decisions.
- Policy approvals and reviews.

Records must be accurate, dated, attributable, protected from unauthorised alteration, and accessible to authorised persons.

6.40 Compliance Management Information

Where proportionate, the Company should maintain compliance indicators to assist management oversight.

Indicators may include:

- Prospective partners awaiting compliance clearance.
- Higher-risk business partners.
- Due-diligence reviews overdue.
- Expired or unverified licences.
- New markets awaiting approval.
- Outstanding compliance conditions.
- Suspected unauthorised onward distribution.
- Regulatory submissions approaching or exceeding deadline.
- Open compliance findings.
- Overdue corrective actions.
- Material incidents and breaches.
- Complaints or disputes indicating a control weakness.
- Training completion rates.
- Policy reviews overdue.
- Material Babylon Gaming or supplier issues.

Indicators must be interpreted in context and do not replace qualitative review.

6.41 Independent Compliance Review

The Company should obtain independent review where proportionate to its risk, scale, and regulatory obligations.

An independent review should be considered:

- At planned intervals.
- Following a serious breach.
- Before or following a material business-model change.
- Where the same person performs multiple potentially conflicting roles.
- Where internal expertise is insufficient.
- Following significant regulatory criticism.
- When required by the CGA.
- To verify completion of material remedial actions.

The review must be conducted by a suitably competent person who is sufficiently independent of the activity being assessed.

Findings, management responses, actions, and closure evidence must be documented.

6.42 Review of the Compliance Framework

The Director and Compliance Officer must review this framework at least annually and whenever a material change occurs.

The review must consider:

- Changes to legislation, regulation, and licence conditions.
- Changes to the Company's activities or licence scope.
- Changes in business partners, markets, products, or distribution models.
- Changes involving Babylon Gaming or another material provider.
- Regulatory correspondence and feedback.
- Compliance-monitoring results.
- Breaches, incidents, complaints, and near misses.
- Audit and assurance findings.
- Corrective-action completion.
- The adequacy of resources, competence, and independence.
- The effectiveness of regulatory change management.
- The accuracy of role allocations and procedures.
- Consistency with the AML/CFT Policy and other internal documents.
- Whether the documented framework reflects actual practice.

Material amendments must be approved by the Director and communicated to affected personnel.

Business- Partner Onboarding

7

Chapter 7 – Business-Partner Onboarding and Due Diligence

7.1 Purpose

This chapter establishes the procedures through which Bet Play B.V. identifies, assesses, approves, activates, monitors, reviews, restricts, and terminates relationships with its business partners.

The framework is intended to ensure that the Company:

- Understands the identity, ownership, control, activities, and regulatory status of each business partner.
- Establishes the legitimate purpose and intended scope of every relationship.
- Conducts proportionate due diligence before entering into a relationship.
- Does not distribute gaming content to unsuitable, unauthorised, sanctioned, or unlawfully operating parties.
- Identifies the jurisdictions, brands, domains, and distribution channels connected with each relationship.
- Obtains any approval required from Babylon Gaming or an upstream provider.
- Applies enhanced due diligence to higher-risk relationships.
- Records compliance, commercial, financial, and management approvals.
- Activates a relationship only after all applicable conditions have been satisfied.
- Monitors business partners throughout the relationship.
- Identifies and responds to material changes, warning indicators, and suspected unauthorised activity.
- Maintains sufficient records to demonstrate compliance with regulatory, contractual, and internal requirements.

This chapter must be read together with the Company's:

- AML/CFT Policy.
- Business Risk Management Framework.
- Regulatory Compliance Framework.
- Sanctions-screening procedures.
- Contract-approval procedures.
- Supplier and outsourcing arrangements.
- Information-security and data-protection controls.
- Recordkeeping and document-retention requirements.

7.2 Scope

This chapter applies to prospective and existing:

- B2B gaming operators.
- Licensed gaming operators.
- Aggregators.
- Platform providers.
- Resellers and distributors.
- White-label providers, where applicable.
- Commercial agents and introducers.
- Payment and settlement counterparties.
- Material suppliers and service providers.
- Any downstream party receiving or accessing gaming content through an approved distribution arrangement.
- Any other corporate counterparty whose relationship may expose the Company to regulatory, financial, contractual, operational, AML/CFT/CPF, sanctions, or reputational risk.

The level of due diligence must be proportionate to the nature, scale, complexity, and risk of the proposed relationship.

7.3 Business-Partner Acceptance Principles

The Company must apply the following principles when considering a business relationship:

7.3.1 No Activation Before Approval

A prospective business partner must not receive access to gaming content, technical integrations, production credentials, commercial services, or other operational capabilities until the required onboarding process has been completed.

7.3.2 Risk-Based Due Diligence

The scope and depth of due diligence must reflect the risks associated with:

- The business partner.
- Its ownership and control.
- Its regulatory status.
- Its activities and business model.

- The jurisdictions involved.
- The proposed distribution arrangements.
- The products or content requested.
- Payment and settlement arrangements.
- Its reputation and regulatory history.
- Any use of downstream parties or resellers.

7.3.3 Evidential Verification

Material information must be supported by reliable, current, and independently verifiable evidence wherever reasonably possible.

Unverified representations must not be treated as established facts merely because they have been provided by the prospective business partner.

7.3.4 Transparency

A prospective business partner must provide complete and accurate information concerning its:

- Legal identity.
- Ownership and control.
- Ultimate beneficial owners.
- Directors and key persons.
- Licences and regulatory permissions.
- Brands and domains.
- Target markets.
- Distribution model.
- Intended use of gaming content.
- Payment arrangements.
- Material regulatory or enforcement history.

The deliberate concealment or misrepresentation of material information is grounds for rejection or termination.

7.3.5 Regulatory and Contractual Compatibility

The proposed relationship must be compatible with:

- Bet Play B.V.'s licence.
- Applicable Curaçao legal and regulatory requirements.
- The business partner's regulatory permissions.

- Babylon Gaming's requirements.
- Rights and restrictions imposed by upstream providers.
- Applicable market and jurisdictional requirements.
- The Company's risk appetite.

7.3.6 Continuing Suitability

Approval establishes suitability only at the time of the assessment. The Company must monitor the relationship and reassess it when relevant circumstances change.

7.4 Prohibited Relationships

The Company must not establish or maintain a relationship where:

- The party's identity cannot be satisfactorily verified.
- Ownership or control cannot be reasonably established.
- Required licences or regulatory permissions are absent, invalid, suspended, revoked, or materially restricted.
- The intended activity falls outside the Company's licence or contractual rights.
- The proposed relationship would breach applicable law, sanctions, or regulatory restrictions.
- The party intends to distribute content into a prohibited jurisdiction.
- The intended use of gaming content is materially unclear or inconsistent with the information provided.
- The party provides false, misleading, altered, or fraudulent documentation.
- The source or destination of material payments cannot be satisfactorily understood.
- The party insists on unexplained payments involving unrelated third parties.
- Sanctions exposure cannot be lawfully and adequately mitigated.
- There are substantiated concerns involving criminality, fraud, money laundering, terrorist financing, proliferation financing, corruption, or organised crime.
- The relationship would expose the Company to an unacceptable regulatory or reputational risk.
- Babylon Gaming or a relevant upstream provider refuses the relationship.
- Required enhanced due diligence cannot be completed.
- The Director, Compliance Officer, or MLRO determines that the residual risk is unacceptable.

A rejected party must not be introduced through another entity or arrangement for the purpose of circumventing the rejection.

7.5 Roles and Responsibilities

7.5.1 Director

The Director is responsible for:

- Approving material and higher-risk business relationships.
- Approving exceptions within their authority.
- Ensuring adequate resources are available for due diligence.
- Reviewing material suitability concerns.
- Determining whether a relationship should be restricted, suspended, rejected, or terminated.
- Ensuring that commercial objectives do not override regulatory requirements.
- Obtaining external professional advice where necessary.

7.5.2 Compliance Officer

The Compliance Officer is responsible for:

- Coordinating the business-partner onboarding process.
- Determining the required scope of due diligence.
- Reviewing corporate, ownership, licensing, market, and reputational information.
- Confirming whether compliance requirements have been satisfied.
- Identifying conditions or restrictions required before approval.
- Assigning or supporting the assignment of the business-partner risk classification.
- Verifying that required internal and supplier approvals have been obtained.
- Monitoring due-diligence expiry and review dates.
- Conducting or coordinating periodic and event-driven reviews.
- Escalating material concerns to the Director and MLRO.
- Maintaining appropriate onboarding and review records.

The Compliance Officer may withhold clearance where information is incomplete, inconsistent, outdated, or insufficient.

7.5.3 MLRO

The MLRO is responsible for:

- Assessing AML/CFT/CPF and sanctions concerns.
- Advising on enhanced due diligence.

- Reviewing higher-risk ownership, control, jurisdictional, payment, and financial-crime factors.
- Reviewing internal suspicious-activity reports.
- Determining whether an external suspicious-activity report is required.
- Ensuring that confidential financial-intelligence information is appropriately protected.

The MLRO's decision concerning suspicious-activity reporting must remain independent.

7.5.4 CFO

The CFO is responsible for:

- Reviewing proposed invoicing, payment, and settlement arrangements.
- Verifying bank-account and payment-instruction information.
- Assessing material financial exposure and credit risk.
- Reviewing unusual or complex payment structures.
- Monitoring overdue receivables and reconciliation discrepancies.
- Escalating financial irregularities.
- Supporting verification of financial standing where relevant.

7.5.5 Account Management

Account Management is responsible for:

- Obtaining an initial understanding of the prospective relationship.
- Providing accurate commercial information to Compliance.
- Collecting requested documentation.
- Identifying intended brands, domains, jurisdictions, and distribution arrangements.
- Communicating due-diligence requirements to the prospective business partner.
- Avoiding commitments before approval.
- Ensuring that conditions and restrictions are communicated.
- Monitoring material changes during the relationship.
- Escalating warning indicators, complaints, disputes, or suspected breaches.

Account Management must not approve its own prospective client or override a compliance decision.

7.5.6 Babylon Gaming and Other Providers

Where Babylon Gaming or another upstream provider must approve a relationship, product, market, or distribution arrangement, the responsible person must:

- Provide the required information to the provider.
- Record the approval, refusal, or conditions imposed.
- Ensure that approval is obtained before activation.
- Communicate relevant restrictions internally.
- Monitor continued compliance with the provider's conditions.

Provider approval does not replace the Company's own due diligence or regulatory responsibilities.

7.6 Initial Business Proposal

Before formal due diligence begins, the Company should obtain sufficient information to understand the proposed relationship.

The initial proposal should identify:

- The legal name of the prospective business partner.
- Country of incorporation.
- Registered and operating addresses.
- Website and principal domains.
- Contact persons.
- Nature of the business.
- Regulatory status.
- Products or services requested.
- Intended gaming content.
- Target and operating markets.
- Expected brands and domains.
- Proposed distribution model.
- Whether resellers or downstream clients are involved.
- Expected implementation date.
- Anticipated transaction or revenue levels.
- Proposed invoicing and payment arrangements.
- Any required technical integration.
- Any existing relationship with Babylon Gaming.
- The commercial relationship owner within Bet Play B.V.

The Company may decline a proposal at this stage where it is clearly outside its licence scope, contractual authority, risk appetite, or operational capability.

7.7 Onboarding Risk Screening

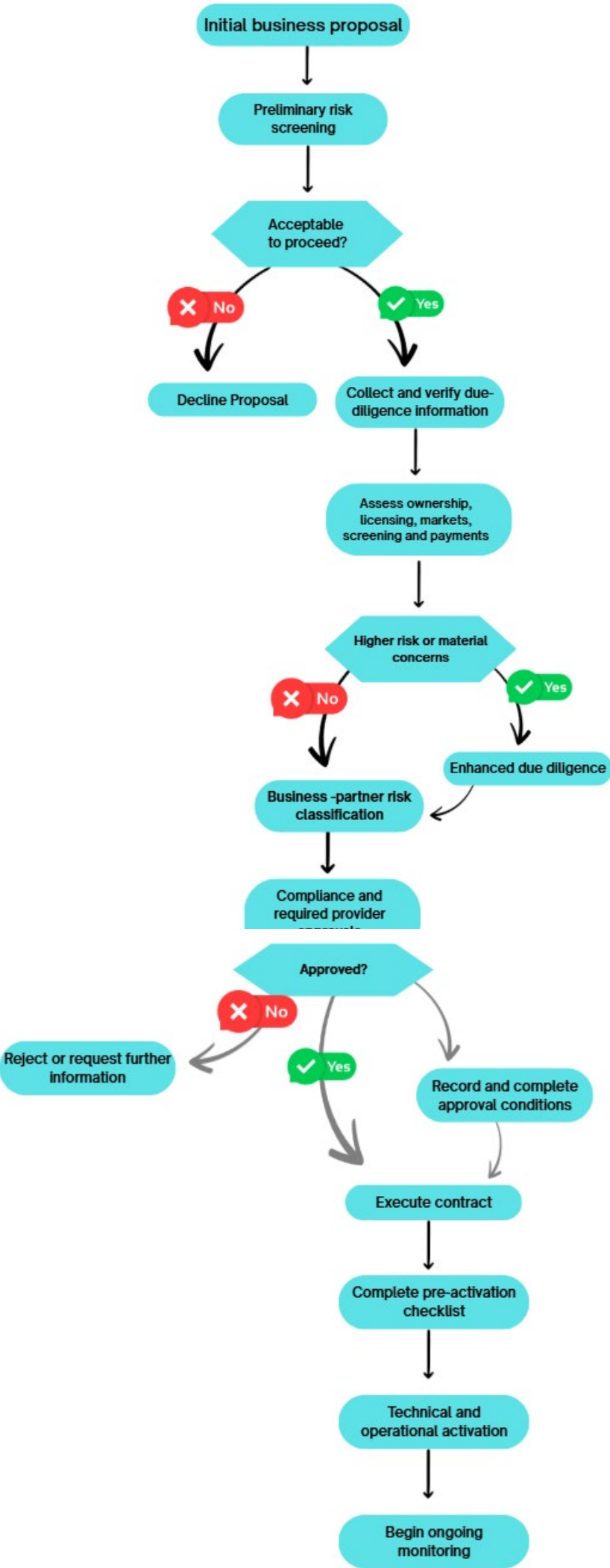
The Compliance Officer must conduct an initial risk screening to determine:

- Whether the proposal is within the Company's permitted activities.
- Whether the relevant jurisdictions are acceptable.
- Whether the party appears to hold required licences.
- Whether the proposed distribution model is permitted.
- Whether material adverse or regulatory information is immediately apparent.
- Whether the relationship involves higher-risk countries or ownership arrangements.
- Whether enhanced due diligence is likely to be required.
- Whether approval from Babylon Gaming or another provider is necessary.
- Whether specialist legal, regulatory, financial, or technical advice is required.

The screening result must be recorded.

An initial screening does not replace the full due-diligence assessment.

See Figure 7.1 Business-Partner Onboarding and Activation Workflow



7.8 Standard Due-Diligence Requirements

Unless otherwise determined through a documented risk assessment, the Company should obtain:

Corporate information

- Certificate of incorporation or equivalent formation document.
- Current commercial-register extract.
- Memorandum and articles of association or equivalent constitutional documents.
- Registered-office details.
- Principal place of business.
- Corporate registration and tax-identification numbers.
- Current organisational and ownership chart.
- Description of the business model and principal activities.

Ownership and control information

- Shareholder register or equivalent ownership record.
- Identification of direct and indirect shareholders.
- Identification of ultimate beneficial owners.
- Explanation of intermediate holding companies.
- Information concerning voting rights and other means of control.
- Details of trusts, nominees, foundations, partnerships, or similar arrangements, where applicable.

Management information

- Current Directors.
- Authorised signatories.
- Key management or compliance personnel relevant to the relationship.
- Persons authorised to provide instructions to the Company.
- Persons authorised to request technical or commercial changes.

Regulatory information

- Copies or reliable evidence of applicable gaming licences.
- Licence number and issuing authority.
- Licensed legal entity.
- Authorised activities.
- Approved brands and domains, where applicable.
- Relevant conditions, limitations, and expiry dates.

- Information concerning regulatory investigations, warnings, suspensions, or enforcement.

Operational information

- Intended brands and domains.
- Target and operating jurisdictions.
- Product and game requirements.
- Distribution and integration arrangements.
- Use of white labels, resellers, aggregators, or downstream operators.
- Intended player-facing operator, where relevant.
- Technical providers involved.
- Relevant information-security and data-protection arrangements.
- Proposed launch date.

Financial information

- Invoicing entity.
- Expected payment method and currency.
- Bank-account details.
- Expected value and frequency of payments.
- Source and destination of funds, where relevant.
- Audited financial statements or other financial-standing information where proportionate.
- Explanation of unusual or complex settlement structures.

Additional documentation may be requested according to the risks identified.

7.9 Verification of Legal Identity

The Company must verify that the legal entity:

- Exists as a validly incorporated or registered entity.
- Remains active and in good standing where this status is available.
- Uses the legal name stated in the proposed contract.
- Has an identifiable registered address.
- Is authorised to enter into the proposed agreement.
- Is represented by a properly authorised person.

Verification should be undertaken using:

- Official commercial registers.
- Regulatory databases.
- Certified corporate documents.

- Documents obtained directly from a competent authority.
- Reliable independent databases.
- Qualified legal or corporate-service providers.

Material inconsistencies must be resolved before approval.

7.10 Identification of Ownership and Control

The Company must understand the complete ownership and control structure of each business partner.

The assessment must identify:

- Direct shareholders.
- Intermediate corporate shareholders.
- Ultimate beneficial owners.
- Persons exercising control through voting rights.
- Persons exercising control through agreements or other arrangements.
- Nominee shareholders or Directors.
- Trusts, foundations, partnerships, or similar structures.
- Any person acting on behalf of another person.

The ownership structure must be traced to the ultimate natural person or persons, unless the entity qualifies for a documented exception under applicable law, such as certain publicly listed entities subject to adequate disclosure requirements.

Complex ownership arrangements must be explained and supported by appropriate documentation.

7.11 Ultimate Beneficial Owner Due Diligence

The Company must obtain sufficient information to identify and verify each applicable ultimate beneficial owner.

Information should include:

- Full legal name.
- Date and place of birth.
- Nationality.
- Residential address.
- Nature and extent of ownership or control.
- Valid government-issued identification.
- Proof of residential address.

- Occupation or principal business activity.
- Source of wealth and source of funds where required by risk.
- PEP and sanctions status.
- Relevant adverse-media or enforcement information.

Where ownership or control is disputed, unclear, concealed, or materially inconsistent, the relationship must not be approved until the matter has been resolved.

7.12 Directors, Key Persons and Authorised Representatives

The Company must identify the Directors and relevant key persons associated with the relationship.

Due diligence may include:

- Identity verification.
- Position and authority.
- Professional background.
- Regulatory approvals.
- PEP and sanctions screening.
- Adverse-media review.
- Relevant criminal, civil, insolvency, or regulatory history.
- Verification of signing authority.

The Company must maintain a current list of persons authorised to:

- Act on behalf of the business partner.
- Submit contractual instructions.
- Request changes to domains, markets, products, or technical access.
- Change payment information.
- Receive confidential information.

Material or unusual instructions received from an unauthorised person must not be acted upon.

7.13 Licence and Regulatory Verification

The Company must independently verify any licence or authorisation relied upon by the business partner.

Verification should establish:

- The identity of the licence holder.

- The issuing authority.
- Licence number.
- Current status.
- Authorised activities.
- Authorised brands and domains.
- Applicable jurisdictions.
- Effective and expiry dates.
- Relevant conditions or restrictions.
- Any public warning, suspension, revocation, or enforcement action.
- Whether the proposed relationship falls within the licence scope.

Evidence of verification must be retained.

Where online verification is unavailable, the Company may request:

- A certified licence copy.
- Direct confirmation from the regulator.
- A legal opinion.
- Confirmation from a suitably qualified adviser.
- Additional corroborating evidence.

7.14 Brands, Domains and Websites

The Company must identify all brands, websites, and domains through which its content will be made available.

The review should consider:

- Ownership and control of the domain.
- Identity of the entity presented as the operator.
- Licensing information displayed.
- Terms and conditions.
- Privacy and responsible-gaming information.
- Restricted-country provisions.
- Contact and complaint information.
- Consistency between the website and the licence.
- Whether prohibited or misleading claims are made.
- Whether Bet Play B.V. or Babylon Gaming is described accurately.
- Whether the website appears to target unauthorised jurisdictions.
- Whether additional brands or mirror domains are being used.

Production access must be limited to approved entities, brands, domains, and distribution arrangements.

