



Mirage Corporation N.V.

OPERATIONS MANUAL

V 1.0

CONTENTS

Executive Introduction.....	7
1. Introduction.....	9
1.1 Purpose of the Manual.....	9
1.2 Company Overview.....	9
1.3 Business Objectives.....	10
1.4 Mission, Vision and Core Values.....	11
1.5 Business Model Overview.....	12
1.6 Governance Principles.....	15
Corporate Governance and Organisational Structure.....	17
2.1 Purpose.....	17
2.1 Ownership Structure.....	17
2.2 Governance Framework.....	19
2.3 Governance Responsibilities.....	20
2.5 Decision-Making and Delegation of Authority.....	22
2.6 Governance Reporting.....	23
2.7 Internal Control Environment.....	24
2.8 Governance Principles.....	25
3. Risk Management Framework.....	27
3.1 Purpose.....	27
3.2 Risk Management Objectives.....	27
3.3 Risk Management Principles.....	28
3.3 Risk Governance.....	29
3.4 Risk Governance.....	31
3.5 Risk Tolerance.....	34
3.6 Risk-Based Approach.....	35
3.7 Risk Assessment Process.....	36
3.8 Key Risk Categories.....	39
3.9 Financial Crime Risk Assessment.....	42
3.10 Risk Monitoring and Reporting.....	43
3.11 Risk Register.....	45
3.12 Key Controls.....	46
3.13 Continuous Improvement.....	46
4. Compliance Framework.....	49
4.1 Purpose.....	49
4.2 Compliance Objectives.....	49

4.3 Compliance Governance	50
4.4 Compliance Function	52
4.5 Money Laundering Reporting Officer (MLRO)	52
4.6 Regulatory Compliance Obligations	53
4.7 Policies and Procedures	54
4.8 Compliance Monitoring and Testing	54
4.9 Reporting and Escalation	56
4.10 Training and Awareness	57
4.11 Record Keeping	58
4.12 Key Controls	59
4.13 Continuous Improvement	59
5. Anti-Money Laundering and Counter Terrorist Financing (AML/CFT) Framework	62
5.1 Purpose	62
5.2 AML/CFT Objectives	62
5.3 Governance and Oversight	63
5.4 Risk-Based Approach	64
5.5 Financial Crime Risk Assessment	65
5.6 Customer Due Diligence	67
5.7 Enhanced Due Diligence	68
5.8 Transaction Monitoring	68
5.9 Sanctions and PEP Screening	70
5.10 Suspicious Activity Reporting	70
5.11 Record Keeping	73
5.12 Training and Awareness	73
5.13 Independent Review and Continuous Improvement	74
6. Customer Due Diligence (CDD) and Know Your Customer (KYC)	77
6.1 Purpose	77
6.2 Objectives	77
6.3 Customer Identification Requirements	78
6.4 Identity Verification	79
6.5 Address Verification	80
6.6 Age Verification	80
6.7 Customer Risk Assessment	81
6.8 Trigger Events for Verification	82
6.9 Enhanced Due Diligence	83
6.10 Ongoing Monitoring	83

6.11 Account Restrictions and Failed Verification.....	84
6.12 Record Keeping.....	85
6.13 Responsibilities	85
6.14 Key Controls.....	87
6.15 Review and Continuous Improvement.....	88
7. Responsible Gaming	90
7.1 Purpose	90
7.2 Responsible Gaming Objectives.....	90
7.3 Governance and Responsibilities	91
7.4 Protection of Vulnerable Persons	92
7.5 Responsible Gaming Information.....	93
7.6 Age Verification and Underage Gambling Prevention	93
7.7 Behavioural Monitoring.....	94
7.8 Responsible Gaming Interventions	95
7.9 Cooling-Off Periods.....	96
7.10 Self-Exclusion	96
7.11 Operator-Initiated Restrictions.....	98
7.12 Deposit Limits and Player Controls	98
7.13 Reality Checks and Self-Assessment Tools.....	99
7.14 Training and Awareness.....	100
7.15 Record Keeping.....	100
7.16 Key Controls.....	101
7.17 Review and Continuous Improvement.....	103
8. customer complaints and dispute resolution	105
8.1 Purpose	105
8.2 Complaint Management Principles	105
8.3 First Line Resolution.....	106
8.4 Formal Complaint Submission	107
8.5 Complaint Registration.....	107
8.6 Complaint Acknowledgement.....	108
8.7 Investigation Process.....	108
8.8 Complaint Resolution	109
8.9 Responsible Gaming Complaints	110
8.10 Complaint Categories.....	110
8.11 Alternative Dispute Resolution (ADR)	111
8.12 Regulatory Escalation	112

8.13 Complaints Register.....	112
8.14 Record Keeping.....	113
8.15 Reporting.....	113
8.16 Key Controls.....	114
8.17 Review and Continuous Improvement.....	116
9. Payment operations and financial controls	118
9.1 Purpose	118
9.2 Department Structure and Responsibilities	118
9.3 Operational Systems and Monitoring Infrastructure	119
9.4 Deposit Processing.....	121
9.5 Withdrawal Processing.....	123
9.6 Fraud Prevention and Transaction Monitoring.....	124
9.7 AML and Financial Crime Escalation	125
9.8 Chargebacks and Disputes.....	126
9.9 PSP Reconciliation.....	126
9.10 Operational Reporting and Analytics.....	127
9.11 Key Performance Indicators (KPIs).....	128
9.12 Record Keeping.....	129
9.13 Key Controls.....	129
9.14 Review and Continuous Improvement.....	132
10. Information Security and Data Protection.....	134
10.1 Purpose	134
10.2 Information Security Objectives	134
10.3 Governance and Responsibilities.....	135
10.4 Information Security Principles.....	136
10.5 Data Protection and Privacy	137
10.6 Data Classification	138
10.7 Access Control	139
10.8 Personal Data Protection.....	140
10.9 Data Subject Rights	141
10.10 Data Retention and Disposal.....	142
10.11 Encryption and Secure Data Storage.....	142
10.12 Third-Party and Vendor Security.....	143
10.13 Security Awareness and Training.....	144
10.14 Information Security Incident Management.....	144
10.15 Compliance Monitoring and Audit	145

10.16 Key Controls	146
10.17 Continuous Improvement	148
11. IT Operations, Incident Management and Business Continuity	150
11.1 Purpose	150
11.2 Objectives	150
11.3 Governance and Responsibilities.....	151
11.4 IT Operations Management.....	152
11.5 Incident Management Framework.....	152
11.6 Incident Reporting	153
11.7 Incident Classification.....	154
11.8 Incident Response Procedures	156
11.9 Regulatory and Customer Communications	156
11.10 Business Continuity Planning.....	157
11.11 Continuity and Recovery Measures	158
11.12 Post-Incident Reviews	159
11.13 Record Keeping.....	159
11.14 Key Controls	159
11.15 Continuous Improvement	162
Chapter 12 – Customer Support and Technical Support Operations	164
12.1 Purpose	164
12.2 Support Function Structure	164
Customer Support Team.....	164
Technical Support Team.....	166
12.3 Customer Support Operations	169
12.4 Customer Communication Channels.....	169
12.5 Service Standards	170
12.6 Customer Support Workflow	171
12.7 Escalation Framework.....	174
12.8 Complaint Handling	175
Complaint Handling Process.....	176
12.9 Responsible Gaming And Compliance Escalations	179
12.10 Operational Systems and Tools	181
12.11 Technical Support Operations.....	184
12.12 Technical Incident Management	184
12.13 Knowledge Management	185
12.14 Performance Monitoring and KPIs.....	185

12.15 Record Keeping.....	186
12.16 Key Controls	186
12.17 Continuous Improvement	188
13. Document Control And Version Management	191
13.1 Purpose	191
13.2 Scope	191
13.3 Document Ownership	192
13.4 Version Control.....	192
13.5 Review and Approval Process.....	193
13.6 Distribution and Accessibility	193
13.7 Change Management	194
13.8 Record Retention	194
13.9 Key Controls.....	194
13.10 Continuous Improvement	196
Document Version Control	196
CONCLUSION	197

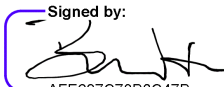
EXECUTIVE INTRODUCTION

Mirage Corporation N.V. is a business-to-consumer (B2C) online gaming operator committed to delivering secure, innovative, and responsible digital entertainment through regulated gaming services. Operating within a highly regulated environment, the Company places strong emphasis on regulatory compliance, operational resilience, responsible gaming, and customer protection across all areas of its business.