Any undisclosed domain or brand must be investigated promptly.

7.15 Market and Jurisdictional Assessment

The prospective business partner must disclose the jurisdictions in which it intends to operate or distribute gaming content.

The Company's assessment should consider:

- Whether the partner is authorised to operate in each jurisdiction.
- Whether B2B supplier authorisation is required.
- Whether the relevant games are permitted.
- Whether local certification is required.
- Whether the jurisdiction is prohibited or restricted by the Company, Babylon Gaming, or an upstream provider.
- Relevant sanctions.
- Regulatory warnings and blacklist entries.
- The partner's localisation, marketing, and distribution arrangements.
- Whether access restrictions or geolocation controls are expected.
- Whether local legal advice is required.
- Whether the market creates elevated AML/CFT/CPF or reputational risk.

Approval may be limited to specifically identified jurisdictions.

The business partner must not enter an additional market using the Company's content without any approval required under the agreement and the Company's procedures.

7.16 Distribution Model and Downstream Parties

The Company must establish whether the business partner will:

- Use the content directly.
- Integrate the content into its own licensed platform.
- Provide content to affiliated operators.
- Act as an aggregator.
- Act as a reseller.
- Sublicense or redistribute content.
- Provide services to white-label operators.
- Use another intermediary or technical provider.

Where a downstream party will receive or access the content, the Company must determine:

- The party's legal identity.
- Ownership and control.
- Regulatory status.
- Brands, domains, and markets.
- Position in the contractual chain.
- Whether the arrangement is permitted by Babylon Gaming or the relevant provider.
- Which entity is responsible for due diligence and monitoring.
- Whether Bet Play B.V. has sufficient information, audit, restriction, and termination rights.
- How unauthorised onward distribution will be prevented and identified.

Undisclosed onward distribution is prohibited.

7.17 Regulatory and Enforcement History

The prospective business partner must disclose material:

- Regulatory investigations.
- Formal warnings.
- Licence suspensions or revocations.
- Administrative sanctions.
- Fines or settlements.
- Criminal proceedings.
- Civil proceedings relevant to integrity or solvency.
- Insolvency or bankruptcy events.
- Refusals of gaming licences.
- Terminations by material suppliers for compliance reasons.
- Blacklist entries.
- Significant unresolved player or commercial disputes.
- Data-protection or information-security enforcement.

The Company must assess:

- The seriousness of the event.
- When it occurred.
- Whether it remains unresolved.
- The business partner's explanation.
- Corrective actions implemented.
- Whether similar conduct could affect the proposed relationship.
- Whether the matter was fully disclosed.
- Whether enhanced monitoring or contractual protections are required.

A historical issue does not automatically require rejection, but concealment of a material issue is itself a significant risk factor.

7.18 Adverse-Media and Reputation Review

The Company must conduct proportionate adverse-media screening concerning:

- The business partner.
- Parent and holding companies.
- Ultimate beneficial owners.
- Directors and relevant key persons.
- Material associated brands.

Relevant information may concern:

- Fraud or dishonesty.
- Money laundering or financial crime.
- Corruption or bribery.
- Organised crime.
- Sanctions evasion.
- Unlawful gambling.
- Regulatory breaches.
- Consumer abuse.
- Insolvency or serious financial misconduct.
- Cybercrime or material data breaches.
- Match-fixing or gaming-integrity concerns.
- Misuse or unauthorised distribution of gaming content.

Adverse information must be assessed for:

- Source reliability.
- Seriousness.
- Recency.
- Relevance.
- Whether allegations were substantiated.
- The subject's response.
- The existence of regulatory or judicial findings.

7.19 Sanctions and PEP Screening

The Company must screen relevant entities and persons against applicable sanctions and PEP information.

Screening should include, where relevant:

- The prospective business partner.
- Parent and intermediate entities.
- Ultimate beneficial owners.
- Directors.
- Authorised signatories.
- Relevant key persons.
- Known controlling persons.
- Payment counterparties.

Potential matches must be reviewed before the relationship proceeds.

A screening alert must not be dismissed solely because the name differs slightly. The review should consider identifying information such as:

- Date of birth.
- Nationality.
- Address.
- Identification number.
- Corporate registration number.
- Known aliases.
- Ownership and control.

Sanctions concerns must be referred immediately to the MLRO and handled in accordance with the AML/CFT Policy and applicable law.

PEP status does not automatically prohibit a relationship but may require enhanced due diligence and senior-management approval.

7.20 Source of Funds and Source of Wealth

Where required by the risk assessment, the Company must obtain information concerning:

- The source of funds used in the relationship.
- The commercial origin of payments.
- The source of the business partner's capital.
- The source of wealth of relevant ultimate beneficial owners.
- The relationship between the payer and contracting entity.
- The destination of payments made by the Company.
- Any financing or investment arrangements relevant to the relationship.

Evidence may include:

- Financial statements.
- Bank statements.
- Tax records.
- Corporate sale agreements.
- Dividend records.
- Investment agreements.
- Loan documents.
- Evidence of business income.
- Independent wealth reports.
- Other reliable supporting documents.

The extent of verification must reflect the risk and materiality of the relationship.

7.21 Financial Standing and Credit Risk

Where the Company will assume material financial exposure, the CFO should assess the business partner's financial standing.

The assessment may consider:

- Audited or management accounts.
- Cash-flow information.
- Credit reports.
- Insolvency records.
- Outstanding judgments.
- Payment history.
- Expected revenue and liability.
- Proposed credit terms.
- Deposit or security arrangements.
- Group support or guarantees.
- Concentration exposure.
- Existing overdue balances.
- Reliability of financial information provided.

Commercial approval must identify any:

- Credit limit.
- Prepayment requirement.
- Deposit.
- Payment frequency.
- Currency condition.

- Settlement restriction.
- Escalation threshold.
- Right to suspend services for non-payment.

7.22 Bank Accounts and Payment Instructions

Payments should ordinarily be made between accounts held in the names of the contracting parties.

Before accepting or making a material payment, the Company should verify:

- The account holder.
- The financial institution.
- The account jurisdiction.
- The relationship between the account holder and contracting party.
- The commercial purpose of the payment.
- Consistency with the contract and invoice.
- Any sanctions or high-risk jurisdictional concerns.

Payments involving an unrelated third party require documented review and approval.

Changes to bank or settlement instructions must be independently verified through an established contact using a reliable communication channel.

Personnel must remain alert to:

- Sudden changes in payment instructions.
- Requests for payment to personal accounts.
- Payments from unrelated entities.
- Overpayments followed by refund requests.
- Payments through multiple jurisdictions without a clear purpose.
- Use of opaque payment instruments.
- Pressure to bypass verification procedures.

7.23 Information Security and Data Protection Review

Where a business partner will exchange, access, process, or receive confidential, personal, regulatory, or technical information, the Company should assess:

- The information involved.
- The purpose and legal basis for processing.
- Access-control arrangements.

- Authentication and credential management.
- Encryption and secure transfer.
- Data location and international transfers.
- Retention and deletion.
- Incident and breach notification.
- Use of subcontractors.
- Audit and assurance evidence.
- Business-continuity arrangements.
- Contractual confidentiality and data-protection provisions.

Access must be limited to what is necessary for the approved relationship.

Production credentials must not be shared with an unauthorised affiliate, reseller, downstream operator, or service provider.

7.24 Business-Partner Risk Assessment

Each prospective business partner must receive a documented risk classification before approval.

The assessment must consider the factors established in Chapter 5, including:

- Entity and ownership risk.
- Regulatory risk.
- Jurisdictional risk.
- Product and distribution risk.
- AML/CFT/CPF risk.
- Sanctions and PEP exposure.
- Reputational risk.
- Financial and payment risk.
- Information-security risk.
- Operational and dependency risk.
- Contractual risk.
- Quality and transparency of the information provided.
- Involvement of Babylon Gaming and other upstream providers.

The assessment must identify:

- Inherent risk.
- Applicable controls.
- Control effectiveness.
- Residual risk.
- Required approval level.

- Review frequency.
- Conditions or restrictions.
- Any unresolved dependencies.

7.25 Risk Classification

Business partners should ordinarily be classified as low, standard, high, or unacceptable risk.

Classification	General characteristics	Typical response
Low	Transparent ownership, reputable regulated activity, low-risk jurisdictions, straightforward distribution, and no material adverse indicators.	Standard due diligence with proportionate monitoring.
Standard	Ordinary regulated B2B relationship presenting manageable regulatory, operational, and financial risks.	Full standard due diligence and periodic review.
High	Complex ownership, higher-risk jurisdictions, PEP exposure, adverse history, onward distribution, unusual payments, weak transparency, or other elevated risk factors.	Enhanced due diligence, senior approval, conditions, and more frequent monitoring.
Unacceptable	Prohibited activity, unverifiable identity or ownership, unlawful markets, material sanctions concerns, fraudulent information, or risks that cannot be adequately controlled.	Reject, suspend, or terminate the relationship.

Risk classification must not be based solely on a numerical score where qualitative factors indicate a higher level of concern.

7.26 Enhanced Due Diligence

Enhanced due diligence must be applied where higher risk is identified.

Enhanced measures may include:

- Additional corporate and ownership documentation.
- Independent verification of ownership and control.
- More detailed source-of-funds or source-of-wealth evidence.

- Additional licence and market verification.
- Local legal opinions.
- Direct confirmation from a regulator.
- Detailed review of regulatory and enforcement history.
- Expanded adverse-media research.
- Verification of operational premises.
- Interviews with Directors, UBOs, or key persons.
- Review of audited financial information.
- More detailed assessment of downstream parties.
- Approval from Babylon Gaming or upstream providers.
- Stronger contractual protections.
- Restricted markets, products, domains, or distribution rights.
- Shorter review periods.
- Enhanced transaction or activity monitoring.
- Approval by the Director.

The reason for applying enhanced due diligence and the resulting conclusion must be documented.

7.27 Reliance on Third-Party Due Diligence

The Company may use information or due-diligence support provided by Babylon Gaming, professional advisers, corporate-service providers, screening providers, or other competent parties.

Before relying on such information, the Company must consider:

- The provider's competence and reliability.
- The scope of the checks performed.
- The date of the information.
- The sources used.
- Whether underlying documents are available.
- Whether the information satisfies the Company's requirements.
- Whether relevant gaps or inconsistencies remain.
- Whether reliance is permitted under applicable requirements.

The Company remains responsible for determining whether the relationship is acceptable.

7.28 Incomplete or Inconsistent Information

Where information is missing, outdated, inconsistent, or unclear, the Company must:

- Identify the deficiency.
- Request clarification or additional evidence.
- Assess whether the issue increases the risk.
- Restrict progress until the matter is resolved.
- Escalate suspected concealment or falsification.
- Consider rejecting the proposal where satisfactory information cannot be obtained.

Commercial urgency is not a valid reason to disregard missing due-diligence information.

7.29 Compliance Approval

The Compliance Officer must document whether:

- Due diligence has been completed.
- Identity, ownership, and control have been established.
- Required licences have been verified.
- Markets, brands, domains, and distribution arrangements are acceptable.
- Screening has been completed.
- Material adverse information has been assessed.
- The risk classification is appropriate.
- Enhanced due diligence has been completed where required.
- Babylon Gaming or another provider has approved the arrangement.
- Conditions or restrictions are necessary.
- The relationship may proceed.

Compliance approval must be dated and attributable to the approving person.

Compliance approval does not replace contractual, financial, technical, or management approval.

7.30 Management Approval

The Director must approve:

- Higher-risk business partners.
- Material new distribution models.
- Reseller or onward-distribution arrangements.
- Materially complex ownership structures.
- Relationships involving significant PEP or reputational exposure.
- Material exceptions to standard requirements.
- Relationships presenting substantial financial or concentration risk.

- Relationships requiring significant conditions or enhanced monitoring.
- Any proposal referred by the Compliance Officer or MLRO.

The approval must record:

- The decision.
- The reasons for the decision.
- Conditions imposed.
- Persons responsible for implementing the conditions.
- Review or expiry dates.
- Any dissenting compliance recommendation.
- Any requirement for external advice or assurance.

The Director must not approve a relationship where doing so would breach applicable law, sanctions, or the Company's licence.

7.31 Conditional Approval

A relationship may be approved subject to documented conditions.

Conditions may include:

- Receipt of specified documents.
- Confirmation of licence status.
- Restriction to approved jurisdictions.
- Restriction to approved brands and domains.
- Prohibition of onward distribution.
- Exclusion of specified content.
- Completion of enhanced due diligence.
- Advance payment or security.
- Additional reporting.
- More frequent review.
- Technical access restrictions.
- Approval of each downstream party.
- Confirmation from Babylon Gaming.
- Amendment of contractual terms.
- Completion of specified information-security measures.

Conditions that must be satisfied before activation must be clearly distinguished from conditions that apply during the relationship.

7.32 Contract Execution

Before activation, the Company must confirm that an appropriate written agreement has been executed.

The agreement should address, where relevant:

- Identity of the parties.
- Nature and scope of the services.
- Approved content.
- Approved jurisdictions.
- Brands and domains.
- Distribution and onward-distribution restrictions.
- Licensing responsibilities.
- Compliance with applicable laws.
- Due-diligence and information obligations.
- Audit and inspection rights.
- Regulatory cooperation.
- Payment and settlement terms.
- Intellectual-property rights.
- Confidentiality and data protection.
- Information-security obligations.
- Incident and breach notification.
- Service suspension.
- Termination rights.
- Recordkeeping.
- Subcontracting.
- Governing law and dispute resolution.
- Babylon Gaming or upstream-provider restrictions.

The contracting entity must match the entity approved through due diligence unless a documented reassessment is completed.

7.33 Pre-Activation Checklist

Before a business partner is activated, the responsible persons must confirm that:

- Required due diligence is complete.
- The business-partner risk assessment is complete.
- Compliance clearance has been recorded.
- AML/CFT/CPF and sanctions concerns have been resolved.
- Required financial approval has been obtained.
- Management approval has been obtained where required.
- Babylon Gaming or upstream-provider approval has been obtained.
- The agreement has been executed.

- Approved markets, brands, domains, products, and distribution rights are recorded.
- Pre-activation conditions have been completed.
- Payment and invoicing details have been verified.
- Technical access is limited to the approved scope.
- Internal relationship ownership has been assigned.
- Monitoring and review requirements are recorded.
- Relevant records have been stored in the approved location.

Activation must be traceable to an identified authorising person and date.

7.34 Technical and Operational Activation

Technical activation must reflect the approved commercial and compliance scope.

The Company must coordinate with Babylon Gaming or the relevant provider to ensure, where applicable, that:

- The correct legal entity is activated.
- Only approved brands and domains are enabled.
- Approved markets and product restrictions are applied.
- Credentials are issued to authorised persons.
- Production and test access are appropriately separated.
- Access rights follow least-privilege principles.
- Required integration testing is completed.
- Technical contacts and escalation routes are recorded.
- Monitoring and incident arrangements are understood.
- Unapproved downstream access is prevented.
- Activation evidence is retained.

Technical capability must not be enabled merely because commercial terms have been agreed.

7.35 Business-Partner File

The Company must maintain a file for each business partner containing, where applicable:

- Initial proposal information.
- Corporate documents.
- Ownership and control information.
- UBO documentation.
- Director and authorised-person information.

- Licensing evidence.
- Market, brand, and domain information.
- Screening results.
- Adverse-media assessments.
- Source-of-funds and financial information.
- Risk assessments.
- Enhanced due-diligence records.
- Compliance approval.
- Management approval.
- Babylon Gaming or provider approval.
- Executed agreements.
- Conditions and restrictions.
- Pre-activation checklist.
- Technical activation evidence.
- Periodic and event-driven reviews.
- Monitoring records.
- Material correspondence.
- Incident, breach, suspension, and termination records.

The file must provide a clear audit trail from initial proposal through termination.

7.36 Ongoing Monitoring

The Company must monitor business partners throughout the relationship.

Monitoring should determine whether:

- The business partner remains active and in good standing.
- Ownership and control remain unchanged.
- Required licences remain valid.
- Approved brands and domains remain accurate.
- The partner continues to operate only in approved markets.
- Distribution remains within the approved contractual chain.
- Payment activity remains consistent with expectations.
- Approval conditions continue to be satisfied.
- Material adverse or regulatory information has arisen.
- Complaints or incidents indicate a control weakness.
- The partner remains compatible with the Company's risk appetite.
- Babylon Gaming or an upstream provider has imposed new restrictions.
- The relationship remains commercially and operationally viable.

The frequency and depth of monitoring must reflect the risk classification.

7.37 Periodic Review

Business-partner files must be reviewed periodically.

As an internal risk-based standard, reviews should ordinarily occur:

- At least every three years for low-risk relationships.
- At least every two years for standard-risk relationships.
- At least annually for high-risk relationships.
- More frequently where required by the risk assessment, applicable law, contractual conditions, or management decision.

The review should confirm:

- Current corporate status.
- Ownership and control.
- Directors and authorised persons.
- Licensing status.
- Brands and domains.
- Markets and distribution arrangements.
- Screening results.
- Regulatory and enforcement history.
- Financial and payment information.
- Outstanding conditions.
- Incidents, disputes, and complaints.
- Continued accuracy of the risk classification.
- Whether the relationship should continue, be restricted, or be terminated.

These internal intervals may be shortened where regulatory or AML/CFT requirements require more frequent review.

7.38 Event-Driven Review

A business partner must be reviewed before the next scheduled date where the Company becomes aware of:

- A change in ownership or control.
- A change in Directors or key persons.
- A change in licence status.
- Entry into a new jurisdiction.
- Addition of a new brand or domain.
- A proposed change to the distribution model.
- Appointment of a reseller or downstream party.

- Material regulatory action or adverse media.
- A sanctions or PEP alert.
- A significant change in payment arrangements.
- An unexplained third-party payment.
- A material information-security incident.
- A serious complaint or contractual dispute.
- Suspected unauthorised distribution.
- Material deterioration in financial standing.
- A request for materially different products or services.
- A material change involving Babylon Gaming or another provider.
- Information suggesting that previous due diligence was inaccurate or incomplete.

The Company may restrict or suspend the relationship while the review is completed.

7.39 Change Notification Obligations

Business partners should be contractually required to notify the Company promptly of material changes, including:

- Ownership and control.
- Directors and authorised representatives.
- Licence status.
- Regulatory investigations or enforcement.
- Brands and domains.
- Operating jurisdictions.
- Distribution arrangements.
- Downstream parties.
- Bank-account details.
- Insolvency or material financial distress.
- Security or data breaches relevant to the relationship.
- Any event affecting the accuracy of information previously provided.

Failure to provide required notification must be treated as a compliance and contractual concern.

7.40 Screening Refresh

Sanctions, PEP, and adverse-media screening must be refreshed:

- At periodic review.
- Following a material ownership or management change.

- When a new authorised representative is appointed.
- Before approving a higher-risk market or distribution change.
- When adverse information is received.
- At any additional frequency required by the business partner's risk classification.

Potential matches and material findings must be documented and resolved.

7.41 Monitoring of Licences, Domains and Markets

The Company should maintain a current record of:

- Each business partner's relevant licences.
- Licence status and expiry dates.
- Approved brands.
- Approved domains.
- Approved markets.
- Approved distribution rights.
- Downstream parties.
- Restrictions and conditions.

Monitoring may include:

- Regulatory-register checks.
- Website reviews.
- Domain and brand verification.
- Review of business-partner reports.
- Information provided by Babylon Gaming.
- Review of technical or operational information available to the Company.
- Adverse-media and regulatory-alert monitoring.
- Investigation of complaints or suspicious activity.

7.42 Warning Indicators

Warning indicators requiring review may include:

- Reluctance to provide ownership information.
- Frequent changes in corporate structure.
- Use of nominees without a clear legitimate explanation.
- Information inconsistent with public records.
- Unverified or misleading licensing claims.
- Use of unapproved domains.
- Activity in undisclosed markets.

- Undisclosed resellers or downstream parties.
- Instructions from unauthorised persons.
- Requests to conceal the identity of the operator.
- Unusual urgency to activate before due diligence is complete.
- Attempts to bypass Babylon Gaming's conditions.
- Payments from unrelated third parties.
- Sudden changes to bank instructions.
- Repeated overdue invoices.
- Significant regulatory or consumer complaints.
- Material adverse media.
- Website content inconsistent with contractual or regulatory requirements.
- Refusal to explain business or payment arrangements.
- Possible falsification or alteration of documents.
- Attempts to reactivate a previously rejected party through another entity.

The existence of one indicator does not necessarily establish misconduct, but it must be assessed proportionately.

7.43 Business-Partner Complaints and Disputes

Complaints or disputes involving a business partner must be recorded and assessed where they may indicate:

- Regulatory non-compliance.
- Misuse of content.
- Unauthorised distribution.
- Misrepresentation.
- Payment irregularity.
- Information-security weakness.
- Failure to observe contractual restrictions.
- Repeated operational deficiencies.
- Harm to the Company's licence or reputation.

Material matters must be escalated to the Director and Compliance Officer.

Where the matter involves suspected financial crime, it must also be referred to the MLRO.

7.44 Restriction and Suspension

The Company may restrict or suspend a relationship where:

- Required due-diligence information becomes outdated or unreliable.

- A licence cannot be verified.
- A material change has not been approved.
- A sanctions or financial-crime concern arises.
- Unauthorised markets or domains are identified.
- Onward distribution is suspected.
- Babylon Gaming or an upstream provider requests suspension.
- A serious contractual breach occurs.
- Material payments remain overdue.
- A regulatory authority raises a concern.
- Continued operation could increase the Company's exposure.

Restriction or suspension measures may include:

- Withholding new content.
- Preventing new domains or brands from being added.
- Disabling technical access.
- Limiting specified markets.
- Suspending commercial or technical support.
- Requiring advance payment.
- Freezing non-essential changes.
- Coordinating service suspension with Babylon Gaming.
- Requiring additional due diligence before reinstatement.

The decision, scope, responsible persons, and conditions for reinstatement must be documented.

7.45 Rejection and Termination

A prospective or existing relationship may be rejected or terminated where:

- Due diligence cannot be completed.
- Material information is false or misleading.
- Ownership or control is concealed.
- Required authorisation is absent or lost.
- The relationship involves prohibited activity or jurisdictions.
- Sanctions or unacceptable financial-crime concerns arise.
- Unauthorised onward distribution occurs.
- Material contractual restrictions are repeatedly breached.
- The business partner refuses to implement required controls.
- Babylon Gaming or an upstream provider withdraws approval.
- The residual risk becomes unacceptable.

- Continuing the relationship may threaten the Company's licence, reputation, financial position, or operations.

Termination must be coordinated with the relevant operational, financial, legal, compliance, and technical functions.

The Company must consider:

- Contractual termination provisions.
- Regulatory or contractual notification.
- Suspension of access and credentials.
- Outstanding invoices and obligations.
- Return or deletion of information.
- Preservation of relevant records.
- Notification to Babylon Gaming.
- Whether suspicious-activity reporting must be considered.
- Whether the relationship may be reconsidered in the future.

7.46 Reinstatement

A suspended or terminated relationship must not be reinstated without a documented reassessment.

The reassessment must confirm:

- The reason for suspension or termination.
- Corrective actions completed.
- Updated due diligence.
- Current licence status.
- Current ownership and control.
- Resolution of regulatory, sanctions, financial, or contractual concerns.
- Approval from Babylon Gaming or another provider.
- Compliance clearance.
- Management approval where required.
- Any additional conditions or monitoring requirements.

Previous approval must not be relied upon where the circumstances have materially changed.

7.47 Exceptions

Any proposed exception to the Company's normal onboarding requirements must:

- Be documented.
- State the requirement affected.
- Explain the legitimate reason for the exception.
- Assess the resulting risk.
- Identify compensating controls.
- Specify its duration.
- Receive approval from the Compliance Officer and Director.
- Be reviewed before expiry.

An exception must not permit:

- Breach of law or licence conditions.
- Circumvention of sanctions.
- Activation of an unidentified party.
- Deliberate concealment of ownership or control.
- Activity outside the Company's contractual rights.
- Suppression of suspicious-activity concerns.

7.48 Recordkeeping and Retention

Business-partner due-diligence records must be:

- Accurate and complete.
- Dated and attributable.
- Legible and retrievable.
- Protected against unauthorised access, loss, or alteration.
- Maintained throughout the relationship.
- Retained after termination for the period required by applicable legal, regulatory, contractual, and internal requirements.

Superseded documents should be retained where necessary to demonstrate the information relied upon at the time of approval or review.

Access to sensitive identification, screening, and financial-crime information must be restricted to authorised persons.

7.49 Data Protection and Confidentiality

Personal information obtained during due diligence must be processed lawfully and only for legitimate purposes.

The Company must:

- Collect only information reasonably required.
- Protect identification and ownership records.
- Restrict access according to role.
- Use secure methods for document transfer and storage.
- Avoid unnecessary circulation of personal information.
- Retain information only for the required period.
- Respond appropriately to data-security incidents.
- Ensure providers processing due-diligence information are subject to suitable obligations.

Information concerning suspicious-activity reports must be subject to additional confidentiality protections.

7.50 Training

Personnel involved in onboarding or managing business partners must receive training appropriate to their responsibilities.

Training should address:

- Onboarding stages and approval requirements.
- Corporate and UBO identification.
- Licence verification.
- Market and jurisdictional assessment.
- Sanctions and PEP awareness.
- Adverse-media review.
- Source-of-funds and payment risks.
- Onward-distribution risks.
- Warning indicators.
- Escalation procedures.
- Recordkeeping and confidentiality.
- Prohibition on activation before approval.
- The respective roles of Bet Play B.V. and Babylon Gaming.

Training must be refreshed when requirements or procedures materially change.

7.51 Quality Assurance and Monitoring

The Compliance Officer should perform periodic checks of business-partner files to confirm:

- Required documents are present and current.
- Ownership has been properly identified.

- Licences were independently verified.
- Screening was completed and resolved.
- Risk classifications are supported.
- Enhanced due diligence was applied where required.
- Approvals are complete.
- Conditions were implemented.
- Activation occurred only after clearance.
- Review dates are being monitored.
- Material changes were assessed.
- Records are complete and appropriately protected.

Deficiencies must be recorded and addressed through corrective action.

7.52 Management Information

Management information may include:

- Prospective partners awaiting documentation.
- Applications awaiting compliance clearance.
- Applications rejected or withdrawn.
- Business partners by risk classification.
- Higher-risk relationships.
- Reviews due or overdue.
- Expired or unverified licences.
- Outstanding approval conditions.
- New markets, brands, or domains awaiting approval.
- Suspected unauthorised distribution.
- Sanctions, PEP, and adverse-media alerts.
- Suspended or terminated relationships.
- Overdue receivables and unusual payment matters.
- Material issues involving Babylon Gaming.
- Open corrective actions.

Urgent or material concerns must be reported immediately rather than waiting for periodic reporting.

7.53 Independent Review

The Company may obtain independent review of its business-partner onboarding arrangements where:

- The relationship is particularly complex or high risk.

- Ownership or control is difficult to establish.
- Specialist market or regulatory advice is required.
- A material conflict of interest exists.
- Serious onboarding deficiencies have been identified.
- Regulatory assurance is requested.
- Internal competence or resources are insufficient.
- Management wishes to verify that remedial actions are effective.

The reviewer's scope, findings, recommendations, management response, and corrective actions must be documented.

7.54 Review of the Onboarding Framework

The Director, Compliance Officer, and MLRO must review this framework at least annually and following any material change.

The review should consider:

- Changes to Curaçao legislation, CGA requirements, or licence conditions.
- Changes to the Company's business model.
- Changes involving Babylon Gaming or upstream providers.
- New markets, products, or distribution models.
- Onboarding and monitoring findings.
- Rejected, suspended, and terminated relationships.
- Regulatory, sanctions, and adverse-media developments.
- Incidents involving unauthorised distribution.
- The adequacy of risk classifications and review frequencies.
- The effectiveness of approval and activation controls.
- The completeness and quality of business-partner files.
- Training and resource requirements.
- Consistency with the AML/CFT Policy and Chapters 5 and 6.
- Whether documented procedures reflect actual practice.

Material amendments must be approved by the Director and communicated to all affected personnel.

Business- Partner Complaints and Dispute Resolution

8

Chapter 8 – Business-Partner Complaints and Dispute Resolution

8.1 Purpose

This chapter establishes Bet Play B.V.'s framework for receiving, recording, investigating, resolving, escalating, and monitoring complaints and disputes arising from its B2B activities.

The objectives are to ensure that:

- Business-partner complaints are handled fairly, consistently, promptly, and transparently.
- Complaints are distinguished from routine operational support requests.
- Material allegations are investigated objectively.
- Relevant contractual, technical, financial, and operational evidence is preserved.
- Responsibilities between Bet Play B.V., Babylon Gaming, business partners, and other providers are clearly identified.
- Complaints involving regulatory, AML/CFT/CPF, sanctions, information-security, data-protection, fraud, or integrity concerns are escalated appropriately.
- Contractual disputes are resolved internally where reasonably possible.
- External dispute-resolution procedures are used where required.
- Complaint information is used to identify recurring problems and improve controls.
- Complete records and management information are maintained.

Complaint handling must not be influenced improperly by commercial pressure, the value of a business relationship, or the identity of the complainant.

8.2 B2B Operating Context

Bet Play B.V. operates exclusively on a B2B basis. The Company does not contract directly with players, operate player accounts, accept player deposits, process player withdrawals, settle player transactions, provide player-facing customer support, determine player complaints, or act as an alternative dispute-resolution provider for players.

For this chapter, a customer means a contracted or prospective business customer, including an operator, aggregator, platform provider, reseller, distributor, or other commercial counterparty.

The relevant B2C operator remains responsible for complaints submitted by its players. Bet Play B.V.'s role is limited to providing appropriate technical or factual assistance where a complaint concerns its gaming content, systems, integration, or conduct.

8.3 Scope

This chapter applies to complaints and disputes received from or concerning contracted and prospective business partners, licensed gaming operators, aggregators, platform providers, resellers, distributors, Babylon Gaming, other upstream content or technology providers, suppliers, service providers, regulators, public authorities, and other commercial counterparties affected by the Company's activities.

Complaints and disputes may concern contractual performance; integration or service delivery; gaming-content availability; game configuration or malfunction; technical records or reporting; service levels; licensing or regulatory status; authorised markets, brands, or domains; suspected unauthorised distribution; intellectual-property use; invoicing and commercial settlement; information security; data protection; conduct of personnel or representatives; restriction, suspension, or termination of services; or any other matter capable of exposing the Company to regulatory, legal, financial, operational, or reputational risk.

8.4 Applicable Framework

Complaint handling must be consistent with applicable Curaçao legislation; requirements and guidance of the Curaçao Gaming Authority; Bet Play B.V.'s licence conditions; applicable civil, commercial, and data-protection law; the Company's contracts; Babylon Gaming's applicable requirements; requirements of other upstream providers; applicable market-specific requirements; and the Company's policies and procedures.

Where requirements differ, the Company must follow the appropriate legal and contractual standard. Material uncertainty must be referred to the Compliance Officer and, where necessary, external legal counsel.

8.5 Complaint-Handling Principles

8.5.1 Accessibility

Business partners must have a reasonably accessible means of raising complaints. Complaints may be received through an account manager, support channel, contractual notice address, or other legitimate channels.

8.5.2 Fairness

Complaints must be considered impartially and on their individual facts. The person whose conduct or decision is the subject of a complaint must not be solely responsible for determining the outcome.

8.5.3 Promptness

Complaints must be acknowledged, investigated, and resolved without unreasonable delay. Urgent matters must be prioritised according to their actual and potential impact.

8.5.4 Transparency

The complainant should be informed how the complaint will be handled, what information is required, the anticipated response time, any material delay, the final outcome, and any available internal or contractual escalation process.

8.5.5 Proportionality

The nature and extent of an investigation must reflect the seriousness, complexity, and potential consequences of the matter.

8.5.6 Confidentiality

Complaint information must be disclosed only to persons who require it for investigation, resolution, oversight, legal advice, contractual coordination, or regulatory reporting.

8.5.7 Non-Retaliation

A business partner or other person must not suffer retaliation for submitting a complaint in good faith or cooperating with an investigation. This does not prevent legitimate contractual remedies where misconduct, breach, or unacceptable risk is independently established.

8.5.8 Evidence-Based Decisions

Complaint outcomes must be supported by relevant facts, records, technical findings, contractual provisions, and applicable requirements.

8.5.9 Continuous Improvement

Complaint information must be used to identify recurring problems, control weaknesses, and opportunities for corrective action.

8.6 Definitions

Customer interaction: A routine B2B communication seeking information, clarification, assistance, or operational support that does not express material dissatisfaction requiring formal resolution.

Complaint: An oral or written expression of dissatisfaction concerning the Company, its personnel, services, content, conduct, decisions, or contractual performance where a response or remedy is expected. The word “complaint” need not be used.

Formal complaint: A complaint submitted through a designated or contractual channel, expressly identified as formal, incapable of resolution through routine support, presenting a material concern, or requiring a documented investigation and determination.

Dispute: A complaint or disagreement that remains unresolved and has been escalated internally or through contractual, mediation, arbitration, judicial, or other external dispute-resolution processes.

Player complaint: A complaint made by or for a player concerning a player account, gaming participation, deposit, withdrawal, transaction, bonus, operator decision, or other player-facing matter. Player complaints are not determined by Bet Play B.V.

Root cause: The underlying failure, weakness, act, omission, decision, or condition that caused or materially contributed to the complaint.

8.7 Roles and Responsibilities

8.7.1 Director

The Director oversees the framework; reviews material or higher-risk complaints; approves significant remedies, settlements, and corrective actions; protects the process from improper commercial influence; determines the Company’s position in

material disputes; authorises external advice or specialist investigation; ensures adequate resources; and reviews management information.

8.7.2 Compliance Officer

The Compliance Officer coordinates the framework; maintains or oversees the complaint register; classifies and triages complaints; identifies regulatory and licence implications; escalates material matters; monitors deadlines; reviews investigations; coordinates regulatory communication; monitors corrective action; analyses trends; conducts quality assurance; and maintains relevant records.

8.7.3 MLRO

The MLRO is responsible for complaints involving suspected money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, or related suspicious corporate or financial activity. The MLRO determines internal or external reporting and any communication restriction needed to avoid tipping off. Personnel must not disclose whether a suspicious-activity report has been or may be submitted.

8.7.4 Finance Function

Finance assists with complaints involving invoices, commercial settlement calculations, bank instructions, corporate payments made or received, credits, overpayments, reconciliations, receivables, and financial irregularities. This does not extend to player deposits, withdrawals, or gaming transactions.

8.7.5 Account Management

Account Management must recognise and forward complaints promptly, provide relationship and contractual information, communicate professionally, avoid premature promises, support approved remedies, and escalate repeated or material concerns. It must not suppress or reclassify a material complaint to avoid escalation.

8.7.6 Technical and Operational Personnel

Technical and operational personnel must preserve system and integration information; investigate content, configuration, integration, or service failures; provide accurate findings; coordinate with Babylon Gaming and other providers; identify affected products, versions, partners, domains, markets, and periods;

support containment and remediation; and retain evidence of testing and conclusions.

8.7.7 All Personnel

All personnel must recognise and report complaints, preserve relevant records, cooperate with investigations, avoid altering evidence, maintain confidentiality, and escalate urgent or material matters immediately.

8.8 Complaint Channels

Complaints may arrive through a designated email address, business-partner support, account managers, contractual notice channels, the Company's website, telephone or video calls, Babylon Gaming or another provider, a regulator, a public authority, a legal representative, or another business communication.

An informally received complaint must be transferred promptly. Where initially oral, the recipient must create a written record and may ask the complainant to confirm material facts.

8.9 Distinguishing Support Requests from Complaints

A matter must be treated as a complaint when it expresses material dissatisfaction; alleges error, failure, unfairness, or breach; requests compensation or another remedy; challenges a decision; alleges loss or harm; concerns legal, licence, or contractual compliance; remains unresolved after routine support; or indicates intended escalation to a regulator, lawyer, arbitrator, or court.

Uncertain cases should be recorded and referred for classification.

8.10 Complaints Involving Babylon Gaming or Other Providers

Where a complaint concerns content, systems, records, or responsibilities controlled by Babylon Gaming or another provider, Bet Play B.V. must record it, identify each party's responsibilities, preserve available information, refer relevant issues through approved channels, specify what is required, monitor the response, avoid unsupported conclusions, coordinate the response to the complainant, escalate delay or inconsistency, and record corrective action.

Referral does not remove Bet Play B.V.'s responsibility to manage its business relationship and fulfil its own obligations.

8.11 Complaint Registration

Each formal complaint must be entered promptly in the complaint register. The record should include a unique reference; receipt date and channel; complainant and partner details; contract or account reference; relevant brand, domain, market, or jurisdiction; event date; category; description; requested remedy; products, games, integrations, systems, invoices, or services involved; disputed amount; responsible person; priority; target dates; evidence; referrals; findings; outcome; remedy; closure date; root cause; and wider control implications.

The register must distinguish routine support interactions, formal B2B complaints, contractual disputes, misdirected player communications, and regulatory or enforcement matters.

8.12 Initial Assessment and Triage

The responsible person must assess whether the matter falls within the Company's responsibility; whether Babylon Gaming or another entity must participate; the complainant's authority; seriousness and urgency; risk of continuing harm; reporting obligations; AML/CFT/CPF, sanctions, fraud, security, privacy, or criminal concerns; risk of evidence loss; need for legal advice or privilege; related matters; and need for interim restriction or suspension. The assessment and actions must be documented.

8.13 Priority Classification

Priority	General characteristics	Required response
Routine	Limited impact, straightforward facts, no material regulatory or financial concern.	Ordinary investigation and response.
Significant	Material service, contractual, technical, invoicing, or repeated operational issue.	Prompt investigation with management or Compliance oversight.
Urgent	Potential continuing harm, serious service failure, suspected unauthorised distribution, security	Immediate escalation and consideration of containment.

	incident, or material financial exposure.	
Critical	Suspected serious regulatory breach, systemic content failure, fraud, sanctions or financial-crime concern, major data incident, or threat to the licence.	Immediate escalation to the Director and Compliance Officer, with specialist involvement as applicable.

Classification must consider actual and potential impact.

8.14 Acknowledgement

Unless a shorter contractual or regulatory period applies, a formal complaint should be acknowledged within seven calendar days. The acknowledgement should confirm receipt, give the reference, identify the responsible contact, summarise the matter, explain the process and anticipated response time, request necessary information, and explain any third-party involvement.

8.15 Verification of Authority

Before disclosing confidential information or implementing a remedy, the Company must verify identity and authority proportionately. A representative may be required to prove authority. Verification must not create an unnecessary obstacle. Anonymous information may still require investigation when it raises credible regulatory, integrity, security, or financial-crime concerns.

8.16 Investigation Planning

For significant, urgent, critical, or complex complaints, an investigation plan should identify the issues; applicable legal, regulatory, contractual, financial, and technical criteria; evidence; persons and entities to consult; responsibilities; target dates; interim controls; provider dependencies; external expertise; and communication arrangements. The substance, not merely the wording, must be addressed.

8.17 Evidence Collection and Preservation

Evidence may include contracts, amendments, service-level agreements, policies, correspondence, tickets, technical and integration logs, content versions,

configuration records, testing and certification, release and change records, incident reports, invoices, credits, B2B settlement records, website or domain captures, provider communication, regulatory correspondence, interviews, and witness accounts.

Evidence must be reliable, retrievable, access-restricted, and protected against alteration. Information controlled by another party must be requested promptly.

8.18 Independence and Conflicts of Interest

Actual or potential conflicts must be disclosed. The matter must be reassigned where practicable, independent oversight introduced, mitigation documented, and external review considered if adequate internal independence is unavailable. A person whose conduct is reviewed may give evidence but must not determine the final outcome.

8.19 Communication During Investigation

Proportionate updates should be provided when an investigation is complex, information remains outstanding, another party must respond, the target date changes, interim action is taken, or material delay arises.

Communications must be accurate, professional, clear, confidentiality-compliant, and non-speculative. Personnel must not admit liability, offer compensation, or make binding commitments without authority.

8.20 Resolution Timeframes

The Company should aim to give a final response within four weeks. If complexity, unavailable information, provider dependency, or another legitimate reason requires more time, the delay and reason must be documented; the complainant informed before the original deadline where practicable; a revised target given; and the case actively monitored.

An extension should not ordinarily exceed a further four weeks unless exceptional circumstances or a contractual dispute process justify longer. A shorter legal, regulatory, contractual, incident, or reporting deadline prevails.

8.21 Technical and Content-Related Complaints

An investigation should identify the game or content, version, partner, brand, domain, event date and time, session or round identifiers, market, jurisdiction, currency, configuration, integration settings, expected approved behaviour, log completeness, releases or changes, wider impact, certification or testing needs, provider involvement, and any reportable incident.