This Operational Manual establishes the governance framework, operational principles, and internal controls that support the Company's day-to-day activities. It provides employees, management, and stakeholders with a structured overview of organisational responsibilities, operational processes, compliance obligations, and control mechanisms designed to promote consistency, transparency, and accountability.

The manual supports the Company's commitment to effective corporate governance by documenting key operational processes across customer operations, technology, payments, compliance, finance, information security, business continuity, and support services. It also promotes a culture of continuous improvement through clearly defined responsibilities, documented procedures, performance monitoring, and risk management practices.

As Mirage Corporation N.V. continues to expand its operations across regulated jurisdictions, this manual serves as a living governance document intended to evolve alongside regulatory developments, technological innovation, and organisational growth while maintaining the highest standards of integrity, security, and operational excellence.

Signed by:


AFE637C78B0C47B

Approved by: Borut Lozej

CEO Mirage Corporation



INTRODUCTION



1

1. INTRODUCTION

1.1 PURPOSE OF THE MANUAL

This Operational Manual has been developed to establish the governance framework, operational procedures, internal controls, and compliance standards applicable to Mirage Corporation N.V. The document serves as a reference guide for directors, officers, employees, contractors, and service providers involved in the operation and management of the Company's licensed gaming activities.

The purpose of this Manual is to ensure that Mirage Corporation N.V. conducts its business in a consistent, transparent, secure, and compliant manner while maintaining the highest standards of integrity, responsible gaming, customer protection, and regulatory compliance. The Manual outlines the key operational processes, responsibilities, reporting lines, and internal controls that support the Company's day-to-day activities and long-term strategic objectives.

This document should be read in conjunction with the Company's policies, including but not limited to its Anti-Money Laundering and Counter Terrorist Financing (AML/CFT) Framework, Responsible Gaming Policy, Data Protection Policy, Information Security Policy, and any other procedures adopted by the Company from time to time.

1.2 COMPANY OVERVIEW

Mirage Corporation N.V. is a company incorporated in Curaçao and licensed by the Curaçao Gaming Authority (CGA) under licence number OGL/2024/1304/0813. Since its establishment, the Company has operated within the online gaming sector, providing gaming and entertainment services to customers through a portfolio of online gaming brands and websites.

The Company operates a business model focused on the provision of online gaming products and services, offering customers access to a

diverse portfolio of casino games and gaming content sourced through established commercial relationships with recognised gaming content providers and aggregation platforms. Through these partnerships, Mirage Corporation N.V. is able to offer a broad range of gaming products while maintaining operational efficiency, platform stability, and regulatory compliance.

Mirage Corporation N.V. conducts its operations through a network of approved service providers and strategic business partners supporting various operational functions including payment processing, customer support, technology development, hosting infrastructure, compliance services, finance, accounting, and corporate administration. The Company remains ultimately responsible for the oversight of all outsourced and third-party activities and maintains appropriate controls to ensure that all service providers operate in accordance with applicable legal, regulatory, and contractual requirements.

1.3 BUSINESS OBJECTIVES

The Company's primary objective is to operate a sustainable, compliant, and commercially successful online gaming business while ensuring the protection of its customers, the integrity of its gaming operations, and adherence to all applicable regulatory obligations.

To achieve these objectives, Mirage Corporation N.V. is committed to:

- Maintaining a safe, fair, and transparent gaming environment for all customers.
- Promoting responsible gaming and customer protection measures.
- Preventing money laundering, terrorist financing, fraud, and other financial crimes.
- Ensuring compliance with all applicable regulatory and licensing requirements.
- Maintaining effective governance, risk management, and internal control frameworks.

- Delivering high standards of customer service and operational excellence.
- Supporting continuous improvement, innovation, and technological advancement.
- Expanding and developing its market presence in a controlled and responsible manner.

1.4 MISSION, VISION AND CORE VALUES

Mission

To provide a secure, entertaining, and responsible online gaming experience by combining innovative technology, regulatory excellence, and exceptional customer service while creating sustainable value for players, business partners, employees, and stakeholders.

Vision

To be recognised as a trusted and innovative online gaming operator, delivering outstanding customer experiences through operational excellence, responsible gaming, technological innovation, and regulatory leadership across all markets in which the Company operates.

Core Values

Integrity

We conduct our business honestly, ethically, and transparently while complying with all applicable legal and regulatory requirements.

Customer Focus

We place players at the centre of our decision-making by delivering secure, fair, and enjoyable gaming experiences supported by responsive customer service.

Responsible Gaming

We actively promote player protection by supporting responsible gaming initiatives, early intervention measures, and regulatory best practices.

Innovation

We continuously improve our technology, products, and operational processes to deliver high-quality gaming experiences.

Collaboration

We encourage teamwork, knowledge sharing, accountability, and open communication across all departments.

Excellence

We strive for operational excellence through continuous improvement, effective governance, and professional standards.