The Company must not alter records, recreate an event without preserving original evidence, issue a definitive conclusion before required investigation, or attribute responsibility without evidence.

8.22 Game Malfunctions Escalated by Operators

Where a player complains to a B2C operator about an alleged game malfunction and the operator escalates the matter to Bet Play B.V., the operator remains responsible for communicating with the player and determining the player complaint. Bet Play B.V. is responsible for investigating matters within its control and providing the operator with accurate, timely, and appropriately evidenced technical findings.

The operator's escalation should include, where available:

- Operator, brand, domain, and jurisdiction.
- Game name, game identifier, and version.
- Date and time of the event, including time zone.
- Player reference in pseudonymised form where practicable.
- Session, game-round, and transaction identifiers.
- Currency, stake, result, and amount disputed.
- Description of the alleged malfunction.
- Relevant screenshots, recordings, error messages, and correspondence.
- Operator-platform and aggregator logs.
- Game rules and configuration applicable at the time.
- Any immediate action already taken.
- The response deadline applicable to the player complaint.

Bet Play B.V. must record the escalation and promptly:

- Assign a case reference and responsible investigator.
- Acknowledge receipt to the operator.
- Assess severity and possible extent.
- Preserve relevant logs, versions, configurations, releases, and other evidence.
- Confirm whether sufficient information has been supplied.
- Coordinate with Babylon Gaming or another provider where necessary.

- Determine whether the affected game should be monitored, restricted, or temporarily disabled.
- Identify whether other operators, players, markets, or rounds may be affected.
- Assess whether the matter is a reportable technical or regulatory incident.
- Give the operator progress updates and a reasoned technical response.

The investigation must determine, so far as reasonably possible:

- Whether the disputed round was accepted and completed.
- Whether the recorded outcome was generated and transmitted correctly.
- Whether the game operated according to its approved rules, mathematics, configuration, and certified version.
- Whether interruption, communication failure, timeout, duplicate instruction, corrupted message, or integration error occurred.
- Whether the operator platform, an intermediary, Bet Play B.V., Babylon Gaming, or another provider contributed.
- Whether the original result can be established reliably from preserved records.
- Whether the issue was isolated or wider.
- Whether corrective action, wider reconciliation, notification, or suspension is required.

Technical records from different systems must be reconciled where practicable. Any inconsistency, missing record, or limitation affecting reliability must be stated clearly.

Bet Play B.V.'s response to the operator should include the case reference; records examined; technical findings; whether a malfunction was confirmed, not identified, or indeterminate; systems or parties involved where evidenced; affected rounds, products, versions, operators, or periods; containment or corrective action; uncertainties; outstanding investigation or provider input; and whether regulatory or contractual notification should be considered.

Bet Play B.V. must not communicate directly with the player unless specifically authorised and legally appropriate; determine the player complaint or promise a refund; recommend rejection based only on one system log; alter, regenerate, or overwrite original evidence; attribute responsibility without adequate evidence; close the escalation merely because it was referred to a provider; or delay notification of a potentially systemic or reportable malfunction while awaiting final root cause.

The operator remains responsible for applying its player-facing terms, regulatory requirements, complaint procedure, and rules for interrupted, void, incomplete, or malfunctioning rounds. Bet Play B.V. may recommend a technical or contractual

remedy but must not make the player-facing decision unless expressly required by agreement and permitted by law.

Where a malfunction is confirmed or reasonably suspected, Bet Play B.V. must consider immediate containment; temporary suspension; identification of all potentially affected operators and rounds; reconciliation or replay analysis using preserved data; notification to Babylon Gaming, affected partners, regulators, or testing laboratories where required; controlled correction, rollback, or release; independent testing or recertification; root-cause analysis; preventive action; and verification before normal operation resumes.

Each case must remain traceable to the operator complaint, technical incident, provider referral, corrective action, and final conclusion. Repeated complaints involving the same game, version, error, integration, or operating condition must be assessed collectively as a possible systemic incident.

8.23 Commercial and Invoicing Complaints

Finance must investigate invoice, commercial-calculation, or corporate-payment complaints against the contract and commercial terms, period, source data, currency and exchange rates, taxes, credits, correspondence, amounts paid, reconciliation differences, notice periods, and potential wider impact.

No invoice may be altered, credited, or cancelled without approval and an audit trail. Such disputes must not be confused with player deposits, withdrawals, wagers, or other player transactions, which are outside the Company's operations.

8.24 Complaints Alleging Fraud or Financial Crime

Suspected fraud, money laundering, terrorist or proliferation financing, sanctions evasion, corruption, identity misuse, unexplained third-party payments, or other criminal conduct must be escalated immediately to the MLRO. The normal process may be modified lawfully to protect an investigation, avoid tipping off, preserve evidence, and coordinate with authorities. Any communication restriction must be lawful and documented.

8.25 Information-Security and Data-Protection Complaints

Alleged unauthorised access, data loss, credential compromise, improper disclosure, cyberattack, or unlawful processing must be referred immediately to responsible security and privacy functions. The Company must assess occurrence, affected

information and systems, containment, notification deadlines, provider or partner notification, authority or individual notification, and whether complaint communication could compromise incident response. Sensitive records must be access-restricted.

8.26 Interim Measures

Proportionate interim measures may include preserving logs; restricting system or content access; suspending a release or configuration; disabling content; preventing expansion to additional domains or markets; holding a disputed B2B payment where contractually allowed; additional verification; enhanced monitoring; technical containment with Babylon Gaming; and restricting or suspending a relationship.

Measures must be documented, proportionate, and must not prejudice the outcome.

8.27 Complaint Outcome

An outcome should ordinarily be classified as upheld, partially upheld, not upheld, resolved by agreement, withdrawn, referred to another responsible entity, unable to determine for insufficient evidence, or declined for a documented legitimate reason. Classification must reflect the evidence and must not be manipulated to improve statistics.

8.28 Remedies and Corrective Action

Appropriate action may include correcting information; technical remediation; reperforming a service; authorised B2B credit or refund; correcting an invoice or calculation; contractual remedy; restricting or suspending content; changing configuration; amending a process or policy; training; disciplinary action; enhanced monitoring; partner remediation; notification; regulatory or contractual reporting; independent testing; or termination. Corrective action may be required even where no financial remedy is due.

8.29 Final Response

The written final response should include the reference, issues, investigation, material evidence, findings, reasoned decision, remedy or corrective action, required complainant action, dates, escalation options, and contact details.

It must distinguish established facts, technical findings, contractual interpretations, matters controlled by another party, and matters that could not be determined.

8.30 Internal Review

A review may be requested where material evidence appears overlooked, the decision appears inconsistent with the contract or applicable requirements, new information arises, a conflict affected the investigation, an agreed remedy was not implemented, or the matter remains materially unresolved.

The reviewer should be suitably authorised and not solely responsible for the original decision. Internal review must not delay access to a contractual or legal process.

8.31 Contractual Dispute Resolution

Unresolved complaints must follow the applicable contract, potentially including senior-management escalation, good-faith negotiation, mediation, expert determination, arbitration, or court proceedings.

The Company must confirm the contract, governing law, forum, notice requirements, evidence preservation, deadlines, authority, affected-party coordination, legal advice, and reporting implications. It must not describe itself as providing player ADR; player-facing ADR remains the operator's responsibility.

8.32 Regulatory Complaints and Enquiries

Communications from the Curaçao Gaming Authority or another authority must be referred immediately to the Director and Compliance Officer. The Company must record them, confirm deadlines, preserve evidence, coordinate contributions, ensure accuracy and completeness, obtain approval, and monitor commitments and corrective action. Contracts must not prevent lawful reporting to an authority.

8.33 Legal Proceedings and Settlement

Threatened or commenced proceedings must be referred promptly to the Director and, where appropriate, legal counsel. Evidence and deadlines must be preserved; contractual notices and insurer notifications observed; positions coordinated with affected parties; unauthorised admissions avoided; reporting implications assessed; and decisions documented.

A settlement must not conceal a reportable breach, restrict lawful reporting, suppress suspicious-activity reporting, include misleading statements, or prevent necessary corrective action.

8.34 Repeated or Abusive Communications

Proportionate controls may be applied to repetitive, threatening, abusive, or obstructive communications, after considering whether the underlying complaint was properly addressed, whether a new issue exists, whether one designated contact is sufficient, whether security or law enforcement is needed, and whether restriction complies with the contract.

Persistence, criticism, or dissatisfaction alone is not abusive or vexatious. Restrictions require approval and documentation.

8.35 Complaint Records

Records must include the original complaint; acknowledgement; classification and assessment; investigation plan; evidence; correspondence; provider referrals; technical findings; decisions; approvals; final response; remedies; corrective actions; internal review; contractual or legal proceedings; closure evidence; root-cause analysis; and regulatory reports.

Records must be dated, attributable, accurate, complete, legible, retrievable, access-protected, alteration-protected, and retained according to applicable legal, regulatory, contractual, and internal requirements.

8.36 Regulatory and Contractual Reporting

The Compliance Officer must determine reporting to the Curaçao Gaming Authority, another regulator, a data-protection authority, a financial-intelligence or law-enforcement authority, Babylon Gaming, an upstream provider, a business partner, an insurer, or another entitled party. Reports must be accurate, complete, timely, and appropriately approved.

Bet Play B.V. is not responsible for an operator's periodic player-complaint reports but must provide accurate and timely technical information where contractually or lawfully required.

8.37 Root-Cause Analysis

Proportionate root-cause analysis is required for upheld, material, critical, recurring, multi-partner or multi-product, regulatory, licence, technical, contractual, financial, governance, legal, suspension, or regulatory-attention cases.

The analysis should identify immediate and underlying causes, contributing control failures, impact, other affected parties, remediation, responsible persons, target dates, and completion verification. Closing the complaint does not remove the duty to address its cause.

8.38 Complaint Monitoring and Management Information

Management information should include complaints by period, category, source, partner, product, market, and jurisdiction; provider involvement; priority; acknowledgement and resolution performance; open and overdue cases; outcomes; amounts and remedies; repeated issues; technical complaints by game, product, or version; invoicing complaints; regulatory, AML/CFT/CPF, sanctions, security, and privacy matters; material misdirected player communications; internal escalations; contractual and legal disputes; root causes; open corrective actions; and partners generating unusual volumes.

Urgent or material concerns must be escalated immediately rather than deferred to periodic reporting.

8.39 Connection with Business-Partner Oversight

The Company must consider whether complaints indicate content misuse, unauthorised domains or markets, undisclosed distribution, misleading statements, weak controls, failure to cooperate, unreliable records, regulatory breach, financial distress, security weakness, a need to change risk classification, or grounds for enhanced monitoring, restriction, suspension, or termination.

Repeated low-severity complaints may collectively indicate a material control weakness.

8.40 Training

Role-appropriate training should address complaint recognition; distinctions among support requests, complaints, and disputes; the B2B-only role; misdirected player communications; registration and escalation; deadlines; fair investigation; evidence preservation; AML/CFT/CPF and tipping-off; security and privacy escalation; Babylon Gaming coordination; contractual dispute procedures; communication; conflicts; root-cause analysis; records; and confidentiality.

Training must be refreshed after material changes to requirements, systems, contracts, or procedures.

8.41 Quality Assurance

The Compliance Officer should periodically review files to confirm correct identification; complete registration; distinction between player communications and B2B complaints; appropriate priority; timely responses; fair, evidence-based investigation; proper function and provider involvement; escalation; adequate reasoning; authorised and implemented remedies; complete records; identified root causes and recurring issues; completed corrective action; and required reporting.

Deficiencies must be documented and corrected.

8.42 Key Controls

The minimum controls are:

- Formal B2B complaints are recorded centrally.
- Routine support is distinguished from complaints.
- Misdirected player communications are referred to the relevant operator.
- Bet Play B.V. does not determine player complaints.
- Operator-escalated game-malfunction cases are recorded, investigated, and linked to technical incidents and corrective actions.
- Urgent and critical complaints are escalated immediately.
- Deadlines are monitored.
- Material investigations are appropriately independent.
- Evidence is preserved and technical conclusions verified.
- Babylon Gaming and other providers are involved where necessary.
- Final decisions are reasoned and written.
- Financial remedies require authority.
- Contractual dispute procedures are followed.
- Regulatory reporting is assessed.
- Root causes and corrective actions are monitored.
- Complaint information informs partner-risk assessments.
- Records are protected and retrievable.

8.43 Exceptions

An exception must be justified, documented, identify the affected requirement, assess risk, receive approval, include compensating controls, and be limited in scope and duration.

It must not suppress regulatory concerns, prevent lawful reporting, conceal evidence, compromise an AML/CFT/CPF investigation, misrepresent the role of Bet Play B.V., an operator, Babylon Gaming, or a regulator, or permit retaliation.

8.44 Review and Continuous Improvement

The Director and Compliance Officer must review the framework at least annually and after material change. The review should consider changes to law, regulation, licence conditions, contracts, and the business model; complaint trends and performance; material disputes; operator-escalated malfunction cases;

Babylon Gaming matters; recurring technical, commercial, or operational problems; reporting and feedback; root-cause analyses; overdue actions; partner-risk implications; training and resources; alignment of documented and actual practice; and consistency with Chapters 7, 9, 10, 11, and 12.

Material amendments must be approved by the Director and communicated to affected personnel.

Information Security and Data Protection

9

Chapter 9 – Information Security and Data Protection

9.1 Purpose

This chapter establishes Bet Play B.V.'s framework for protecting information, systems, credentials, intellectual property, personal data, and business records against unauthorised access, loss, alteration, disclosure, destruction, or unavailability.

The framework is intended to preserve confidentiality, integrity, availability, authenticity, accountability, privacy, and regulatory compliance throughout the information lifecycle.

9.2 B2B Operating Context

Bet Play B.V. operates on a B2B basis. It does not operate player accounts or intentionally maintain the player databases of B2C operators. It may nevertheless receive limited player-related information in technical logs, game-malfunction escalations, security investigations, regulatory enquiries, or misdirected communications.

Such information must be limited to what is necessary, pseudonymised where practicable, protected as personal data, and not repurposed for player support, marketing, profiling, or account administration.

9.3 Scope

This chapter applies to:

- Company personnel, contractors, Directors, and authorised third parties.
- Information in electronic, paper, verbal, visual, backup, and archived form.
- Company-managed and externally hosted systems.
- Devices, networks, cloud services, repositories, support tools, development environments, and communication channels.
- Information exchanged with Babylon Gaming, operators, aggregators, suppliers, advisers, authorities, and other counterparties.
- Personal data for which Bet Play B.V. acts as controller, processor, or recipient.

9.4 Applicable Framework

The Company must comply with applicable Curaçao law, licence conditions, Curaçao Gaming Authority requirements, contractual security and privacy duties, applicable market-specific data-protection requirements, and its own approved policies. Where territorial scope or the Company's privacy role is uncertain, the matter must be referred to the Compliance Officer and legal or privacy advisers.

9.5 Security and Privacy Principles

The Company must apply risk-based security, least privilege, need-to-know access, defence in depth, secure configuration, privacy by design and default, data minimisation, purpose limitation, accuracy, retention limitation, and demonstrable accountability.

Commercial urgency does not justify bypassing security or privacy controls.

9.6 Information Classification

Information must be classified at least as public, internal, confidential, or restricted. Classification must reflect legal duties, contractual sensitivity, personal-data content, security impact, and harm arising from misuse.

Restricted information includes credentials, cryptographic secrets, security findings, suspicious-activity information, sensitive personal data, regulator-protected material, and production access data. Handling, transmission, storage, printing, copying, and disposal controls must correspond to classification.

9.7 Roles and Responsibilities

The Director approves the framework, risk acceptance, material expenditure, and significant corrective action. The Compliance Officer oversees legal, licence, privacy, and reporting implications. The responsible security function maintains technical standards, monitoring, vulnerability management, and incident coordination. System and information owners approve access and define acceptable use. The MLRO controls access to financial-crime information. All personnel must protect information, use only approved services, and report suspected incidents immediately.

Where duties are outsourced, ownership and accountability remain with Bet Play B.V.

9.8 Information Asset Inventory and Ownership

The Company must maintain a proportionate inventory of material information assets, systems, services, repositories, integrations, domains, certificates, and critical suppliers. Each material asset must have an owner, classification, business purpose, location, dependency record, recovery requirement, and access-control basis.

Unsupported, unknown, or ownerless material assets must be investigated and remediated.

9.9 Risk Assessment

Security and privacy risks must be assessed periodically and before material systems, suppliers, integrations, markets, or processing activities are introduced. Assessments must consider threats, vulnerabilities, data types, access paths, third-party dependencies, likelihood, impact, existing controls, residual risk, and treatment actions.

High residual risks require documented Director approval and time-bound treatment.

9.10 Identity and Access Management

Access must be individually attributable, approved by the relevant owner, limited to job need, and reviewed periodically. Shared accounts are prohibited unless technically unavoidable, formally approved, and subject to compensating logging and credential controls.

Joiner, mover, and leaver procedures must ensure prompt provisioning, adjustment, and revocation. Dormant, unnecessary, duplicate, and orphaned accounts must be disabled.

9.11 Privileged Access

Administrative access must be restricted, separately approved, strongly authenticated, logged, and used only for authorised purposes. Privileged credentials must not be used for routine activity. Emergency access must be time-limited and reviewed after use.

Production access by developers or providers must be controlled under Chapter 13 and traceable to an approved task, change, or incident.

9.12 Authentication and Credentials

Multi-factor authentication must be used for privileged, remote, cloud, banking, source-code, and other material access wherever supported. Passwords and secrets must meet approved standards and must not be shared through unapproved channels, embedded in source code, or stored in unsecured documents.

Credentials suspected of compromise must be revoked or rotated promptly.

9.13 Acceptable Use and Endpoint Security

Company information may be processed only on approved devices and services unless an exception is authorised. Devices must use supported software, secure configuration, screen locking, malware protection where appropriate, encryption, patching, and remote-management controls.

Unapproved removable media, personal cloud storage, credential sharing, and circumvention of security controls are prohibited.

9.14 Network and Infrastructure Security

Networks and hosted environments must be segmented proportionately, securely configured, monitored, and protected against unauthorised exposure. Internet-facing services must be inventoried and subject to additional review. Firewalls, access rules, remote access, certificates, and administrative interfaces must be controlled and reviewed.

9.15 Encryption and Key Management

Confidential and restricted information must be encrypted in transit and at rest where appropriate to risk and technology. Cryptographic keys and certificates must have assigned owners, controlled generation and storage, rotation and renewal arrangements, revocation procedures, and recovery provisions.

Private keys and production secrets must not be placed in tickets, email, or source repositories.

9.16 Secure Communications and Information Transfer

Information transfers must use approved recipients, channels, and formats. Personnel must verify unusual or sensitive requests independently, especially those

involving credentials, bank details, bulk exports, source code, regulatory information, or personal data.

Transfers to Babylon Gaming or business partners must be limited to authorised contractual and operational purposes and recorded where material.

9.17 Logging and Monitoring

Material systems must generate logs sufficient to investigate access, changes, errors, game-related technical events, security activity, and administrative actions. Logs must use reliable time synchronisation, be protected against unauthorised alteration, retained for an appropriate period, and accessible only to authorised personnel.

Alerts must be triaged and linked to Chapter 10 where they indicate an incident.

9.18 Vulnerability, Patch, and Configuration Management

The Company must identify vulnerabilities through supplier notices, scanning, testing, monitoring, and credible external information. Findings must be risk-rated, assigned, tracked, and remediated within approved timeframes.

Critical exposure requires immediate assessment and may require isolation, temporary controls, service restriction, or emergency change. Deviations from approved configuration must be documented and corrected.

9.19 Security Testing

Material systems and externally exposed services must receive proportionate security testing before release and periodically thereafter. Testing may include code review, dependency scanning, vulnerability assessment, penetration testing, configuration review, and recovery testing.

Testing must be authorised, scoped, safely conducted, and followed by documented remediation and verification.

9.20 Supplier and Babylon Gaming Security

Before a material provider is engaged, the Company must assess its security, privacy, resilience, access, subcontracting, incident-notification, audit, return-of-data, and termination arrangements. Contracts must allocate responsibilities clearly.

Provider assurances do not replace Bet Play B.V.'s obligation to monitor risks within its licence and contractual responsibilities. Material provider weaknesses or delays must be escalated.

9.21 Personal-Data Inventory and Privacy Roles

The Company must identify material personal-data processing, data categories, data subjects, purposes, lawful bases or contractual grounds, recipients, locations, retention periods, and whether it acts as controller, joint controller, processor, or independent recipient.

Privacy roles must be documented in contracts where required. Bet Play B.V. must not assume that all technical data is anonymous merely because direct names are absent.