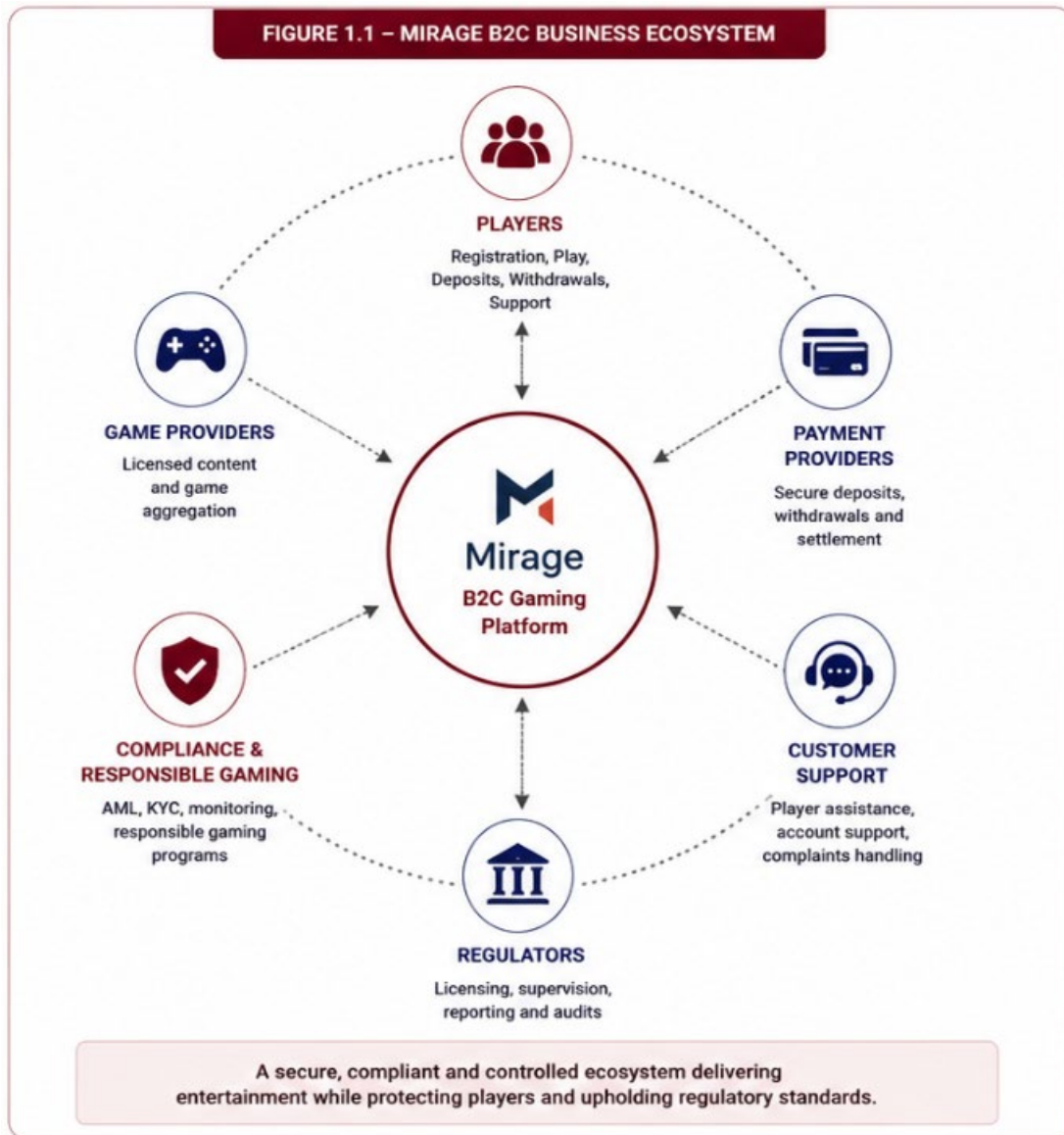
1.5 BUSINESS MODEL OVERVIEW

Mirage Corporation N.V. operates as a licensed business-to-consumer online gaming operator, delivering gaming products and services directly to registered players through its digital gaming platform. The Company collaborates with licensed game providers, payment service providers, technology partners, and regulatory authorities to ensure the secure, compliant, and efficient delivery of gaming services.

The Company's operating model integrates multiple business functions, including customer operations, responsible gaming, compliance, payments, finance, technology, and customer support, ensuring that all player activities are managed within a controlled governance framework.

Operational activities are supported by secure technology platforms, continuous monitoring, risk management processes, and internal

controls designed to safeguard customer interests while maintaining regulatory compliance and business continuity.



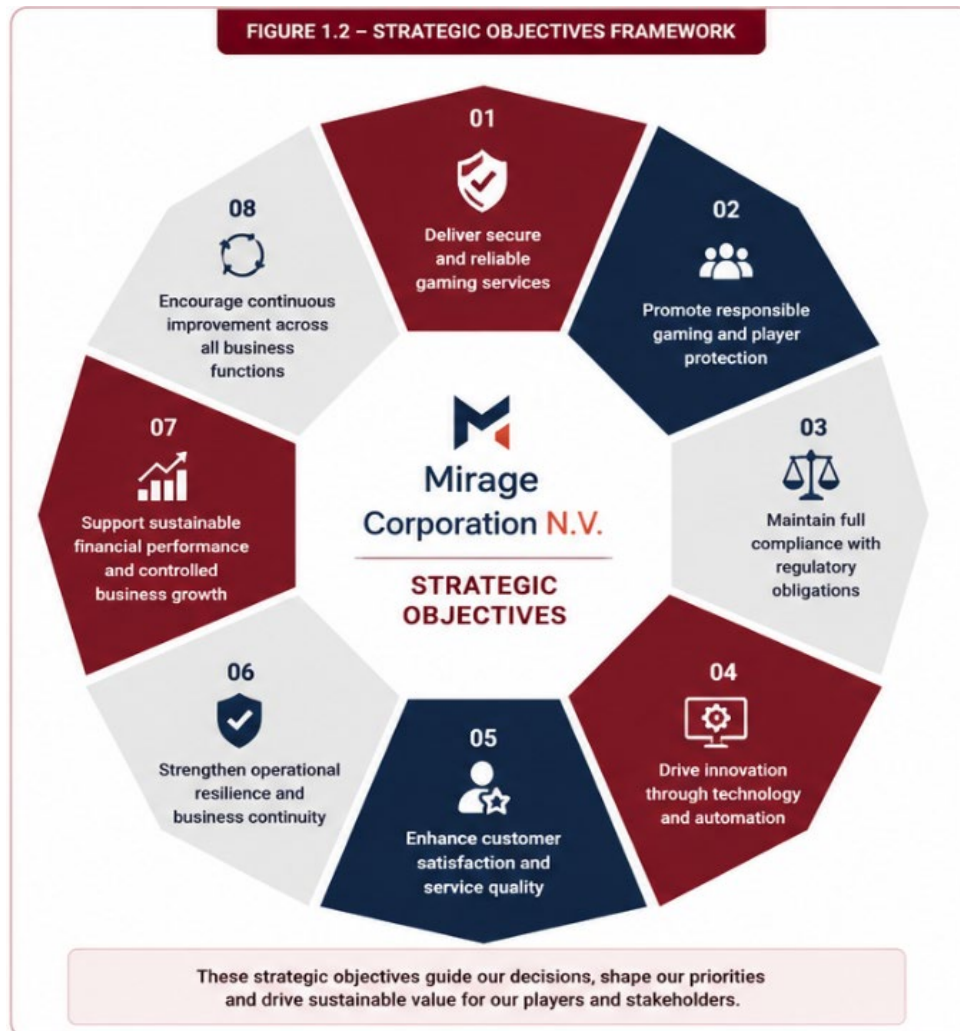
Strategic Objectives

Mirage Corporation N.V. pursues its strategic objectives through a balanced approach focused on sustainable growth, operational excellence, customer protection, and regulatory compliance.

The Company's primary strategic objectives include:

- Delivering secure and reliable gaming services.

- Promoting responsible gaming and player protection.
- Maintaining full compliance with regulatory obligations.
- Driving innovation through technology and automation.
- Enhancing customer satisfaction and service quality.
- Strengthening operational resilience and business continuity.
- Supporting sustainable financial performance and controlled business growth.
- Encouraging continuous improvement across all business functions.



1.6 GOVERNANCE PRINCIPLES

The Company's governance framework is founded on principles designed to support effective decision-making, accountability, transparency, and long-term sustainability.

These principles include:

- Clear allocation of responsibilities and authority.
- Effective risk management and internal control.
- Regulatory compliance and ethical business conduct.
- Protection of customer interests and personal data.
- Continuous monitoring and performance improvement.
- Collaboration across business functions.
- Accurate documentation and record retention.
- Independent oversight and periodic review of governance processes.

These principles apply across all departments and operational activities and provide the foundation for the governance framework described throughout this manual.



CORPORATE GOVERNANCE & ORGANISATIONAL STRUCTURE AND INTERNAL CONTROL



2

CORPORATE GOVERNANCE AND ORGANISATIONAL STRUCTURE

2.1 PURPOSE

Mirage Corporation N.V. maintains a corporate governance framework designed to promote effective leadership, accountability, transparency, regulatory compliance, and sound decision-making throughout the organisation.

The governance framework establishes the organisational structure, allocation of responsibilities, reporting lines, and internal control mechanisms that support the Company's strategic objectives while ensuring that operational activities are conducted in accordance with applicable legal, regulatory, and internal requirements.

Corporate governance provides the foundation for responsible business conduct by defining clear ownership of responsibilities, promoting ethical decision-making, supporting effective risk management, and ensuring appropriate oversight across all business functions.

This framework is intended to support sustainable growth, operational resilience, customer protection, and continuous improvement while maintaining confidence among regulators, customers, business partners, and other stakeholders.

2.1 OWNERSHIP STRUCTURE

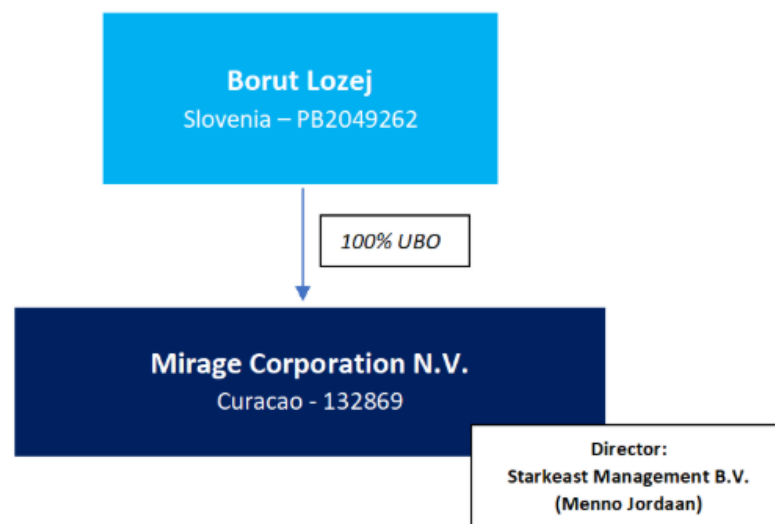
Mirage Corporation N.V. operates as a licensed Business-to-Consumer (B2C) online gaming operator under the supervision of the Curaçao Gaming Authority.

The Company's Ultimate Beneficial Owner ("UBO") provides strategic direction through the Board of Directors and Senior Management. Day-to-day operational responsibilities are delegated to appropriately qualified management personnel responsible for overseeing key

operational functions, including Compliance, Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT), Responsible Gaming, Payment Operations, Information Technology, Customer Support, and Information Security.

The ownership and governance structure is designed to promote transparency, effective decision-making, regulatory compliance, and operational resilience. Clear reporting lines and delegated authorities ensure that strategic objectives are implemented effectively while maintaining appropriate oversight of the Company's licensed activities.

Where required by applicable laws and regulatory requirements, details relating to the Company's ownership structure, Ultimate Beneficial Owners, Directors, and Key Persons shall be maintained and made available to the Curaçao Gaming Authority and other competent authorities upon request.



2.2 GOVERNANCE FRAMEWORK

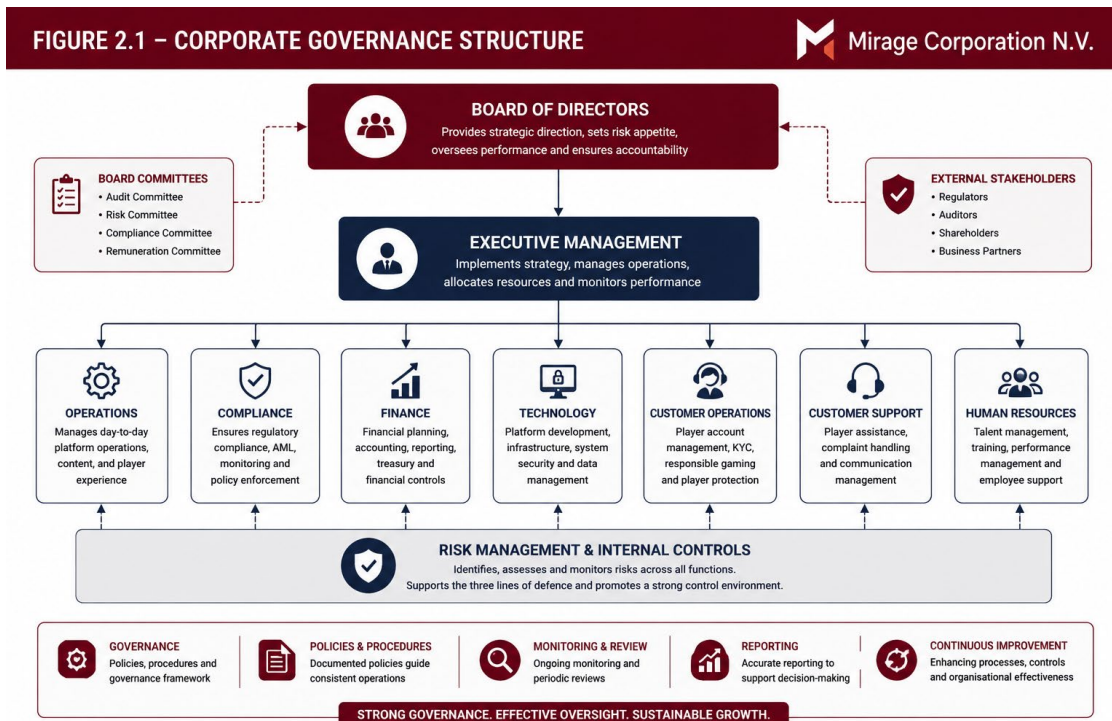
The governance framework operates through clearly defined organisational responsibilities, management oversight, documented policies and procedures, internal controls, performance monitoring, and periodic review.

Governance activities are integrated into the Company's day-to-day operations and apply across all departments, including executive management, operations, compliance, finance, customer support, technology, information security, and human resources.

The framework promotes collaboration between business functions while ensuring that appropriate segregation of duties, accountability, and independent oversight are maintained where required.

Governance activities include:

- Strategic planning and business oversight.
- Risk identification and management.
- Regulatory compliance monitoring.
- Operational performance management.
- Financial oversight.
- Information security governance.
- Responsible Gaming oversight.
- Customer protection.
- Business continuity planning.
- Continuous improvement initiatives.



2.3 GOVERNANCE RESPONSIBILITIES

Corporate governance is supported by clearly defined responsibilities throughout the organisation.

Board of Directors

The Board of Directors provides strategic direction, approves the Company's governance framework, oversees business performance, establishes risk appetite, and ensures appropriate corporate oversight.

Executive Management

Executive Management is responsible for implementing corporate strategy, allocating resources, monitoring operational performance, and ensuring that business objectives are achieved in accordance with approved governance principles.

Department Management

Department managers are responsible for implementing Company policies, supervising operational activities, managing departmental risks, maintaining internal controls, and reporting significant issues to senior management.

Employees

All employees are responsible for complying with Company policies and procedures, performing assigned responsibilities with integrity, safeguarding Company assets and information, and reporting concerns or incidents through the appropriate channels.

2.4 Three Lines of Defence

Mirage Corporation N.V. applies the principles of the Three Lines of Defence model to support effective governance and risk management.