9.22 Data Minimisation and Pseudonymisation

Only data reasonably necessary for the stated purpose may be collected, accessed, or retained. Operator escalations should use pseudonymous player references unless direct identification is necessary and lawful. Unnecessary screenshots, documents, and free-text personal information must be removed or rejected securely.

9.23 Data-Subject Rights and Privacy Enquiries

Privacy enquiries or rights requests must be recorded, verified proportionately, and referred promptly to the responsible privacy function. Where Bet Play B.V. acts only as processor, it must assist the relevant controller and must not respond beyond its authority.

Misdirected player requests should be referred to the relevant B2C operator without creating a player-support relationship.

9.24 Cross-Border Transfers and Disclosures

Before personal data is transferred or made remotely accessible across borders, the Company must determine whether the transfer is lawful and whether contractual, technical, organisational, or other safeguards are required. Disclosures to authorities must be verified, authorised, limited, and documented.

9.25 Retention and Secure Disposal

Information must be retained according to approved schedules reflecting legal, regulatory, contractual, operational, evidential, and limitation requirements. Legal holds, investigations, complaints, incidents, and regulatory matters suspend ordinary disposal for relevant records.

At the end of retention, information and media must be destroyed or anonymised securely and the disposal recorded where material.

9.26 Backups

Critical information and configurations must be backed up according to recovery requirements. Backups must be encrypted or otherwise protected, access-restricted, monitored, separated from ordinary production risk where practicable, and tested through restoration exercises under Chapter 10.

9.27 Security and Personal-Data Incidents

Suspected loss, compromise, unauthorised access, improper disclosure, ransomware, credential theft, malicious code, service attack, or unlawful processing must be reported immediately and managed under Chapter 10.

The Company must preserve evidence, contain risk, determine affected information and parties, and assess notification duties without waiting for perfect certainty. Communications must not obstruct investigation or expose sensitive security details.

9.28 Records of Processing and Security Evidence

The Company must maintain sufficient evidence of risk assessments, access approvals, reviews, training, supplier assessments, processing records, privacy decisions, tests, vulnerabilities, incidents, notifications, exceptions, and corrective actions.

Records must be accurate, attributable, protected, and retrievable.

9.29 Monitoring and Management Information

Management information should cover access reviews, privileged access, vulnerabilities and remediation age, patch compliance, security alerts, incidents, privacy requests, supplier risks, backup tests, exceptions, training, and overdue

corrective actions. Critical matters must be escalated immediately rather than deferred to periodic reporting.

9.30 Training and Awareness

Personnel must receive induction and periodic training appropriate to their access and role. Training must cover phishing, credential protection, secure communications, information classification, privacy, incident reporting, remote work, provider access, and secure handling of player-related technical information.

Specialist training is required for privileged users, developers, finance personnel, support personnel, and incident responders.

9.31 Key Controls

Minimum controls are: asset ownership; risk assessment; individual access; least privilege; multi-factor authentication; controlled privileged access; secure configuration; vulnerability management; protected logs; approved transfers; data minimisation; provider due diligence; backups and restoration tests; immediate incident escalation; and complete security and privacy records.

9.32 Exceptions

Any exception must identify the affected control, justification, owner, risk, duration, approval, compensating measures, and review date. Exceptions must not authorise unlawful processing, conceal an incident, bypass sanctions or financial-crime restrictions, or permit uncontrolled access to restricted information.

9.33 Review and Continuous Improvement

The Director and responsible security and compliance functions must review this framework at least annually and following a material incident, regulatory change, system change, provider change, or audit finding. Material amendments must be approved, communicated, implemented, and reflected in training and technical standards.

IT Operations, Incident Management and Business Continuity

10

Chapter 10 – IT Operations, Incident Management and Business Continuity

10.1 Purpose

This chapter establishes Bet Play B.V.'s framework for reliable IT operations, event and incident management, crisis coordination, business continuity, disaster recovery, and return to normal service.

Its objectives are to minimise disruption, protect the Company's licence and B2B obligations, preserve evidence, support affected operators, and ensure that material incidents are contained, communicated, reported, corrected, and learned from.

10.2 Scope and B2B Context

This chapter applies to Company systems, integrations, games and content within its responsibility, administrative services, communication channels, outsourced services, and dependencies on Babylon Gaming and other providers.

Bet Play B.V. does not operate player accounts or player payment systems. An incident may nevertheless affect games supplied to operators, operator integrations, game-round records, reporting, licensed distribution, confidential data, or the ability of an operator to serve players. The relevant operator remains responsible for player communications and player-facing decisions; Bet Play B.V. must provide timely technical facts and appropriate B2B coordination.

10.3 Governance Principles

The Company must use clear ownership, risk-based priority, timely escalation, evidence preservation, controlled change, accurate communication, regulatory awareness, documented recovery objectives, tested plans, and lessons learned.

Incident response takes priority over ordinary commercial activity where necessary to prevent material harm.

10.4 Roles and Responsibilities

The Director has executive authority during critical incidents, approves crisis decisions, regulatory positions, major service restrictions, and exceptional

expenditure. The incident manager coordinates response and maintains the incident record. Technical personnel investigate, contain, recover, and preserve evidence. The Compliance Officer assesses licence, legal, notification, and business-partner implications. The MLRO controls financial-crime escalation. Business Partner Support manages approved operator communications. System owners validate recovery and accept service return. Providers must perform duties assigned by contract, but accountability for Bet Play B.V.'s own obligations remains with the Company.

10.5 IT Service and Dependency Inventory

The Company must identify critical services, owners, business purposes, operating hours, upstream and downstream dependencies, hosting and provider arrangements, data flows, recovery objectives, monitoring, support contacts, and fallback procedures.

Changes to critical dependencies must update the inventory and continuity analysis.

10.6 Routine IT Operations

Routine operations must include service monitoring, capacity and performance review, scheduled jobs, certificate and domain renewal, backup monitoring, access administration, patch and vulnerability coordination, log review, provider oversight, and maintenance of operating procedures.

Repeated manual intervention, unexplained warnings, capacity pressure, and failed jobs must be treated as control indicators rather than normalised.

10.7 Event Monitoring and Alerting

Monitoring must be proportionate to service criticality and capable of identifying availability loss, latency, error spikes, integration failures, security activity, certificate expiry, data-processing failures, unusual game behaviour, and dependency outages.

Alerts must have owners, priority rules, escalation paths, and documented resolution. Monitoring failure itself must be detected where practicable.

10.8 Incident Definition and Classification

An incident is an unplanned event that causes or threatens loss of confidentiality, integrity, availability, compliance, safety, contractual performance, or reliable operation.

Incidents must be classified as:

Severity	Characteristics	Response
Low	Limited impact, no material external effect, routine recovery.	Record and resolve through normal operations.
Significant	Material degradation, repeated failures, limited partner impact, or meaningful control weakness.	Prompt incident coordination and management visibility.
Major	Serious or extended outage, multiple partners, suspected security or data impact, or potentially reportable malfunction.	Immediate incident-team activation and executive escalation.
Critical	Licence-threatening event, widespread systemic failure, major cyberattack, severe data compromise, fraud, or inability to operate critical services.	Immediate crisis governance, containment, continuity activation, and notification assessment.

Classification must consider potential impact, not only confirmed harm.

10.9 Incident Reporting and Intake

Personnel and providers must report suspected incidents immediately through approved channels. The incident record must capture time detected, reporter, affected services, symptoms, initial impact, severity, known dependencies, actions taken, evidence location, owners, and next update time.

No person may suppress or delay an incident because facts are incomplete or commercial impact is uncertain.

10.10 Initial Response

The responsible team must acknowledge the incident, assign an incident manager, validate severity, stabilise the situation, preserve evidence, identify affected services and partners, establish a response channel, engage required providers, assess reporting deadlines, and decide whether continuity arrangements or service restrictions are required.

10.11 Containment

Containment may include isolating systems, revoking credentials, blocking traffic, disabling a game or integration, suspending a release, reverting a configuration, restricting partner access, increasing monitoring, preserving logs, or activating an alternative service.

Containment must be proportionate, authorised at the appropriate level, documented, and reviewed as facts develop.

10.12 Technical Investigation and Evidence

Investigations must identify timeline, affected components, versions, changes, accounts, interfaces, logs, data, providers, operators, markets, and control failures. Original evidence must be preserved; working copies must be distinguished. Time zones and clock differences must be reconciled.

Where game rounds are implicated, the procedure in Chapter 8 for operator-escalated game malfunctions must be followed and linked to the incident record.

10.13 Babylon Gaming and Provider Coordination

Provider incidents must be recorded internally and actively managed. Bet Play B.V. must identify contractual responsibilities, request evidence and response times, monitor progress, challenge unsupported conclusions, assess wider exposure, and maintain its own operator and regulatory obligations.

Referral to Babylon Gaming or another provider does not close the incident.

10.14 Communications

Incident communications must be timely, accurate, consistent, audience-appropriate, and approved. They must distinguish known facts, reasonable

assessments, unknown matters, temporary controls, required recipient actions, and the timing of the next update.

Personnel must not speculate, attribute fault without evidence, expose sensitive security information, admit liability without authority, or promise player remedies.

10.15 Business-Partner Notification

Affected operators and partners must be notified where required by contract, law, licence conditions, risk, or practical coordination needs. Notices should identify affected services and periods, current status, containment, required partner action, data or game-round implications, and update arrangements.

Operators remain responsible for player-facing notices and complaint decisions. Bet Play B.V. must supply reliable information needed for those duties.

10.16 Regulatory and Other External Reporting

The Compliance Officer must assess notification to the Curaçao Gaming Authority, other regulators, data-protection authorities, testing laboratories, insurers, law enforcement, affected counterparties, or other entitled parties. Shorter mandatory deadlines override internal processes.

Reports must be accurate, approved, timely, and updated when material facts change. A reportable incident must not be delayed solely because root cause remains unknown.

10.17 Security and Personal-Data Incidents

Cybersecurity and personal-data incidents must also follow Chapter 9. The Company must determine compromised information, affected data subjects and parties, attack path, ongoing risk, notification requirements, evidence needs, and secure recovery measures.

Tipping-off, legal privilege, confidentiality, and law-enforcement requirements must be respected.

10.18 Game and Content Incidents

Where games or content may be malfunctioning, the Company must identify affected games, versions, configurations, operators, brands, domains, markets, currencies, periods, sessions, rounds, and releases. It must determine whether to monitor,

restrict, or suspend content and whether wider reconciliation or recertification is required.

Return to service requires evidence that the affected condition is corrected or safely controlled.

10.19 Recovery and Service Restoration

Recovery steps must be approved, tested where practicable, and recorded. Restoration must consider security, data integrity, configuration, dependencies, capacity, monitoring, and unresolved risk. Business and system owners must validate service before normal status is declared.

Temporary fixes must be logged as technical debt or corrective action with an owner and deadline.

10.20 Closure

An incident may close only when service is stable, required notices are made, evidence is preserved, affected records are reconciled, partner communications are complete, residual risks are accepted, and corrective actions are assigned.

Closure does not require every long-term remediation action to be complete, but those actions must remain tracked.

10.21 Root-Cause Analysis and Lessons Learned

Major, critical, repeated, reportable, or materially disputed incidents require root-cause analysis. The review must identify immediate and underlying causes, detection and response performance, control failures, provider contributions, affected parties, communication effectiveness, and preventive action.

Lessons learned should be completed promptly and must avoid blame-driven conclusions unsupported by evidence.

10.22 Business Impact Analysis

The Company must periodically identify critical activities, maximum tolerable disruption, recovery time objectives, recovery point objectives, minimum staffing, information and system needs, manual alternatives, provider dependencies, single points of failure, and legal or contractual deadlines.

The analysis must reflect the B2B content-supply model and foreseeable loss of Babylon Gaming, hosting, communications, access, personnel, premises, or key records.

10.23 Business Continuity Plans

Plans must define activation authority, crisis roles, contacts, priorities, workarounds, alternate communications, remote-working arrangements, provider escalation, record access, financial authority, regulatory coordination, and return-to-normal criteria.

Plans must be concise enough to use during disruption and available securely when normal systems are unavailable.

10.24 Disaster Recovery

Disaster-recovery arrangements must address critical infrastructure, configurations, code and deployment artefacts, databases, logs, credentials, keys, certificates, backups, alternate environments, restoration order, validation, and reconciliation.

Recovery must not introduce unapproved software, unverified data, weakened security, or unsupported configurations.

10.25 Backup and Restoration Testing

Backups must follow Chapter 9 and be tested periodically by restoring representative critical data and configurations. Tests must confirm completeness, integrity, timing, access, dependency compatibility, and achievement of recovery objectives. Failures require corrective action.

10.26 Continuity Activation and Crisis Management

The Director or delegated authority may activate continuity or crisis arrangements. Activation, decisions, priorities, resource allocation, communications, exceptions, and transition stages must be logged.

The Company must maintain a common operating picture and a defined cadence for executive and stakeholder updates.

10.27 Testing and Exercises

The Company must conduct risk-based tabletop, communication, provider, technical recovery, remote-working, and full or partial continuity exercises. Scenarios should include provider outage, cyberattack, game malfunction, data compromise, loss of access, and key-person unavailability.

Exercise findings must have owners, deadlines, and verification.

10.28 Change Freeze and Emergency Change

During major incidents, the incident manager may impose a change freeze. Emergency changes must follow Chapter 13, be limited to what is necessary, approved by authorised persons, logged, tested as far as practicable, monitored, and retrospectively reviewed.

10.29 Records

The Company must retain incident tickets, timelines, decisions, evidence, communications, provider responses, notifications, recovery records, approvals, root-cause analyses, exercise reports, and corrective actions. Records must be protected, attributable, and retrievable.

10.30 Monitoring and Management Information

Management information should cover availability, performance, incident volumes and severity, detection and recovery times, repeated incidents, provider performance, notification timeliness, continuity tests, backup restoration, overdue actions, and accepted risks.

10.31 Training

All personnel must understand incident reporting and continuity arrangements. Incident managers, technical responders, support personnel, executives, Compliance, and provider coordinators require role-specific training and exercises.

10.32 Key Controls

Minimum controls are: service and dependency inventories; monitoring; defined severity; immediate reporting; named incident ownership; evidence preservation;

controlled containment; provider coordination; accurate B2B communication; notification assessment; tested recovery; continuity plans; exercises; root-cause analysis; and tracked corrective action.

10.33 Exceptions

Incident and continuity exceptions must be documented, risk-assessed, approved, time-limited, and supported by compensating controls. No exception may suppress mandatory reporting, destroy evidence, conceal player-impact information from an operator, or permit unsafe restoration.

10.34 Review and Continuous Improvement

The Director and relevant control functions must review this framework at least annually and after major incidents, exercises, material provider changes, or regulatory findings. Amendments must be approved, communicated, and reflected in plans, contacts, training, monitoring, and contracts.

Business Partner Support Operations

11

Chapter 11 – Business Partner Support Operations

11.1 Purpose

This chapter establishes Bet Play B.V.'s framework for providing consistent, secure, timely, and traceable operational and technical support to B2B customers and other authorised counterparties.

11.2 B2B-Only Scope

Business Partner Support serves operators, aggregators, platform providers, resellers, distributors, Babylon Gaming, and other authorised commercial or technical counterparties. It does not provide player-facing customer service, administer player accounts, process deposits or withdrawals, award bonuses, determine game outcomes, or decide player complaints.

A player who contacts Bet Play B.V. must be handled under Chapter 8 and referred to the relevant B2C operator. Limited technical information may be gathered only where necessary to support an operator escalation or protect regulatory, security, or integrity interests.

11.3 Support Services

Support may include authorised enquiries concerning onboarding, integration, credentials, environments, documentation, content availability, configuration, releases, service status, game rules, reporting, technical errors, commercial administration, and coordination of incidents or complaints.

Legal interpretation, binding commercial concessions, player remedies, regulatory admissions, and unapproved technical changes are outside ordinary support authority.

11.4 Principles

Support must be accessible to authorised partners, professionally delivered, risk-prioritised, evidence-based, confidential, appropriately segregated, and fully traceable. Tickets must not be closed merely to improve service metrics.

11.5 Roles and Responsibilities

The Director oversees resources and material escalations. The support lead owns procedures, queues, quality, service reporting, and staffing. Support personnel authenticate requesters, record matters, troubleshoot within authority, protect information, and escalate appropriately. Account Management manages relationship context but must not override security or incident classification. Technical teams provide specialist analysis. Compliance assesses regulatory matters. Finance owns billing matters under Chapter 14. Babylon Gaming and providers support matters within their responsibility.

11.6 Approved Channels and Hours

The Company must define approved email, portal, ticketing, telephone, and emergency channels; operating hours; languages; supported services; and out-of-hours escalation. Critical channels must be monitored and tested.

Requests through informal channels must be transferred to the approved record promptly.

11.7 Partner and Contact Authentication

Before disclosing confidential information, changing access, or taking material action, Support must verify the organisation, requester, authority, and channel proportionately. Contractual contact lists and role-based permissions must be kept current.

Unusual changes of contact, domain, credential, IP address, beneficiary information, or urgency require independent verification. Finance changes follow Chapter 14, with system implementation under Chapter 13 where applicable.

11.8 Ticket Registration

Each support matter requiring action must receive a unique reference and record the requester, organisation, channel, date and time, affected service, operator/brand/domain, market, environment, description, business impact, priority, owner, actions, evidence, communications, escalation, resolution, and closure approval where appropriate.

Sensitive data must not be copied into tickets unnecessarily.

11.9 Classification

Tickets must be classified as information request, access request, service request, integration issue, content or configuration issue, suspected malfunction, incident, security or privacy matter, complaint, billing matter, or change request.

Misclassification must be corrected without losing the original history.

11.10 Priority and Service Targets

Priority	Typical impact	Handling expectation
P4 Routine	– General information or low-impact request.	Normal queue and agreed service target.
P3 Moderate	– Limited operational impact or workaround available.	Prompt ownership and scheduled resolution.
P2 – High	Material degradation, important launch blocker, or multiple affected users or services.	Rapid specialist escalation and frequent updates.
P1 Critical	– Outage, suspected systemic malfunction, security event, or severe regulatory or partner impact.	Immediate Chapter 10 escalation and continuous coordination.

Priority must reflect actual and potential impact, affected markets, urgency, regulatory deadlines, and breadth. Commercial status alone must not determine priority.

11.11 Acknowledgement and Ownership

Support must acknowledge matters within the applicable service target, confirm the reference and priority, identify the owner, request missing information, and state the next expected update. Tickets must have continuous ownership through handoffs.

11.12 Information Gathering

Support should obtain only information relevant to diagnosis, including affected service, game and version, environment, timestamps and time zone, identifiers, error

messages, reproduction steps, recent changes, scope, logs, screenshots, and business impact.

Player identifiers should be pseudonymised. Credentials, payment-card data, and unnecessary identity documents must not be requested or stored in tickets.

11.13 Standard Troubleshooting

Troubleshooting must follow approved knowledge articles and procedures, preserve evidence, distinguish test and production environments, and record commands, checks, outcomes, and changes. Support must not alter production data, game outcomes, source code, certified content, or security controls outside its authority.

11.14 Access and Credential Requests

Access requests require authenticated authority, defined role and environment, owner approval, least privilege, expiry where appropriate, and a traceable record. Credentials must be transmitted securely and never placed in ordinary ticket text.

Provisioning and revocation must comply with Chapter 9.

11.15 Integration Support

Integration support must use approved specifications, environments, test data, endpoints, certificates, and release versions. Support must record deviations and prevent test credentials or data from being used in production.

11.16 Game and Content Queries

Support may provide approved game rules, configuration information, version status, certification references, and service availability. It must not provide unsupported interpretations, disclose confidential mathematics or source material, or promise a player-facing outcome.

11.17 Player-Originated Malfunction Escalations

Where an operator raises a matter originating from a player allegation of game malfunction, Support must link the operator ticket to the complaint procedure and, where incident criteria are met.

Support must collect the operator, brand, domain, jurisdiction, game, version, timestamp, pseudonymous player reference, session/round/transaction identifiers, disputed amount, logs, configuration, evidence, and operator deadline. Bet Play B.V. provides technical findings to the operator; the operator remains responsible for the player complaint and remedy decision.

11.18 Complaints and Disputes

Expressions of material dissatisfaction, allegations of breach, requests for compensation, repeated unresolved matters, or threats of regulatory or legal escalation must be referred to Chapter 8. The support ticket must remain linked to the complaint record and technical work.

11.19 Incident Escalation

Suspected outage, systemic error, security incident, data compromise, widespread malfunction, or serious regulatory risk must be escalated immediately under Chapter 10. Support must not wait for complete diagnosis before escalating.