First Line – Operational Management

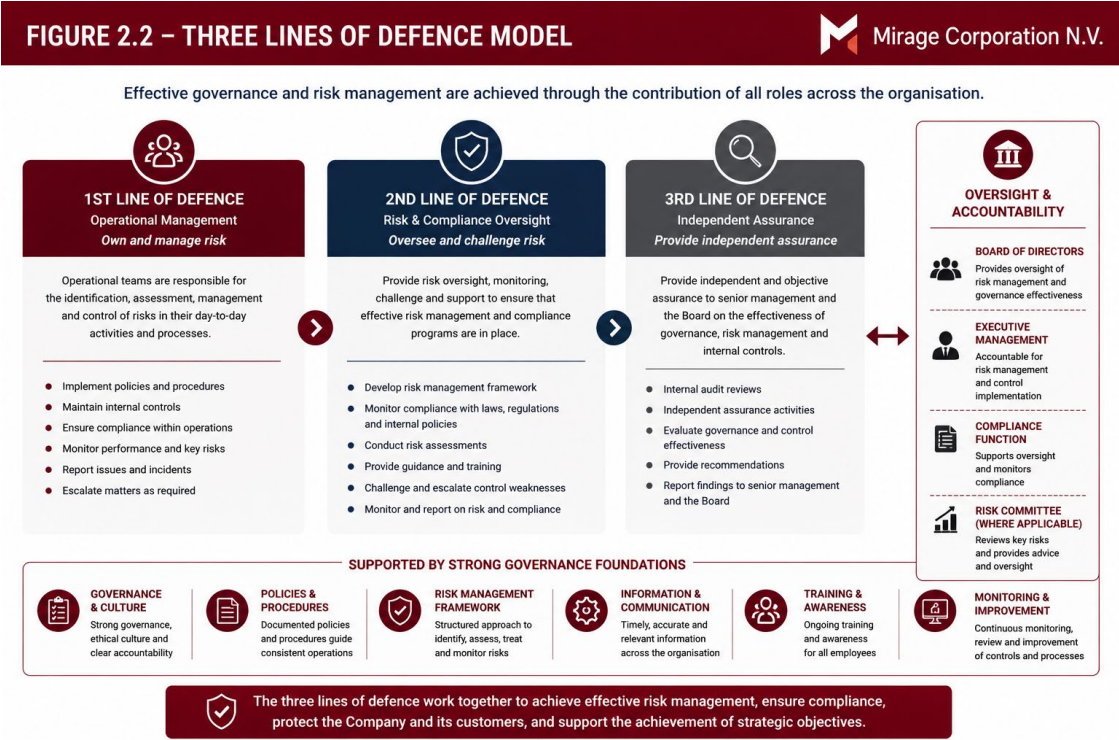
Operational departments own and manage risks arising from their daily activities. They are responsible for implementing internal controls, complying with Company procedures, and managing operational performance.

Second Line – Compliance and Risk Oversight

The Compliance function provides independent oversight of regulatory obligations, monitors adherence to Company policies, advises management on regulatory developments, and supports the implementation of effective risk management practices.

Third Line – Independent Assurance

Independent assurance may be provided through internal reviews, external audits, regulatory inspections, or other independent assessment activities to evaluate the effectiveness of governance arrangements, internal controls, and compliance processes.



2.5 DECISION-MAKING AND DELEGATION OF AUTHORITY

Decision-making within the Company is conducted through clearly defined governance arrangements that ensure decisions are taken at the appropriate organisational level.

Strategic decisions relating to business direction, major investments, regulatory matters, and corporate governance are reserved for senior management or the Board of Directors where applicable.

Operational decisions relating to day-to-day business activities are delegated to departmental management within approved authority limits.

Escalation procedures ensure that significant operational, regulatory, financial, or reputational issues are promptly referred to the appropriate level of management for review and decision.

2.6 GOVERNANCE REPORTING

Effective governance relies upon accurate, timely, and transparent reporting throughout the organisation.

Management information is generated from operational systems and departmental reporting processes to support oversight, performance monitoring, risk management, and informed decision-making.

Governance reporting may include:

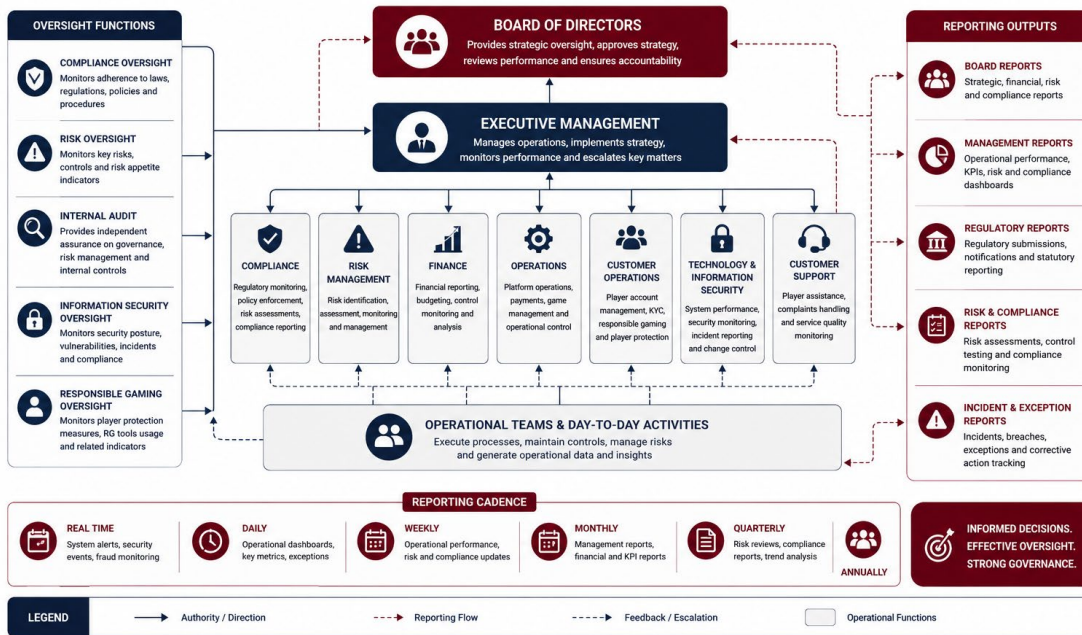
- Operational performance reports.
- Compliance monitoring reports.
- Responsible Gaming reports.
- Customer complaints analysis.
- Financial reporting.
- Risk assessments.
- Information security reporting.
- Incident and business continuity reporting.
- Internal audit findings.
- Regulatory reporting.

Reporting frequencies are determined according to operational requirements, regulatory obligations, and management information needs.

FIGURE 2.3 – GOVERNANCE REPORTING AND OVERSIGHT FRAMEWORK



Timely, accurate and relevant information flows throughout the organisation to support effective oversight, informed decision-making and accountability.



2.7 INTERNAL CONTROL ENVIRONMENT

The Company maintains an internal control environment designed to safeguard assets, ensure reliable reporting, protect customer information, support regulatory compliance, and reduce operational risk.

Internal controls include preventive, detective, and corrective measures integrated into business processes.

Examples of internal controls include:

- Segregation of duties.
- Role-based system access.
- Approval workflows.
- Dual authorisation processes.
- Reconciliations.

- Monitoring activities.
- Exception reporting.
- Incident management.
- Change management controls.
- Policy and procedure reviews.

The effectiveness of internal controls is monitored through management oversight, periodic reviews, compliance monitoring, and continuous improvement activities.

2.8 GOVERNANCE PRINCIPLES

The Company's governance framework is guided by the following principles:

- Accountability through clearly defined responsibilities.
- Integrity and ethical business conduct.
- Transparency in decision-making and reporting.
- Regulatory compliance across all business activities.
- Effective risk management and internal control.
- Protection of customer interests and confidential information.
- Collaboration between departments.
- Continuous monitoring and performance improvement.
- Documentation and record retention.
- Commitment to operational resilience and sustainable growth.

These principles apply across all organisational levels and provide the foundation for the governance framework described throughout this Operational Manual.



RISK **MANAGEMENT** **FRAMEWORK**

3



3. RISK MANAGEMENT FRAMEWORK

3.1 PURPOSE

Mirage Corporation N.V. recognises that effective risk management is fundamental to maintaining the integrity, sustainability, and regulatory compliance of its operations. As a licensed online gaming operator, the Company is exposed to a variety of strategic, operational, regulatory, financial, technological, and reputational risks that must be appropriately identified, assessed, monitored, and managed.