11.20 Security and Privacy Escalation

Credentials, unauthorised access, suspicious files, phishing, improper disclosure, personal-data requests, or excessive data supplied by a partner must be referred under Chapters 9 and 10. Sensitive content must be access-restricted.

11.21 Change Requests

A request that alters production configuration, functionality, integration, content, access model, or certified behaviour is a change request and must follow Chapter 14. Support must not disguise a change as troubleshooting.

11.22 Babylon Gaming and Provider Escalation

Provider referrals must specify the issue, priority, evidence, requested action, required response time, partner deadline, and Bet Play B.V. owner. Progress must be monitored and communicated. A provider referral does not transfer ticket ownership or justify unsupported conclusions.

11.23 Communications and Updates

Updates must state current status, verified findings, actions, outstanding dependencies, workarounds, risks, and next update time. Known facts must be separated from assumptions. Personnel may not admit liability, allocate blame, promise credits, or disclose restricted information without authority.

11.24 Workarounds

Workarounds must be risk-assessed, approved, documented, communicated clearly, time-limited, monitored, and replaced by a permanent correction. A workaround must not weaken security, change game outcomes, or bypass licence or certification controls.

11.25 Resolution and Closure

A ticket may close when the requested service is completed or the issue is resolved or transferred to a governed process; relevant evidence is recorded; the partner has been informed; linked incident, complaint, finance, or change records exist; and follow-up actions are assigned.

Partner confirmation should be obtained for material matters. Automatic closure rules must allow reasonable reopening.

11.26 Reopening and Recurrence

Reopened or repeated tickets must retain links to earlier records. Recurrence involving the same game, integration, version, provider, or error must be analysed collectively and may require incident escalation, problem management, or root-cause analysis.

11.27 Knowledge Management

Approved support knowledge must be accurate, current, version-controlled, classified, reviewed by relevant owners, and retired when obsolete. Confidential internal procedures must not be sent externally. Lessons from tickets, incidents, complaints, and releases should improve knowledge articles.

11.28 Service-Level Management

The Company must monitor acknowledgement, update, escalation, and resolution targets. Exclusions, pauses, and dependencies must be defined and evidenced. Service-level reporting must not conceal partner-impacting delay caused by providers.

11.29 Quality Assurance

Periodic ticket reviews must assess authentication, classification, priority, timeliness, technical accuracy, privacy, evidence, communication, escalation, closure, and links to complaints, incidents, changes, and corrective actions. Deficiencies require remediation and coaching.

11.30 Records and Management Information

Records must be attributable, complete, protected, searchable, and retained appropriately. Management information should cover volumes, categories, priorities, ageing, service performance, reopenings, recurring problems, complaints, incidents, provider dependencies, operator-escalated malfunctions, access requests, and overdue actions.

11.31 Training

Support personnel require training on the B2B-only role, authentication, secure ticket handling, game and integration basics, player-related escalation boundaries, complaint recognition, incident severity, privacy, security, change control, provider coordination, and communication.

11.32 Key Controls

Minimum controls are: approved channels; verified contacts; central tickets; risk-based priority; named ownership; secure data handling; controlled troubleshooting; immediate incident escalation; complaint and malfunction linkage; governed access and change requests; provider follow-up; reasoned closure; quality review; and recurring-issue analysis.

11.33 Exceptions

Any exception must be documented, approved, risk-assessed, time-limited, and supported by compensating controls. No exception may authorise player support, player payment processing, unauthorised disclosure, unlogged production changes, suppression of a complaint or incident, or unsupported alteration of a game result.

11.34 Review and Continuous Improvement

The support lead, Director, and relevant control functions must review this framework at least annually and following material service, system, provider, regulatory, or organisational changes. Material amendments must be approved and reflected in contracts, targets, tools, knowledge, training, and related chapters.

Product, Content and Business Development

12

Chapter 12 – Product, Content and Business Development

12.1 Purpose

This chapter establishes Bet Play B.V.'s framework for selecting, developing, approving, positioning, licensing, distributing, and monitoring products and gaming content, and for pursuing B2B commercial opportunities in a controlled and regulatorily appropriate manner.

12.2 B2B Operating Model

Bet Play B.V. supplies or facilitates gaming content and related services to approved business partners. It does not market directly to players, acquire players, operate player accounts, set player bonuses, process player money, or determine player complaints.

Business development must therefore focus on licensed or otherwise eligible B2B counterparties, authorised brands, domains, markets, integrations, and distribution arrangements.

12.3 Scope

This chapter applies to product strategy, content roadmap, new games and features, third-party content, certification, localisation, pricing, commercial proposals, marketing claims, prospective-partner engagement, contracting inputs, authorised distribution, launch approval, post-launch monitoring, intellectual property, and product retirement.

12.4 Principles

Product and commercial decisions must be lawful, evidence-based, contractually clear, technically deliverable, secure, financially supportable, market-authorised, and consistent with licence conditions. Revenue opportunity must not override compliance, integrity, player-protection dependencies, certification, or security.

12.5 Roles and Responsibilities

The Director approves strategy, material opportunities, launches, risk acceptance, and contracts within authority. Product owns requirements, roadmap, lifecycle, and product evidence. Business Development identifies and qualifies opportunities without making unauthorised commitments. Compliance assesses licensing, markets, distribution, claims, and regulatory risk. Technical teams assess feasibility, security, integration, release, and support. Finance validates pricing and financial terms. Legal or external counsel supports rights and contracts. Babylon Gaming and other providers supply evidence and perform assigned content responsibilities.

12.6 Product and Content Inventory

The Company must maintain an inventory of products and content identifying owner, provider, version, status, certification, permitted jurisdictions, currencies and languages, integration method, dependencies, intellectual-property basis, launch history, restrictions, and retirement status.

12.7 Product Strategy and Roadmap

The roadmap must align with approved business strategy, licence scope, market permissions, partner demand, technical capacity, risk appetite, provider capability, certification lead times, security, support, and continuity needs. Material priorities and changes must be approved and documented.

12.8 Product Proposal and Business Case

A material proposal must describe purpose, target B2B users, intended markets, functionality, provider roles, financial assumptions, technical dependencies, legal and licensing requirements, security and privacy impact, certification, support model, implementation resources, risks, and exit arrangements.

Assumptions must be distinguished from confirmed facts.

12.9 Stage-Gate Approval

Material products and content must pass proportionate gates covering concept, feasibility, compliance, design, build or acquisition, testing, certification, commercial readiness, launch, and post-launch review. Approval evidence and conditions must be retained.

No gate may be bypassed solely to meet a commercial date.

12.10 Regulatory and Market Assessment

Before offering content in a market, Compliance must assess licence scope, local prohibitions or conditions, certification, game rules, technical standards, responsible-gaming dependencies, language and disclosure requirements, reporting, data location, sanctions, and distribution structure.

Authorisation must be specific enough to identify the relevant partner, brand, domain, market, product, and material restrictions.

12.11 Content Due Diligence

Third-party or Babylon Gaming content must be supported by evidence of ownership or lawful rights, technical quality, game integrity, mathematics where applicable, certification, security, maintenance, incident support, version control, authorised markets, and contractual permission for onward B2B distribution.

Missing or contradictory evidence must be resolved before launch.

12.12 Product Requirements

Requirements must be clear, testable, version-controlled, and approved. They must address functionality, game rules, operator configuration, interfaces, data, logging, reporting, accessibility where applicable, security, privacy, performance, resilience, localisation, certification, and support.

12.13 Game Integrity and Fairness Evidence

For gaming content, the Company must obtain and preserve relevant game descriptions, rules, mathematics or provider attestations, random-number-generation evidence where applicable, return-to-player information, test results, certificates, version mappings, and change history.

Bet Play B.V. must not represent content as certified, fair, or approved beyond the evidence held.

12.14 Certification and Testing Laboratories

Required testing and certification must be completed by appropriately qualified or recognised bodies before launch. Certificates must correspond to the actual version, configuration, market, and operating conditions. Expiry, conditions, exclusions, and recertification triggers must be monitored.

12.15 Responsible-Gaming and Player-Protection Dependencies

Although the B2C operator controls player accounts and player-protection interactions, product design and distribution must not obstruct the operator's legal duties. Relevant game information, restrictions, session or transaction data, and technical controls must be made available as contractually and lawfully required.

Bet Play B.V. must not make player-facing responsible-gaming claims it cannot substantiate.

12.16 Security and Privacy by Design

Products and integrations must follow provisions and processes laid out on this manual. Designs must minimise personal data, restrict access, protect credentials and interfaces, generate adequate logs, support incident response, and define retention and deletion. High-risk processing or material security exposure requires formal assessment before approval.

12.17 Intellectual Property and Branding

The Company must confirm ownership, licences, sublicensing rights, territorial rights, brand permissions, attribution, restrictions, and infringement risks before using or distributing names, artwork, software, trademarks, music, mathematics, documentation, or other protected material.

Use outside approved rights is prohibited.

12.18 Localisation and Market Presentation

Translations, currency displays, game rules, help text, regulatory statements, and product descriptions must be accurate and approved. Localisation must not change certified behaviour or create misleading claims. Market-specific restrictions must be reflected in configuration and distribution controls.

12.19 Opportunity Qualification

Prospective opportunities must be assessed for strategic fit, legal eligibility, jurisdiction, licensing, ownership, reputation, sanctions, financial viability, technical compatibility, expected distribution chain, resource requirements, and conflicts.

No content or production access may be provided merely because a prospect is commercially attractive.

12.20 Prospective-Partner Due Diligence

Due diligence and approval under Chapter 7 must occur before contracting or launch. Business Development must identify the legal entity, ownership, licences, brands, domains, markets, platform, aggregators, resellers, and intended onward distribution.

Material changes between prospecting and launch require reassessment.

12.21 Proposals and Commercial Communications

Proposals must be accurate, approved where required, time-limited, and clear about assumptions, exclusions, dependencies, pricing, markets, implementation, service levels, certification, and authority. Personnel must not promise regulatory approval, exclusivity, functionality, launch dates, credits, or player outcomes without authority and evidence.

12.22 Contracting Handover

Before signature, commercial, product, technical, compliance, finance, security, support, data-protection, intellectual-property, and provider responsibilities must be aligned. Final agreed terms must be handed over to the functions responsible for onboarding, billing, delivery, monitoring, and renewal.

Side agreements and undocumented concessions are prohibited.

12.23 Distribution Controls

Content may be supplied only to approved counterparties and authorised brands, domains, platforms, markets, and jurisdictions. Onward distribution requires explicit permission and visibility of the distribution chain.

Technical access controls and ongoing monitoring must support contractual restrictions. Suspected unauthorised distribution must be escalated under Chapters 7 and 11.

12.24 Launch Readiness

Launch approval must confirm executed contract, partner approval, permitted markets and domains, correct certified version, completed testing, production credentials, configuration, monitoring, support readiness, incident contacts, billing setup, documentation, provider readiness, and unresolved-risk disposition.

A launch checklist must be approved and retained.

12.25 Controlled Launch and Early-Life Support

Higher-risk launches should use phased release, restricted scope, enhanced monitoring, rollback arrangements, defined success criteria, and early-life support. Unexpected behaviour must be assessed promptly and may require suspension or rollback.

12.26 Marketing and Product Claims

Claims about licensing, certification, fairness, performance, exclusivity, availability, markets, security, or commercial results must be accurate, current, approved, and supported by evidence. Materials must be clearly B2B and must not imply that Bet Play B.V. is the player-facing operator.

12.27 Demonstrations and Test Environments

Demonstrations must use approved environments, accounts, content, and data. Demo access must be limited, monitored, and separate from production. Demonstrations must not be made available as unlicensed real-money play or expose production credentials, personal data, or restricted content.

12.28 Product Changes

Product and content changes must follow Chapter 13. The Company must assess certification, market permission, contractual notice, partner testing, security, data, support, billing, documentation, and rollback implications before release.

12.29 Product Incidents and Malfunctions

Suspected defects, integrity concerns, systemic errors, or game malfunctions must be handled under Chapters 9, 10, 11, and 13 as applicable. Product owners must support impact analysis, version identification, partner notification, containment, root-cause analysis, and corrective prioritisation.

12.30 Post-Launch Monitoring

Monitoring should cover availability, errors, operator feedback, complaints, malfunctions, configuration drift, usage, market restrictions, certification, support demand, security findings, provider performance, commercial outcomes, and unauthorised distribution.

Material deviations require corrective action or reconsideration of continued availability.

12.31 Product Review and Retirement

Products must be reviewed periodically for legal status, commercial viability, quality, certification, security, provider support, technical debt, complaints, and strategic fit. Retirement must address partner notice, contracts, access removal, data and records, billing, certificates, documentation, support, and replacement options.

12.32 Conflicts of Interest and Incentives

Actual or potential conflicts in product selection, provider choice, commercial terms, or market approval must be declared and managed. Incentives must not encourage bypassing due diligence, inaccurate claims, unauthorised distribution, or concealment of defects.

12.33 Records and Management Information

The Company must retain business cases, approvals, requirements, rights evidence, certificates, market assessments, partner due diligence, proposals, contracts, launch checklists, changes, claims approvals, monitoring, incidents, complaints, retirement decisions, and exceptions.

Management information should cover pipeline quality, approvals, launches, certification status, authorised distribution, product incidents, partner feedback, provider dependencies, revenue performance, and overdue actions.

12.34 Training

Relevant personnel require training on the B2B-only model, licence and market boundaries, partner due diligence, product lifecycle, certification, game integrity, security and privacy by design, intellectual property, claims, contracting authority, distribution controls, and incident escalation.

12.35 Key Controls

Minimum controls are: product inventory; business case; stage gates; market approval; rights and certification evidence; testable requirements; due diligence; accurate proposals; controlled distribution; launch checklist; monitored early life; evidence-backed claims; governed changes; post-launch monitoring; and controlled retirement.

12.36 Exceptions

Exceptions must be justified, risk-assessed, approved, time-limited, and supported by compensating controls. No exception may permit unlicensed distribution, unsupported certification claims, unauthorised intellectual-property use, player-facing operations, bypass of partner due diligence, or release of a materially unsafe or untested product.

12.37 Review and Continuous Improvement

The Director, Product, Business Development, Compliance, and relevant control functions must review this framework at least annually and following material changes, incidents, market expansion, provider changes, or regulatory findings. Amendments must be approved and reflected in workflows, contracts, training, product records, and related chapters.

Technology and Development Operations

13

Chapter 13 – Technology and Development Operations

13.1 Purpose

This chapter establishes Bet Play B.V.'s framework for governing software development, configuration, integration, testing, release, deployment, maintenance, and technical change so that technology remains secure, reliable, traceable, supportable, and consistent with approved gaming content and regulatory obligations.

13.2 Scope and Operating Model

This chapter applies whether technology is developed by Bet Play B.V., Babylon Gaming, contractors, or other providers. It covers source code, configuration, infrastructure as code, integrations, APIs, games and content within scope, build pipelines, environments, databases, technical documentation, deployment artefacts, and changes to production services.

Outsourcing development does not outsource Bet Play B.V.'s responsibility to understand, approve, evidence, and monitor changes affecting its licence, partners, systems, or content.

13.3 Principles

Technology work must use defined ownership, least privilege, segregation of environments and duties, secure design, peer review, proportionate testing, version control, reproducible builds, approved release, rollback capability, protected evidence, and post-release monitoring.

No commercial deadline justifies an uncontrolled production change.

13.4 Roles and Responsibilities

The Director approves material technology strategy, risk acceptance, and exceptional releases. Product owns approved requirements and acceptance criteria. Engineering or provider development teams design and implement changes. Technical leads review architecture and code. Quality assurance provides independent testing proportionate to risk. Security and Compliance assess relevant controls and regulatory impact. Release authority approves deployment. Operations

monitors production and coordinates incidents. Babylon Gaming and providers supply required artefacts, evidence, access, and support.

No person should solely request, develop, approve, deploy, and validate the same material change.

13.5 Technology Inventory and Ownership

The Company must maintain an inventory of material applications, services, repositories, libraries, APIs, environments, pipelines, integrations, domains, certificates, databases, owners, providers, versions, support status, and dependencies.

Unsupported or unowned technology must have a documented treatment plan.

13.6 Development Lifecycle

The lifecycle must include authorised demand, requirements, risk and design assessment, implementation, review, testing, approval, release, deployment, verification, monitoring, documentation, and closure. The depth of control may be proportionate to risk but material stages must remain evidenced.

13.7 Requirements and Traceability

Requirements must be approved, testable, uniquely identifiable, version-controlled, and traceable through implementation, tests, defects, release, and documentation. Changes to game rules, mathematics, outcomes, certification-relevant behaviour, data processing, security, or external interfaces require explicit identification.

13.8 Architecture and Design Review

Material designs must assess security, privacy, resilience, capacity, failure modes, observability, data integrity, backward compatibility, provider dependencies, recovery, certification, support, and decommissioning. Decisions and accepted trade-offs must be recorded.

13.9 Secure Development

Development must follow Chapter 9 and approved secure-coding standards. Inputs, authentication, authorisation, secrets, sessions, errors, logs, encryption, dependencies, and data handling must be designed to prevent foreseeable misuse.

Credentials and production data must not be embedded in code or used in development without explicit, lawful, and protected arrangements.

13.10 Source-Code and Repository Controls

Repositories must use individual access, role-based permissions, multi-factor authentication where supported, protected branches, version history, backup or resilient hosting, and prompt removal of leavers. Direct unreviewed changes to protected production branches are prohibited except under documented emergency procedures.

13.11 Third-Party Components and Supply Chain

Libraries, packages, images, tools, and external code must have an identifiable source, licence, supported version, integrity controls, vulnerability review, and owner. Material dependencies must be inventoried sufficiently to respond to security notices and incidents.

Untrusted or abandoned components must not be introduced without documented risk treatment.

13.12 Development, Test, and Production Separation

Environments must be separated logically or physically according to risk. Production credentials, secrets, and access must not be available routinely in development. Test data should be synthetic or anonymised. Movement of code, configuration, and data between environments must be controlled and logged.

13.13 Change Classification

Changes must be classified as standard, normal, major, or emergency based on risk, impact, complexity, reversibility, partner effect, certification, security, and regulatory significance. Standard changes require a pre-approved repeatable procedure; normal and major changes require case-specific assessment and approval; emergency changes follow section 13.25.

13.14 Change Request

A change record must include purpose, owner, affected services, requirements, risk and impact, dependencies, implementation steps, testing, security and compliance

assessments, partner or provider coordination, data migration, monitoring, rollback, schedule, approvals, and result.

Related tickets, product approvals, incidents, complaints, certificates, and releases must be linked.

13.15 Risk and Impact Assessment

Assessment must consider availability, performance, data integrity, security, privacy, game behaviour, certification, jurisdictions, operator integrations, backward compatibility, billing data, support demand, recovery, and cumulative interaction with other changes.

Material uncertainty requires additional testing, phased release, or deferral.

13.16 Code Review

Material code changes require review by a competent person other than the author. Review must assess correctness, security, maintainability, requirements, tests, logging, failure handling, dependencies, and unintended changes. Review comments and approval must be retained.

13.17 Testing Strategy

Testing must be risk-based and may include unit, integration, system, regression, security, performance, failover, compatibility, data migration, user acceptance, and game-specific testing. Acceptance criteria and expected results must be defined before final approval.

Test failures must not be waived without documented analysis and authority.

13.18 Gaming Content Testing and Certification

Changes affecting game rules, mathematics, return-to-player, random-number generation, outcome determination, critical game flow, or certification-relevant configuration must receive specialist review and external testing or recertification where required.

The deployed artefact and configuration must match the approved and certified version. Version mapping evidence must be retained.

13.19 Defect Management

Defects must be recorded, severity-rated, assigned, prioritised, linked to affected versions, and tracked through correction and verification. Known defects accepted for release require documented impact, workaround, owner, expiry or review date, and approval.

Repeated support tickets or operator complaints must be assessed as possible systemic defects.

13.20 Build and Pipeline Security

Build and deployment pipelines must use controlled access, protected secrets, approved dependencies, integrity checks, reliable logs, and separation of approval from execution where practicable. Build artefacts must be uniquely versioned and protected against unauthorised replacement.

13.21 Release Planning

Release plans must define scope, versions, environments, schedule, dependencies, testing evidence, approvals, partner notice, provider readiness, maintenance window, implementation, monitoring, rollback, support coverage, and success criteria.

Conflicting or overlapping changes must be coordinated.

13.22 Release Approval

Before approval, the release authority must confirm requirements, reviews, tests, unresolved defects, certification, security, privacy, documentation, operational readiness, partner obligations, and rollback. Conditional approvals must be explicit and tracked.

Developers must not self-approve material production releases.

13.23 Deployment

Deployments must follow the approved plan, use authorised accounts and artefacts, record timestamps and operators, preserve previous versions where needed for rollback, and restrict unplanned steps. Material deviation requires pause and reassessment unless emergency action is necessary.

13.24 Post-Deployment Validation and Monitoring

After deployment, the Company must validate version, configuration, functionality, security, integrations, logs, performance, alerts, game behaviour where relevant, and partner connectivity. Enhanced monitoring must continue for a risk-appropriate period.

Failure of acceptance criteria requires rollback, containment, or authorised remediation.

13.25 Emergency Changes

Emergency changes are permitted only to address urgent incidents, security exposure, severe malfunction, legal or regulatory risk, or critical service restoration. They require the highest practicable approval, recorded justification, limited scope, pre-change backup or rollback where possible, testing, active monitoring, and prompt retrospective review.

Emergency status must not be used to avoid ordinary planning.

13.26 Rollback and Recovery

Material changes must have feasible rollback or alternative recovery arrangements. Rollback criteria, authority, data implications, dependencies, timing, and validation must be defined. Where rollback is impossible, the release requires explicit risk acceptance and stronger forward-recovery controls.

13.27 Configuration Management

Production configurations must be versioned or otherwise controlled, approved, documented, and protected. Environment-specific settings, feature flags, endpoints, certificates, market restrictions, game parameters, and secrets must be managed separately from ordinary code where appropriate.

Unauthorised configuration drift must be detected and corrected.

13.28 Database and Data Changes

Schema changes, migrations, corrections, and bulk updates require validation, backup or recovery arrangements, integrity checks, access control, and

reconciliation. Direct production data changes must be exceptional, specifically authorised, executed through traceable methods, and independently verified.

Original game-round or evidential records must not be overwritten to resolve a complaint or incident.

13.29 API and Integration Management

Interfaces must have documented ownership, authentication, authorisation, schemas, versioning, rate and error handling, logging, security, service expectations, and deprecation arrangements. Breaking changes require partner assessment, notice, testing, and controlled migration.

13.30 Provider Development and Deliverables

Where Babylon Gaming or another provider develops or operates technology, Bet Play B.V. must obtain sufficient requirements, versions, change notices, testing evidence, certification, security information, deployment confirmation, incident support, and audit trail to fulfil its own obligations.

Provider confidentiality or proprietary rights do not justify the absence of evidence needed for licence, security, integrity, or partner assurance.

13.31 Technical Documentation

Documentation must cover architecture, interfaces, configurations, build and deployment, operating procedures, monitoring, troubleshooting, recovery, known limitations, versions, and ownership. Documents must be current, access-controlled, and updated as part of change closure.

13.32 Access to Production

Production access must comply with Chapter 9 and must be individually approved, least-privileged, strongly authenticated, logged, periodically reviewed, and removed promptly when no longer needed. Provider access must be time-bound where practicable and linked to an authorised activity.

13.33 Monitoring and Observability

Technology must generate sufficient metrics, logs, traces, health checks, and alerts to detect failure, performance degradation, integration errors, security activity, and

abnormal game behaviour. Monitoring requirements are part of design and release acceptance, not an afterthought.

13.34 Incident, Complaint, and Support Linkage

Technology records must link to relevant Chapter 8 complaints, Chapter 10 incidents, and Chapter 11 tickets. Technical teams must provide evidence-based findings, preserve original data, state limitations, and avoid making player-facing decisions.

13.35 Maintenance and Technical Debt

Supported versions, patches, capacity, certificates, dependencies, and technical debt must be monitored. Deferred work must have risk, owner, target date, and review. Accumulated technical debt that threatens security, reliability, certification, or support must be escalated.

13.36 Decommissioning

Retirement must address contracts, partner notice, dependencies, access, data retention and deletion, code and artefact retention, credentials, domains, certificates, monitoring, billing, documentation, provider obligations, and secure disposal. Decommissioned services must not remain unintentionally exposed.

13.37 Records and Metrics

The Company must retain requirements, designs, reviews, commits, tests, defects, certificates, approvals, builds, releases, deployments, access logs, emergency changes, rollback evidence, incidents, and decommissioning records.

Management information should cover deployment frequency, change success and failure, emergency changes, rollback, defects, vulnerability remediation, release lead time, provider performance, unauthorised changes, technical debt, and overdue actions.

13.38 Quality Assurance and Independent Review

Periodic reviews must test whether changes were authorised, segregated, reviewed, tested, certified, deployed as approved, monitored, documented, and linked to

incidents or complaints. Material systems should receive independent technical or security assurance proportionate to risk.

13.39 Training

Technology personnel require role-appropriate training in secure development, version control, review, testing, gaming-content integrity, certification, privacy, secrets, production access, change management, incident response, evidence preservation, and provider governance.

13.40 Key Controls

Minimum controls are: technology inventory; approved lifecycle; traceable requirements; secure design; protected repositories; dependency governance; environment separation; peer review; risk-based testing; certification mapping; controlled pipelines; independent release approval; monitored deployment; emergency-change review; rollback; protected production access; documentation; and linked incident and complaint evidence.

13.41 Exceptions

Exceptions must identify the control, risk, affected systems and markets, approval, compensating controls, duration, monitoring, and remediation. No exception may authorise unauditable production changes, alteration of original evidence, deployment of uncertified content where certification is required, uncontrolled secrets, or concealment of a defect or incident.

13.42 Review and Continuous Improvement

The Director and relevant Product, Technology, Security, Compliance, Operations, and provider owners must review this framework at least annually and following material incidents, audit findings, platform changes, or regulatory developments. Amendments must be approved and embedded in tools, pipelines, contracts, standards, training, and operating practice.

Commercial Billing, Finance and Accounting Operations

14

Chapter 14 – Commercial Billing, Finance and Accounting Operations

14.1 Purpose

This chapter establishes Bet Play B.V.'s framework for controlling its B2B billing, receivables, supplier payments, corporate bank accounts, accounting records, financial reporting, tax compliance, budgeting, and related financial risks.

The objectives are to ensure that:

- Commercial charges are supported by approved contracts and reliable source data.
- Invoices, credit notes, payments, and accounting entries are accurate, complete, authorised, and traceable.
- Company funds and bank accounts are protected against error, misuse, fraud, and unauthorised access.
- Duties are segregated so far as proportionate to the Company's size and operating model.
- Receivables, liabilities, cash positions, disputes, and exceptions are monitored.
- Financial activity is assessed for AML/CFT/CPF, sanctions, fraud, tax, regulatory, and contractual implications.
- Financial records are retained and made available for audit, regulatory review, and management oversight.
- Dependencies on Babylon Gaming, business partners, banks, accountants, and other service providers are governed appropriately.

14.2 B2B Financial Operating Model

Bet Play B.V. operates exclusively on a B2B basis. Its financial activities relate to its own commercial and corporate obligations, including:

- Billing contracted business partners.
- Collecting B2B receivables.
- Paying suppliers, professional advisers, authorities, and other approved creditors.

- Paying taxes, licence fees, payroll-related liabilities, and corporate expenses where applicable.
- Reconciling its bank accounts, invoices, accounting records, and contractual settlement data.
- Managing authorised refunds, credits, intercompany balances, and other corporate transactions.

The Company does not:

- Accept or hold player deposits.
- Process player withdrawals.
- Maintain player wallets or balances.
- Authorise or settle wagers.
- Process player-facing payment transactions.
- Contract with payment service providers for player deposits or withdrawals.
- Determine whether money is payable to a player.
- Perform cashier, chargeback, or payment-support functions for players.

Those responsibilities remain with the relevant B2C operator. The use of player activity, game-round information, gross gaming revenue, net gaming revenue, or similar data to calculate a B2B contractual fee does not make Bet Play B.V. responsible for the underlying player funds or transactions.

14.3 Scope

This chapter applies to:

- Customer and business-partner invoicing.
- Usage-based, fixed-fee, minimum-guarantee, revenue-share, and other contractual charges.
- Accounts receivable and collection activity.
- Supplier invoices and accounts payable.
- Corporate payments and expense reimbursements.
- Bank accounts and online-banking access.
- Cash-flow and liquidity monitoring.
- Credit notes, refunds, rebates, discounts, and write-offs.
- Foreign-currency transactions.
- Taxes, statutory charges, licence fees, and other public liabilities.

- Intercompany and related-party transactions.
- Financial reconciliations and accounting entries.
- Financial reporting and management information.
- Fraud, financial-crime, and sanctions controls relevant to corporate transactions.
- Financial records and audit trails.

This chapter must be read with Chapter 7 on business-partner oversight, Chapter 8 on complaints and disputes, Chapter 9 on information security and data protection, and Chapter 10 on incident management and business continuity.

14.4 Applicable Framework

Financial activities must be conducted consistently with:

- Applicable Curaçao legislation and tax requirements.
- Requirements and guidance of the Curaçao Gaming Authority.
- The Company's licence conditions.
- Applicable AML/CFT/CPF and sanctions requirements.
- Applicable accounting and recordkeeping requirements.
- Contracts entered into by the Company.
- Babylon Gaming's applicable contractual and operational requirements.
- Requirements of banks and other financial institutions used by the Company.
- Applicable data-protection and information-security requirements.
- The Company's internal policies, delegated authorities, and procedures.

Material uncertainty must be referred to the Director, Compliance Officer, MLRO, external accountant, auditor, tax adviser, or legal counsel as appropriate.

14.5 Core Financial-Control Principles

The Company must apply the following principles:

- No financial obligation may be created or paid without a legitimate business purpose.
- Charges and payments must be supported by sufficient documentation.
- Approval authority must be clear, current, and proportionate to value and risk.
- No person should control initiation, approval, execution, recording, and reconciliation of the same transaction.

- Changes to beneficiary or bank-account information require independent verification.
- Accounting records must reflect the substance of transactions accurately.
- Exceptions must be visible, documented, investigated, and resolved.
- Commercial urgency must not override financial-crime, sanctions, fraud, or approval controls.
- Company funds must not be mixed with player funds or held on behalf of a B2C operator's players.

14.6 Roles and Responsibilities

14.6.1 Director

The Director is responsible for:

- Approving the financial-control framework and delegated authorities.
- Approving bank-account openings, closures, and authorised signatories.
- Approving material contracts, payments, credits, refunds, write-offs, and settlements within the applicable authority framework.
- Reviewing material receivables, liquidity risks, fraud concerns, and financial exceptions.
- Ensuring that adequate resources and independent oversight are available.
- Reviewing financial management information.

14.6.2 Finance Function

- The finance function is responsible for:
- Maintaining accurate accounting records.
- Preparing and issuing authorised invoices.
- Validating supplier invoices and payment requests.
- Monitoring receivables and liabilities.
- Preparing reconciliations.
- Maintaining supporting records and audit trails.
- Escalating discrepancies, overdue balances, unusual transactions, and control failures.
- Preparing financial and tax information for review and filing.

14.6.3 Compliance Officer

The Compliance Officer is responsible for:

- Assessing regulatory and licence implications of material financial matters.
- Supporting due diligence on financial counterparties.
- Reviewing unusual or higher-risk financial arrangements where required.
- Coordinating regulatory notification where applicable.
- Monitoring relevant exceptions and corrective actions.

14.6.4 MLRO

The MLRO is responsible for:

- Assessing suspicious corporate payments or receipts.
- Determining whether enhanced review, restriction, rejection, freezing, or reporting is required.
- Managing AML/CFT/CPF, sanctions, and tipping-off considerations.
- Maintaining appropriate confidential records of financial-crime assessments.

14.6.5 Account Management and Commercial Personnel

Account Management and commercial personnel are responsible for:

- Ensuring commercial terms are documented and approved.
- Providing accurate billing instructions and relevant contractual evidence.
- Confirming authorised business-partner contacts.
- Supporting resolution of billing queries and overdue receivables.
- Avoiding unauthorised amendments, discounts, credits, or payment commitments.

14.6.6 All Personnel

All personnel must protect financial information, follow delegated authorities, preserve records, report suspected fraud or error, and avoid committing the Company to expenditure without approval.

14.7 Delegated Financial Authority

The Company must maintain a current delegated-authority matrix covering, as applicable:

- Contract approval.
- Purchase commitments.
- Invoice issuance and adjustment.
- Supplier payment approval.
- Bank-transfer release.
- Credit notes and refunds.
- Discounts and rebates.
- Debt write-offs.
- Expense reimbursement.
- Intercompany and related-party transactions.
- Settlements of disputes.
- Emergency payments.

The matrix must define monetary thresholds, required approvers, prohibited self-approval, and circumstances requiring Director approval.

Transactions must not be divided into smaller amounts to avoid an approval threshold.

14.8 Segregation of Duties

So far as proportionate and practicable, the following duties must be separated:

- Creating or changing counterparty master data.
- Preparing an invoice or payment.
- Approving an invoice or payment.
- Releasing a bank transaction.
- Recording the transaction in the accounting system.
- Reconciling the relevant account.
- Approving a credit, refund, or write-off.

Where staffing limitations prevent full segregation, the limitation must be documented and compensating controls applied, such as Director review, dual authorisation, independent reconciliation, transaction alerts, or periodic external review.

14.9 Contract-to-Billing Control

No business partner may be invoiced unless there is an approved contractual or other documented basis for the charge.

Before billing begins, the responsible functions must confirm:

- The correct legal entity and billing details.
- The effective contract and amendments.
- The products, services, brands, domains, markets, and currencies covered.
- The pricing model and applicable rates.
- Any minimum fees, caps, tiers, discounts, rebates, or taxes.
- The billing frequency and period.
- The required source data and calculation method.
- The payment terms and permitted payment accounts.
- Any invoice-dispute or notice period.
- Any reporting or supporting-document requirements.

Changes to commercial terms must be approved and communicated to Finance before being applied.

14.10 Billing Source Data

Where charges depend on usage, game activity, revenue, or other operational data, the Company must identify the authoritative data source and responsible data owner.

Controls must provide reasonable assurance that source data is:

- Complete for the billing period.
- Attributable to the correct business partner, brand, domain, market, product, and contract.
- Based on the correct time zone, currency, and cut-off.
- Protected against unauthorised alteration.
- Reconciled to relevant provider or partner data where required.
- Capable of being reproduced and explained.

Missing, duplicated, late, or inconsistent data must be investigated before invoicing or handled through a documented and approved estimate or adjustment process.

14.11 Revenue-Share and Usage-Based Calculations

Where B2B fees are calculated using player-related operational data, Finance must apply the contractual definition exactly and must not assume that terms such as gross gaming revenue or net gaming revenue have a universal meaning.

The calculation must consider, where contractually relevant:

- Stakes or turnover.
- Winnings.
- Voids, cancellations, rollbacks, or interrupted rounds.
- Bonuses or promotional deductions.
- Taxes, jackpot contributions, platform charges, or agreed exclusions.
- Currency conversion.
- Negative carry-forward arrangements.
- Minimum guarantees, floors, caps, or tiered rates.
- Adjustments from earlier periods.

These calculations determine only the B2B amount owed under the contract. They do not constitute processing, custody, or settlement of player funds.

14.12 Invoice Preparation and Review

Each invoice must be prepared from approved terms and validated source data.

Before issue, the invoice must be reviewed for:

- Correct legal entity and address.
- Unique invoice number.
- Correct invoice and service dates.
- Contract and partner reference.
- Accurate description of services.
- Correct quantities, rates, and calculations.
- Currency and tax treatment.
- Payment terms and due date.
- Approved Company bank details.
- Required supporting schedules.
- Appropriate approval.

Material manual adjustments must be explained and independently reviewed.

14.13 Invoice Issuance and Delivery

Invoices must be issued through an approved channel to an authorised business-partner contact.

The Company must retain evidence of issuance and, where relevant, receipt. Sensitive invoice information and bank details must be transmitted using appropriately secure methods.

Any request to resend an invoice to a new contact or account must be assessed for authenticity and confidentiality risk.

14.14 Credit Notes, Rebates, Refunds, and Adjustments

A credit note, rebate, corporate refund, or billing adjustment must:

- Have a documented reason.
- Refer to the original transaction where applicable.
- Be calculated accurately.
- Receive approval under the delegated-authority matrix.
- Be recorded in the accounting system.
- Preserve the original invoice and audit trail.
- Be reflected in relevant reconciliations and tax records.

An issued invoice must not be deleted, overwritten, or informally replaced to conceal an error.

No refund may be sent to an unverified third-party account merely because a business partner requests it.

14.15 Accounts Receivable

Finance must maintain an accurate receivables ledger showing amounts invoiced, received, credited, disputed, overdue, and written off.

Receivables must be monitored according to due date and risk. Collection activity should be proportionate and documented and may include:

- Payment reminders.
- Confirmation of invoice receipt.
- Reconciliation with the business partner.
- Escalation to Account Management.
- Formal demand under the contract.

- Credit restriction or service limitation where contractually permitted.
- Referral to the Director, legal counsel, or a collection specialist.
- Suspension or termination under Chapter 7 where justified.

Collection action must not obscure a genuine complaint or invoice dispute.

14.16 Credit Risk and Overdue Debt

Before or during a business relationship, the Company should assess credit risk proportionately by considering:

- Legal identity and ownership.
- Payment history.
- Financial condition and adverse information.
- Expected exposure and concentration.
- Jurisdiction and banking arrangements.
- Contractual security, prepayment, deposit, or guarantee arrangements.
- Unresolved disputes or regulatory concerns.

Material overdue balances, repeated late payment, broken payment promises, or signs of financial distress must inform ongoing due diligence under Chapter 7.

14.17 Billing Disputes

Billing disputes must be recorded, investigated, and resolved under Chapter 8.

The Company must identify:

- The undisputed and disputed amounts.
- The contractual basis for the charge.
- The relevant source data and calculation.
- Applicable notice periods.
- Whether collection activity should continue for the undisputed balance.
- Whether a provision, credit, correction, or escalation is required.

A disputed invoice must not be altered without approval and a complete audit trail.

14.18 Supplier Onboarding and Master Data

Before a supplier is paid, the Company must verify, proportionately to risk:

- Its legal name and registration information.
- The legitimacy of the service or goods supplied.
- The contract, engagement, or purchase approval.

- Its tax and invoicing details where applicable.
- Its bank-account ownership and payment instructions.
- Relevant conflicts of interest, sanctions, or adverse information.
- Whether enhanced due diligence is required.

Creation or amendment of supplier master data must be authorised and traceable.

14.19 Supplier Invoice Validation

Before payment, a supplier invoice must be checked for:

- Authenticity and correct supplier identity.
- Approved contractual or purchase basis.
- Evidence that the goods or services were received.
- Accuracy of amounts, rates, currency, and tax.
- Duplicate invoice or payment risk.
- Correct payment terms and beneficiary account.
- Required approval.
- Unusual descriptions, urgency, routing, or payment requests.

An invoice must not be approved solely by the person who supplied it or benefits directly from its payment.

14.20 Payment Preparation, Approval, and Release

Corporate payments must be prepared from validated documentation and released only by authorised persons.

Controls must include, as appropriate:

- Payment-batch review.
- Dual authorisation.
- Verification of beneficiary, amount, currency, purpose, and due date.
- Comparison with the approved invoice or obligation.
- Review of bank fees and exchange rates.
- Confirmation that sanctions or financial-crime concerns have been addressed.
- Retention of bank confirmation and approval evidence.

Blank approvals, shared banking credentials, or retrospective routine approvals are prohibited.

14.21 Bank-Account and Beneficiary Changes

A request to change payment instructions presents a heightened fraud risk.

Before using new or amended bank details, the Company must:

- Treat the request independently from the invoice or email in which it appears.
- Verify the change with a known authorised contact using a trusted channel.
- Check the account holder, bank, country, and currency for consistency.
- Apply appropriate sanctions and risk screening.
- Record who requested, verified, approved, and implemented the change.
- Consider a cooling-off period or test payment where proportionate.

Personnel must not rely solely on reply email, caller identification, or documents supplied with the change request.

14.22 Corporate Bank-Account Controls

Bank accounts may be opened or closed only with Director approval and appropriate documentation.

The Company must maintain a register of:

- Bank and account name.
- Account number or identifier.
- Currency and purpose.
- Opening and closing dates.
- Authorised users and signatories.
- Transaction and approval limits.
- Authentication devices and access arrangements.

Access must be individual, least-privilege, protected by strong authentication, and removed promptly when no longer required. Bank alerts should be enabled for material or unusual activity where available.