As a licensed online gaming operator, the Company is exposed to a range of risks arising from its products, services, technology systems, customer activity, payment operations, regulatory obligations, third-party providers, and market environment. These risks must be identified, assessed, controlled, monitored, and reported in a structured and consistent manner.

The purpose of this Risk Management Framework is to establish a structured approach to risk management throughout the organisation and to ensure that potential risks are proactively managed in a manner that supports the Company's strategic objectives, protects its customers, and safeguards its licence and reputation.

Risk management is embedded across all operational functions and forms part of the Company's wider governance, compliance, AML/CFT, responsible gaming, information security, payment, and business continuity arrangements.

3.2 RISK MANAGEMENT OBJECTIVES

The Company's risk management objectives are to:

- Identify and assess risks that may affect the Company's operations, customers, licence, reputation, financial position, or technology environment.

- Support compliance with applicable laws, regulations, licence conditions, and internal policies.
- Prevent and mitigate money laundering, terrorist financing, fraud, underage gambling, irresponsible gambling, and other forms of harm or misconduct.
- Protect customers, business assets, information systems, and personal data.
- Promote responsible, risk-based decision-making across all departments.
- Support operational resilience and business continuity.
- Ensure that significant risks are escalated to appropriate management levels.
- Maintain accurate records of risk assessments, mitigation measures, and management decisions.
- Promote a culture of accountability, transparency, and continuous improvement.

The risk management framework is designed to be proportionate to the nature, scale, complexity, and risk profile of the Company's activities.

3.3 RISK MANAGEMENT PRINCIPLES

The Company's approach to risk management is guided by the following principles:

Risk-Based Decision-Making

Business decisions should take into account the level of risk involved, the effectiveness of existing controls, regulatory expectations, and the potential impact on customers, operations, and the Company's licence.

Accountability

Risk ownership is assigned to the relevant business function or process owner. Department heads are responsible for identifying, managing, and escalating risks within their areas of responsibility.

Proportionality

Controls and monitoring activities are applied according to the level of risk identified. Higher-risk activities are subject to enhanced oversight, additional controls, and more frequent review.

Customer Protection

Risks that may affect customers, including responsible gaming concerns, underage gambling, fraud, data protection issues, payment disputes, or unfair treatment, are prioritised and escalated appropriately.

Regulatory Compliance

Risk management activities are aligned with the Company's legal, regulatory, licensing, AML/CFT, responsible gaming, and reporting obligations.

Continuous Monitoring

Risks are monitored on an ongoing basis through operational reviews, compliance monitoring, transaction monitoring, incident reporting, complaints analysis, customer activity reviews, and management reporting.

Continuous Improvement

Lessons learned from incidents, audits, complaints, regulatory developments, customer feedback, internal reviews, and operational performance are used to strengthen controls and improve the risk management framework.

3.3 RISK GOVERNANCE

Risk management is the responsibility of all employees, management, and key function holders within Mirage Corporation N.V.

Board of Directors

The Board of Directors has ultimate responsibility for the oversight of the Company's risk management framework and shall ensure that appropriate systems and controls are implemented and maintained.

The Board shall:

- Review significant risks affecting the business.
- Monitor the effectiveness of risk mitigation measures.
- Review material incidents and emerging risks.
- Ensure sufficient resources are allocated to risk management activities.
- Receive periodic risk reports from senior management and key function holders.

Senior Management

Senior Management is responsible for implementing the risk management framework and ensuring that identified risks are appropriately managed within their respective areas of responsibility.

Senior Management shall:

- Promote a risk-aware culture.
- Ensure that risk controls are implemented and maintained.
- Escalate material risks to the Board where appropriate.
- Monitor operational risks and emerging threats.

Compliance Function

The Compliance Function supports the risk management process by identifying regulatory risks, monitoring compliance obligations, conducting reviews, and advising management on risk mitigation measures.

Money Laundering Reporting Officer (MLRO)

The MLRO is responsible for overseeing financial crime risk management, including money laundering, terrorist financing, sanctions exposure, fraud risks, and suspicious activity monitoring.

3.4 RISK GOVERNANCE

Risk management is a shared responsibility across the Company. While the Board of Directors and Senior Management provide overall oversight, all departments are responsible for identifying and managing risks arising from their activities.

Board of Directors

The Board of Directors has ultimate responsibility for oversight of the Company's risk management framework.

The Board is responsible for:

- Reviewing significant risks affecting the Company.
- Ensuring that appropriate systems and controls are maintained.
- Monitoring material incidents and emerging risks.
- Receiving periodic updates from Senior Management and key function holders.
- Ensuring that sufficient resources are available to manage key risks.
- Supporting a culture of responsible and compliant business conduct.

Senior Management

Senior Management is responsible for implementing the risk management framework and ensuring that risk controls operate effectively across the business.

Senior Management is responsible for:

- Promoting a risk-aware culture.
- Ensuring that departmental risks are identified and managed.
- Reviewing significant operational, compliance, financial, technology, and customer-related risks.
- Escalating material risks to the Board where appropriate.
- Supporting remediation and improvement actions.
- Ensuring that risk management is incorporated into business planning and operational decision-making.

Compliance Function

The Compliance Function supports the risk management framework by identifying regulatory risks, monitoring compliance obligations, conducting reviews, advising management, and supporting remediation activities.

The Compliance Function is responsible for:

- Monitoring regulatory developments.
- Supporting compliance risk assessments.
- Reviewing policies and procedures.
- Monitoring implementation of compliance controls.
- Supporting regulatory reporting and inspections.
- Reporting significant compliance risks to Senior Management.

Money Laundering Reporting Officer

The MLRO is responsible for oversight of money laundering, terrorist financing, sanctions, fraud, and financial crime risks.

The MLRO is responsible for:

- Monitoring financial crime risks.
- Reviewing suspicious activity and transaction monitoring alerts.
- Supporting customer risk assessments.
- Overseeing AML/CFT controls.
- Escalating material financial crime risks to Senior Management and the Board.
- Maintaining records of AML-related investigations and decisions.

Responsible Gaming Officer

The Responsible Gaming Officer is responsible for overseeing risks relating to player protection, gambling-related harm, self-exclusion, cooling-off, responsible gaming interventions, and vulnerable customers.

Department Heads

Department Heads are responsible for identifying and managing risks within their business areas.

Responsibilities include:

- Maintaining effective departmental controls.
- Ensuring employees follow internal procedures.
- Escalating risks, incidents, and control failures.
- Supporting audits, reviews, and investigations.
- Implementing corrective actions where weaknesses are identified.

Employees and Contractors

All employees and contractors are responsible for performing their duties in accordance with Company policies and procedures and for reporting any actual or suspected risks, incidents, breaches, or control failures through the appropriate channels.

3.5 RISK TOLERANCE

Mirage Corporation N.V. seeks to minimise risks that may adversely affect regulatory compliance, customer protection, financial integrity, operational continuity, information security, or the Company's reputation.

The Company maintains a low tolerance for:

- Regulatory breaches.
- Money laundering, terrorist financing, sanctions breaches, fraud, or other financial crime risks.
- Underage gambling.
- Failure to protect vulnerable customers.
- Unauthorised access to systems or customer data.
- Material information security incidents.
- Failure to meet legal or regulatory reporting obligations.
- Misleading customer communications or unfair customer treatment.
- Significant failures in payment processing, withdrawals, or customer account controls.

The Company recognises that certain operational risks are inherent in online gaming operations. Such risks may be accepted only where

appropriate controls, monitoring arrangements, escalation procedures, and management oversight are in place.

Where risks exceed acceptable levels, the Company shall take appropriate action, which may include additional controls, enhanced monitoring, management escalation, process changes, customer restrictions, suspension of activities, or termination of business relationships.