Company accounts must not be used as player-funds accounts, pass-through accounts for business partners, or personal accounts of Directors, employees, or contractors.

14.23 Incoming Receipts

Incoming receipts must be matched promptly to the correct payer, invoice, and business relationship.

Unidentified, unexpected, excess, third-party, or misdirected receipts must be investigated. The Company must not automatically return funds to new instructions supplied by the sender; the source and lawful return destination must first be verified.

Suspicious or unexplained receipts must be escalated to the MLRO before further action where appropriate.

14.24 Reconciliations

Reconciliations must be performed at a frequency proportionate to transaction volume and risk.

They should include, as applicable:

- Bank accounts to the general ledger.
- Accounts receivable to issued invoices and receipts.
- Accounts payable to supplier invoices and payments.
- Billing source data to invoice calculations.
- Partner or Babylon Gaming statements to Company records.
- Tax control accounts to filings and payments.
- Intercompany balances between relevant entities.
- Foreign-currency balances and revaluations.

Reconciliations must be dated, prepared by an identifiable person, reviewed independently where practicable, and supported by evidence. Unreconciled items must be aged, investigated, assigned, and resolved.

14.25 Babylon Gaming and Other Provider Dependencies

Where billing, settlement, technical data, or supplier charges depend on Babylon Gaming or another provider, the Company must:

- Document the respective responsibilities and authoritative records.
- Obtain information through approved channels.

- Validate that reports cover the correct partner, products, markets, currencies, and period.
- Reconcile material differences.
- Escalate late, incomplete, inconsistent, or unexplained information.
- Avoid issuing unsupported final calculations.
- Preserve provider reports and correspondence.
- Monitor corrective actions and recurring discrepancies.

Reliance on a provider does not remove Bet Play B.V.'s responsibility for the accuracy of its own invoices, payments, accounting records, and regulatory reporting.

14.26 Foreign Currency

Foreign-currency transactions must use an approved exchange-rate source and the contractual rate basis where specified.

The Company must document:

- The transaction currency.
- The accounting currency.
- The rate and date applied.
- Material conversion fees or gains and losses.
- Any hedging arrangement, where applicable.

Manual or exceptional exchange rates require documented justification and approval.

14.27 Taxes, Licence Fees, and Statutory Payments

The Company must identify, calculate, approve, file, and pay applicable taxes, licence fees, and statutory charges accurately and on time.

Responsibilities and deadlines must be documented and monitored. Information submitted by an external accountant or adviser remains subject to appropriate Company review.

Uncertainty, missed deadlines, material errors, assessments, penalties, or disputes must be escalated promptly.

14.28 Expenses and Reimbursements

Business expenses must be reasonable, supported, related to Company activity, and approved by a person who did not incur the expense.

Expense claims should include:

- Date and business purpose.
- Amount and currency.
- Receipt or other supporting evidence.
- Relevant attendees or counterparties where necessary.
- Required approval.

Personal, unsupported, duplicate, or prohibited expenses must not be reimbursed. Exceptions require documented justification and approval.

14.29 Intercompany and Related-Party Transactions

Intercompany and related-party transactions must:

- Have a legitimate and documented business purpose.
- Be supported by an agreement or other appropriate evidence.
- Be approved without conflicted self-approval.
- Be recorded accurately and transparently.
- Receive appropriate tax, transfer-pricing, legal, and regulatory consideration.
- Be reconciled periodically.

Conflicts of interest must be disclosed and managed.

14.30 Prohibited and Restricted Practices

The Company prohibits:

- Fictitious, misleading, backdated, or duplicate invoices.
- Off-book accounts or undisclosed funds.
- Payments without a legitimate business purpose.
- Payments to unverified third parties without documented justification and approval.
- Use of personal bank accounts for Company receipts or payments.
- Shared banking credentials or authentication devices.
- Splitting transactions to evade approval limits.

- Altering records to conceal an error, dispute, or unauthorised payment.
- Secret commissions, kickbacks, bribes, or facilitation payments.
- Processing or holding player money.
- Routing money for a business partner without a documented lawful basis and appropriate approval.

14.31 Fraud Prevention and Payment Diversion

Personnel must remain alert to:

- Impersonation of Directors, employees, suppliers, or business partners.
- Business-email compromise.
- Urgent or confidential payment demands.
- New bank details combined with pressure to pay quickly.
- Requests to bypass normal approvers.
- Invoices inconsistent with the contract or prior activity.
- Duplicate or altered invoices.
- Overpayment followed by a request to refund another account.
- Unusual third-party payments.
- Unexpected changes in jurisdiction, currency, beneficiary, or payment route.

Suspected fraud must be escalated immediately. Payment release should be stopped where safe and lawful, evidence preserved, bank contact considered, and the incident managed under Chapter 10.

14.32 AML/CFT/CPF and Sanctions Escalation

Financial activity must be assessed in conjunction with the Company's AML/CFT/CPF and sanctions framework.

The MLRO must be informed promptly of activity involving:

- An unexplained payer or beneficiary.
- An unusual third-party payment.
- Payments inconsistent with the known business model.
- Complex or opaque payment routing.
- High-risk or sanctioned jurisdictions or persons.

- Attempts to disguise the source, destination, or purpose of funds.
- Repeated overpayments, reversals, or refund requests.
- Suspected fraud, corruption, or criminal property.

Personnel must not tip off a counterparty or disclose a confidential report or investigation. Commercial settlement, refund, or account closure must not proceed where the MLRO has imposed a lawful restriction.

14.33 Errors, Failed Payments, and Exceptions

Payment failures, duplicate payments, incorrect receipts, mispostings, rejected transfers, and other exceptions must be recorded and resolved promptly.

The Company must:

- Identify the cause and affected amount.
- Preserve relevant instructions, approvals, and bank records.
- Take proportionate recovery or containment action.
- Correct the accounting records transparently.
- Notify affected parties where appropriate.
- Assess fraud, regulatory, contractual, tax, and reporting implications.
- Conduct root-cause analysis for material or recurring failures.

14.34 Emergency Payments

An emergency payment procedure may be used only where delay would expose the Company to material harm and the ordinary process cannot reasonably be completed.

The payment must still have:

- A verified beneficiary.
- A legitimate and documented purpose.
- Available supporting evidence.
- Approval at the level required for the risk and value.
- Appropriate financial-crime and sanctions consideration.
- Prompt retrospective completion of the normal records and independent review.

Convenience, poor planning, or avoidable lateness does not constitute an emergency.

14.35 Cash-Flow and Liquidity Monitoring

The Company must monitor expected receipts, committed payments, taxes, licence fees, supplier obligations, and other foreseeable cash needs.

Material liquidity pressure must be escalated to the Director. Management must consider whether it affects:

- The Company's ability to meet obligations as they fall due.
- Continuity of critical services.
- Regulatory or licence requirements.
- The need to restrict expenditure or obtain lawful financing.
- Business-partner, supplier, or regulator notification.

14.36 Financial Close and Accounting Entries

Period-end procedures must ensure that financial activity is recorded completely and in the correct period.

Controls should cover:

- Cut-off of invoices and expenses.
- Accruals and prepayments.
- Deferred or unbilled revenue where applicable.
- Provisions and bad-debt assessments.
- Foreign-currency revaluation.
- Reconciliation completion.
- Review of unusual journals and suspense accounts.
- Management review of material variances.

Manual journal entries must state their purpose, include supporting evidence, and receive appropriate review.

14.37 Management Information

Financial management information should include, as applicable:

- Revenue and costs against budget or prior period.
- Invoices issued and amounts collected.
- Receivables ageing and overdue debt.

- Disputed invoices and credit notes.
- Supplier liabilities and payment status.
- Cash position and forecast.
- Material foreign-currency exposure.
- Unreconciled items.
- Write-offs, refunds, and exceptional payments.
- Tax and licence-fee deadlines.
- Fraud alerts and unusual transactions.
- Control exceptions and overdue corrective actions.
- Concentration by material business partner or supplier.

Material issues must be escalated immediately rather than deferred to periodic reporting.

14.38 Recordkeeping and Audit Trail

The Company must retain complete and retrievable records of:

- Contracts and commercial approvals.
- Billing instructions and source data.
- Calculations and invoices.
- Credit notes, rebates, refunds, and write-offs.
- Supplier onboarding and invoices.
- Payment preparation, approval, and bank confirmation.
- Receipts and allocation records.
- Bank statements and reconciliations.
- Accounting entries and supporting schedules.
- Tax filings and statutory payments.
- Financial disputes and correspondence.
- Fraud, AML/CFT/CPF, and sanctions escalations, subject to access restrictions.
- Exceptions, investigations, and corrective actions.

Records must be accurate, dated, attributable, access-controlled, protected from unauthorised alteration, and retained for the period required by law, regulation, contract, and Company policy.

14.39 Information Security and Access

Financial systems and records must be protected under Chapter 9.

Controls must include:

- Individual user accounts.
- Role-based access.
- Strong authentication.
- Periodic access review.
- Prompt removal or amendment of access.
- Secure storage and transmission.
- Logging of material changes and approvals.
- Controlled export and sharing of financial data.
- Backup and recovery appropriate to criticality.

Banking, accounting, and billing access must not be shared.

14.40 Business Continuity

The Company must maintain proportionate arrangements for continuing critical billing and corporate-payment activities during system, provider, personnel, or banking disruption.

Arrangements should identify:

- Critical deadlines and obligations.
- Alternative authorised personnel.
- Secure access to essential records.
- Manual or alternative procedures.
- Bank and provider contacts.
- Approval and fraud controls that remain mandatory.
- Recovery and reconciliation after normal operations resume.

Business continuity must not be used to waive beneficiary verification, delegated authority, or financial-crime controls.

14.41 Monitoring and Quality Assurance

Periodic review should assess whether:

- Invoices agree to contracts and source data.
- Receipts and payments are recorded accurately.
- Approvals comply with delegated authority.
- Segregation of duties is operating effectively.
- Bank and beneficiary changes were verified independently.
- Reconciliations are timely and complete.
- Exceptions and overdue items are resolved.
- Access rights remain appropriate.
- Records support the transaction trail.
- Required tax, contractual, and regulatory obligations were met.
- Provider dependencies and recurring discrepancies are controlled.

Deficiencies must be documented, assigned, remediated, and verified.

14.42 Key Controls

The Company's minimum financial controls are:

- Bet Play B.V. handles only its own B2B and corporate financial activity.
- Player funds and player transactions are excluded from its operations.
- Billing is based on approved contracts and validated source data.
- Revenue-share calculations are distinguished from player payment processing.
- Invoices and adjustments are reviewed and traceable.
- Supplier identities, obligations, and bank details are verified.
- Payments require documented approval and, where appropriate, dual authorisation.
- Bank-account and beneficiary changes receive independent verification.
- Duties are segregated or compensating controls are documented.
- Receivables and overdue debts are monitored.
- Bank, ledger, billing, and provider records are reconciled.
- Unusual transactions are escalated to the MLRO.
- Fraud indicators and payment-diversion attempts are addressed immediately.
- Access to banking and financial systems is individual and restricted.
- Financial records are complete, protected, and retrievable.
- Material exceptions and corrective actions are monitored to closure.

14.43 Exceptions

Any exception to the normal financial-control process must:

- Be justified and documented.
- Identify the requirement affected.
- Assess the financial, fraud, regulatory, and operational risk.
- Receive approval at the appropriate level.
- Include compensating controls.
- Be limited in scope and duration.
- Be reviewed after use where material.

An exception must not permit:

- Processing or holding player funds.
- Circumvention of sanctions or AML/CFT/CPF controls.
- Concealment of a transaction or accounting entry.
- Self-approval of a conflicted transaction.
- Use of an unverified beneficiary.
- Falsification, destruction, or unauthorised alteration of records.
- Splitting of transactions to evade authority limits.

14.44 Training

Personnel involved in contracting, billing, collections, accounting, payments, or reconciliation must receive role-appropriate training covering:

- The Company's B2B-only financial model.
- Delegated authority and segregation of duties.
- Contract-to-billing controls.
- Invoice and supplier validation.
- Bank-detail verification.
- Fraud and business-email-compromise indicators.
- AML/CFT/CPF, sanctions, and tipping-off restrictions.
- Secure handling of financial information.
- Reconciliation and exception management.
- Complaints and billing disputes.
- Recordkeeping and escalation.

Training must be refreshed following material changes to requirements, systems, banking arrangements, responsibilities, or procedures.

14.45 Accounting Policies and Standards

The Company must maintain approved accounting policies appropriate to its legal form, reporting obligations, business model, and applicable accounting framework. Policies must address revenue recognition, expenses, foreign currency, related parties, estimates, materiality, accruals, prepayments, provisions, fixed assets, impairment, tax, and correction of errors.

Departures from an approved policy require documented technical analysis and appropriate approval. Accounting treatment must reflect the substance of transactions and must not be selected to obscure liabilities, accelerate unsupported revenue, or conceal related-party activity.

14.46 Chart of Accounts and Ledger Governance

The chart of accounts must be structured, documented, and controlled so transactions are classified consistently and financial statements can be supported. Creation, renaming, mapping, disabling, or merging of ledger accounts requires authorised review.

Suspense, clearing, and manual adjustment accounts must have owners, defined purposes, regular reconciliation, and timely clearance. Unsupported balances must be escalated.

14.47 Revenue Recognition

Revenue must be recognised only when supported by an approved contract, reliable measurement, performance evidence, and the applicable accounting policy. Finance must assess fixed fees, minimum guarantees, revenue share, usage charges, credits, rebates, variable consideration, disputed amounts, and contract modifications.

Billing and accounting recognition must be reconciled, but an issued invoice must not automatically be treated as earned revenue where the applicable criteria are not met.

14.48 Accruals, Prepayments, Estimates, and Provisions

Period-end accruals, prepayments, estimates, and provisions must have documented calculation, business rationale, source evidence, preparer, reviewer,

reversal or utilisation method, and reassessment date. Material estimates must be reviewed for bias and consistency with current information.

Old or unexplained balances must not be carried forward without investigation.

14.49 Fixed Assets and Intangible Assets

Material fixed and intangible assets must be recorded in an asset register showing description, owner, acquisition date, cost, location or repository, useful life, depreciation or amortisation method, accumulated charge, impairment, disposal, and supporting approval.

Capitalisation decisions for software, development, licences, equipment, or similar expenditure must follow the approved accounting policy. Asset existence and continued use must be reviewed periodically.

14.50 Period-End and Year-End Close

The Company must maintain a close checklist with responsibilities, deadlines, dependencies, reconciliations, cut-off procedures, journal controls, review evidence, issue tracking, and approval. The close must address bank balances, receivables, payables, revenue, expenses, taxes, payroll-related balances where applicable, intercompany accounts, accruals, prepayments, provisions, assets, foreign currency, and subsequent events.

The ledger must be restricted from unauthorised changes after close. Post-close adjustments require documented reason and approval.

14.51 Journal Entries

Manual journals must state the purpose, accounts, period, amount, supporting evidence, preparer, and approver. Material, unusual, late, round-sum, suspense, related-party, revenue, and management-directed journals require enhanced review.

No person may prepare and approve the same material manual journal. Recurring journals must be reviewed periodically for continued validity.

14.52 Financial Statements and Management Accounts

Financial statements and management accounts must be prepared from reconciled records and reviewed for completeness, consistency, material movements,

classification, disclosures, estimates, going concern, and subsequent events. The Director must approve statutory financial statements before filing or issue.

Information supplied to regulators, banks, auditors, tax authorities, shareholders, and counterparties must be consistent with the approved records or differences must be explained.

14.53 Budgeting, Forecasting, and Variance Analysis

The Company should maintain proportionate budgets and cash-flow forecasts based on documented assumptions. Actual performance must be compared with budget and prior periods, with material revenue, cost, liquidity, collection, tax, and provider variances investigated.

Forecasts must be updated when assumptions change materially and must distinguish committed amounts from opportunities or uncertain estimates.

14.54 Going Concern and Capital Adequacy

Management must assess the Company's ability to meet obligations and continue operations over an appropriate forward-looking period. The assessment should consider cash, overdue receivables, contractual commitments, taxes, licence costs, provider dependencies, concentration, disputes, contingencies, financing, stress scenarios, and operational disruption.

Material uncertainty must be escalated to the Director and relevant advisers and reflected in reporting where required.

14.55 External Accountants, Audit, and Tax Compliance

External accountants, auditors, and tax advisers must be competent, appropriately engaged, given controlled access to complete information, and subject to confidentiality and security requirements. Management retains responsibility for records, judgments, filings, and representations.

Audit and adviser requests, proposed adjustments, findings, management representations, tax returns, filing approvals, deadlines, payments, and corrective actions must be tracked. The Company must not withhold material information or provide misleading evidence.

14.56 Review and Continuous Improvement

The Director, supported by Finance and the Compliance Officer, must review this framework at least annually and following a material change or incident.

The review should consider:

- Changes in legislation, tax rules, licence conditions, or regulatory expectations.
- Changes to the business model, contracts, pricing, systems, banks, or providers.
- Billing accuracy and collection performance.
- Overdue and disputed receivables.
- Payment errors, fraud attempts, and unusual transactions.
- Reconciliation exceptions.
- Tax, audit, and regulatory findings.
- Babylon Gaming and other provider dependencies.
- Access-control and segregation-of-duty limitations.
- Business-continuity performance.
- Complaints, incidents, root causes, and overdue corrective actions.
- Whether procedures reflect actual practice.
- Accounting policies, close quality, audit and tax findings, budgeting, and going-concern assessment.

Material amendments must be approved by the Director and communicated to affected personnel.

Operational Manual Closing Statement

This Operational Manual establishes the principal governance arrangements, responsibilities, procedures, and internal controls applicable to Bet Play B.V.'s B2B gaming activities.

The Manual must be read and applied as a whole. No chapter, procedure, commercial objective, or operational instruction may be interpreted in a manner that overrides applicable law, licence conditions, regulatory requirements, contractual obligations, or an approved internal control.

Bet Play B.V. is committed to conducting its activities with integrity, accountability, transparency, security, and appropriate regulatory oversight. In particular, the Company will:

- Operate strictly within its authorised B2B business model.
- Maintain a clear separation between its responsibilities and those of B2C operators.
- Protect the integrity, security, and lawful distribution of its gaming content.
- Conduct appropriate due diligence and ongoing monitoring of business partners.
- Maintain effective AML/CFT/CPF and sanctions controls.
- Investigate material complaints, incidents, malfunctions, and control failures promptly.
- Preserve complete, accurate, and retrievable records.
- Maintain appropriate financial, technical, security, and operational controls.
- Cooperate openly and promptly with competent authorities.
- Identify and address emerging risks.
- Promote a culture in which personnel raise concerns without fear of retaliation.
- Review and improve its governance arrangements continuously.

All Directors, officers, employees, contractors, and other persons acting on behalf of Bet Play B.V. are responsible for understanding and complying with the provisions relevant to their roles. A person who is uncertain about the correct course of action must seek guidance from the Director, Compliance Officer, MLRO, or another appropriately authorised person before proceeding.

Actual or suspected breaches of this Manual must be reported promptly. Material breaches must be investigated, documented, escalated, and remediated. Where

required, the Company must notify the Curaçao Gaming Authority, another competent authority, an affected business partner, Babylon Gaming, or another entitled party.

Exceptions to this Manual are permitted only where they are lawful, justified, risk-assessed, documented, time-limited, supported by appropriate compensating controls, and approved at the required level. No exception may be used to conceal misconduct, avoid regulatory obligations, suppress lawful reporting, compromise an investigation, or expose the Company to unacceptable risk.

The Manual must be reviewed at least annually and whenever there is a material change to:

- Applicable legislation or regulatory requirements.
- The Company's licence conditions.
- The Company's ownership, governance, or organisational structure.
- Its products, technology, systems, or operating model.
- Its relationship with Babylon Gaming or another material provider.
- The markets, jurisdictions, or business partners it serves.
- Its risk assessment.
- Its contractual obligations.
- A material incident, complaint, audit finding, regulatory enquiry, or control failure.

Amendments must be approved by the Director or other designated governing authority, recorded in the document-control history, and communicated to affected personnel. Relevant training must be provided where changes affect roles, responsibilities, procedures, or controls.

This Manual does not replace professional legal, regulatory, accounting, technical, security, or compliance advice where specialist advice is required. If any provision conflicts with applicable law, a licence condition, or a binding regulatory direction, the applicable legal or regulatory requirement takes precedence and the Manual must be amended promptly.

Through approval of this Manual, the management of Bet Play B.V. confirms its commitment to providing sufficient authority, independence, information, systems, and resources for the effective operation of the controls described herein.

-----END OF OPERATIONAL MANUAL -----