3.6 RISK-BASED APPROACH

The Company applies a risk-based approach to business operations and compliance management.

This means that the level of control, review, and monitoring applied to a particular activity is proportionate to the level of risk identified.

Risk factors considered may include:

- Customer profile and behaviour.
- Transaction value, frequency, and pattern.
- Payment method used.
- Jurisdictional exposure.
- Responsible Gaming indicators.
- AML/CFT risk indicators.
- Technology dependencies.
- Third-party service provider reliance.
- Regulatory requirements.
- Previous incidents, complaints, or control weaknesses.
- Potential impact on customers, operations, or the Company's licence.

Higher-risk matters are subject to enhanced review, additional documentation, greater management oversight, and more frequent monitoring.

3.7 RISK ASSESSMENT PROCESS

The Company applies a structured risk assessment process to identify, evaluate, manage, and monitor risks across its operations.



Risk Identification

Risks may be identified through:

- Day-to-day business operations.
- Customer activity monitoring.
- Transaction monitoring.
- Compliance reviews.
- AML/CFT reviews.
- Responsible Gaming reviews.
- Customer complaints.
- Internal audits.
- Incident reports.
- Payment investigations.
- Staff feedback.
- Regulatory developments.
- Third-party provider assessments.
- Technology monitoring.
- Market and industry developments.

Risk Assessment

Identified risks are assessed according to:

- Likelihood of occurrence.
- Potential impact.
- Existing controls.
- Control effectiveness.
- Residual risk exposure.
- Regulatory implications.
- Customer impact.
- Operational consequences.
- Financial or reputational exposure.

Risk assessments may be qualitative or quantitative depending on the nature of the risk and the available information.

Risk Evaluation

Following assessment, risks are evaluated to determine whether existing controls are sufficient or whether additional mitigation is required.

Risks may be categorised as low, medium, high, or critical depending on their likelihood and impact.

Risk Mitigation

Mitigation measures may include:

- Policies and procedures.
- Customer due diligence.
- Enhanced due diligence.
- Transaction monitoring.
- Responsible Gaming interventions.
- Access controls.
- Segregation of duties.
- Training and awareness.
- Technical controls.
- Vendor management controls.
- Approval workflows.
- Incident response measures.
- Business continuity arrangements.
- Management reporting.

Risk Monitoring

The effectiveness of risk controls is monitored through:

- Compliance monitoring.
- AML/CFT monitoring.
- Responsible Gaming monitoring.
- Operational reviews.
- Management reporting.

- Internal audits.
- Payment monitoring.
- Customer support trends.
- Incident analysis.
- Complaint reviews.
- Key performance indicators and key risk indicators.

Risk Reporting

Material risks, incidents, control failures, or emerging issues shall be reported to the appropriate level of management without undue delay.

Where required, risks may be escalated to Senior Management, the Board of Directors, the MLRO, the Responsible Gaming Officer, the Data Protection Officer, or other relevant function holders.

Review and Improvement

Risk assessments and mitigation measures are reviewed periodically to ensure that they remain effective and aligned with business activities, regulatory expectations, and operational developments.

3.8 KEY RISK CATEGORIES

The Company monitors a range of risk categories relevant to its licensed online gaming activities.

Regulatory and Compliance Risk

Regulatory and compliance risk arises from failure to comply with applicable laws, regulations, licence conditions, regulatory expectations, or internal policies.

Potential consequences include regulatory sanctions, penalties, licence restrictions, enforcement action, operational limitations, and reputational damage.

Mitigation measures include compliance monitoring, regulatory horizon scanning, policy management, training, internal reviews, and management oversight.

Money Laundering and Financial Crime Risk

Financial crime risk includes exposure to money laundering, terrorist financing, sanctions breaches, fraud, identity theft, payment abuse, bonus abuse, and other suspicious or criminal activity.

Mitigation measures include customer due diligence, enhanced due diligence, transaction monitoring, sanctions and PEP screening, suspicious activity reporting, payment monitoring, and AML/CFT training.

Responsible Gaming and Customer Protection Risk

Responsible Gaming risk arises where customers may be exposed to gambling-related harm or where the Company fails to identify or respond appropriately to indicators of vulnerability.

Mitigation measures include age verification, behavioural monitoring, deposit limits, cooling-off periods, self-exclusion, customer interventions, staff training, and escalation to the Responsible Gaming Officer.

Operational Risk

Operational risk arises from failures in people, processes, systems, internal controls, or external service providers.

Examples include process failures, human error, poor documentation, customer support disruption, payment processing errors, failed escalations, or inadequate oversight.

Mitigation measures include documented procedures, training, supervision, quality assurance, incident management, reconciliations, and continuous improvement.

Technology and Information Security Risk

Technology and information security risks include cyber threats, data breaches, system outages, unauthorised access, infrastructure failures, loss of data, and technology provider disruption.

Mitigation measures include access controls, monitoring, encryption, vulnerability management, backup procedures, disaster recovery planning, incident response, and information security training.

Payment and Financial Transaction Risk

Payment risk includes failed deposits, delayed withdrawals, payment fraud, chargebacks, PSP disruption, reconciliation discrepancies, incorrect balances, or misuse of payment methods.

Mitigation measures include PSP monitoring, transaction monitoring, reconciliation, withdrawal controls, fraud checks, AML escalation, and payment performance reporting.

Reputational Risk

Reputational risk may arise from customer complaints, regulatory action, poor customer experience, payment delays, responsible gaming failures, data breaches, negative publicity, or third-party failures.

Mitigation measures include effective complaint handling, transparent customer communications, responsible gaming controls, regulatory compliance, and strong operational oversight.

Third-Party Risk

The Company relies on third-party providers for services such as payments, gaming content, platform technology, identity verification, hosting, compliance systems, and operational support.

Third-party risk may arise from service disruption, weak controls, regulatory non-compliance, data protection failures, security weaknesses, or poor performance.

Mitigation measures include due diligence, contractual controls, service monitoring, security reviews, performance reporting, and ongoing oversight.

3.9 FINANCIAL CRIME RISK ASSESSMENT

The Company conducts financial crime risk assessments in accordance with its AML/CFT framework.

Financial crime risk assessments consider:

- Customer risk.
- Geographic risk.
- Product and service risk.
- Transaction risk.
- Payment method risk.
- Delivery channel risk.
- Sanctions exposure.
- Fraud indicators.
- Previous suspicious activity.
- Use of high-risk jurisdictions or payment instruments.

The MLRO is responsible for overseeing financial crime risk assessments and ensuring that higher-risk customers, transactions, and activities are subject to appropriate controls and monitoring.

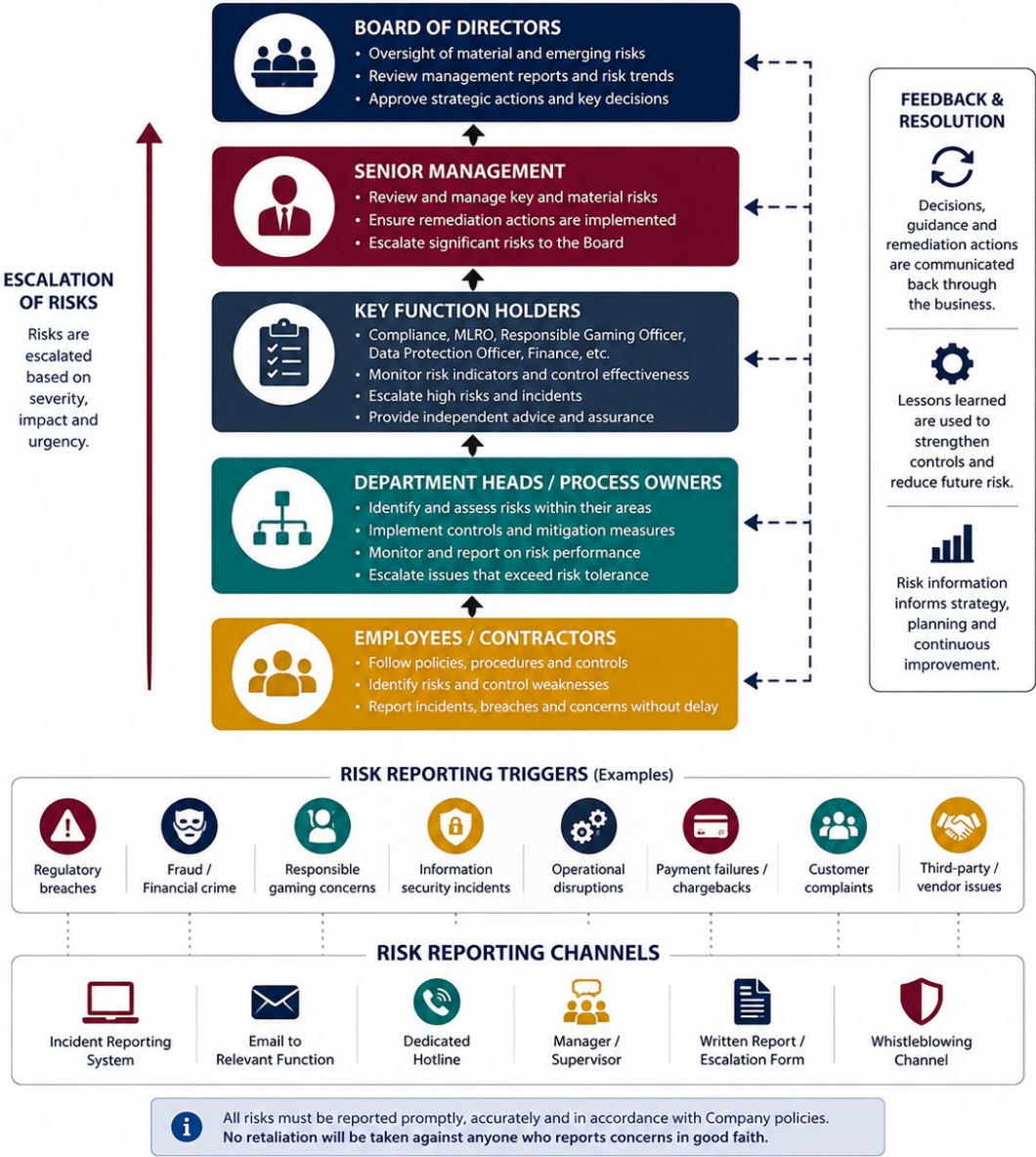
Financial crime risks identified through transaction monitoring, customer reviews, payment investigations, or internal reports shall be assessed and escalated in accordance with the Company's AML/CFT procedures.

3.10 RISK MONITORING AND REPORTING

Risk monitoring is conducted across the Company through operational systems, compliance reviews, transaction monitoring, responsible gaming monitoring, customer support reporting, payment reporting, technology monitoring, and management oversight.

FIGURE 3.2
RISK REPORTING AND ESCALATION FRAMEWORK

Timely identification, escalation and communication of risks to ensure effective oversight, informed decision-making and regulatory compliance.



Risk indicators may include:

- Increase in customer complaints.
- Increase in suspicious activity alerts.
- Increase in payment disputes or chargebacks.
- Repeated failed verification attempts.
- Increased responsible gaming alerts.
- System downtime or service disruption.
- Withdrawal delays.
- Regulatory developments.
- Repeated control failures.
- Third-party service interruptions.
- Data protection incidents.
- High-risk customer activity.

Material risks shall be escalated according to their seriousness and potential impact.

Escalation may be made to:

- Department Managers.
- Compliance Function.
- MLRO.
- Responsible Gaming Officer.
- Data Protection Officer.
- Senior Management.

- Board of Directors.

Risk reporting supports informed decision-making, timely remediation, and effective governance oversight.

3.11 RISK REGISTER

The Company shall maintain a Risk Register documenting significant risks identified across its operations.

The Risk Register may include:

- Risk description.
- Risk category.
- Risk owner.
- Inherent risk rating.
- Existing controls.
- Residual risk rating.
- Mitigation actions.
- Action owners.
- Target completion dates.
- Review dates.
- Current status.

The Risk Register shall be reviewed periodically and updated whenever material changes occur to the Company's operations, regulatory obligations, risk profile, technology environment, products, payment arrangements, or third-party relationships.

The Risk Register supports management oversight, prioritisation of remediation actions, internal audit readiness, and regulatory transparency.

3.12 KEY CONTROLS

The Company's risk management framework is supported by the following key controls:

Control Area	Key Control
Governance	Risk oversight by Senior Management and the Board
Risk Ownership	Risks assigned to relevant departments and process owners
Risk Assessment	Risks assessed according to likelihood, impact, and control effectiveness
Risk Register	Significant risks documented and periodically reviewed
Compliance Monitoring	Regulatory and operational controls reviewed by Compliance
AML/CFT Monitoring	Financial crime risks monitored by the MLRO and relevant teams
Responsible Gaming Monitoring	Player protection risks reviewed and escalated where required
Incident Reporting	Material incidents documented, investigated, and escalated
Management Reporting	Significant risks reported to management for oversight and action
Continuous Improvement	Lessons learned used to strengthen controls and procedures

3.13 CONTINUOUS IMPROVEMENT

Risk management is an ongoing process. Mirage Corporation N.V. shall periodically review its risk management framework to ensure that it remains effective, proportionate, and aligned with the Company's business activities, regulatory obligations, customer protection responsibilities, and operational risk profile.

Improvements may arise from:

- Regulatory developments.
- Compliance reviews.
- AML/CFT reviews.
- Responsible Gaming assessments.
- Customer complaints.
- Payment investigations.
- Internal audits.
- Operational incidents.
- Technology incidents.
- Third-party reviews.
- Management recommendations.

Lessons learned shall be incorporated into policies, procedures, controls, training, monitoring activities, and management reporting to strengthen the Company's overall governance and control environment.

COMPLIANCE FRAMEWORK



4



4. COMPLIANCE FRAMEWORK

4.1 PURPOSE

The Compliance Framework establishes the governance arrangements, responsibilities, monitoring activities, and internal controls through which Mirage Corporation N.V. ensures compliance with applicable laws, regulatory requirements, licence conditions, industry standards, and internal policies.

Compliance forms an integral part of the Company's corporate governance framework and supports responsible business conduct, customer protection, operational integrity, and sustainable growth. The framework is designed to promote a proactive compliance culture by embedding regulatory obligations into the Company's day-to-day operations and decision-making processes.

Compliance activities are conducted using a risk-based approach and support all operational functions, including customer operations, responsible gaming, AML/CFT, payment processing, information security, data protection, finance, customer support, and business continuity.

4.2 COMPLIANCE OBJECTIVES

The objectives of the Compliance Framework are to:

- Promote compliance with all applicable legal, regulatory, and licensing obligations.
- Support the Company's commitment to ethical and responsible business conduct.
- Protect customers and maintain the integrity of gaming operations.
- Ensure policies and procedures remain aligned with applicable regulatory requirements.
- Identify, assess, and monitor compliance risks.

- Promote effective communication between business functions.
- Support operational decision-making through regulatory guidance.
- Facilitate timely reporting of compliance issues and regulatory matters.
- Promote continuous improvement through monitoring, review, and training.

The Compliance Framework operates alongside the Company's Risk Management Framework and supports the implementation of effective internal controls across all business activities.

4.3 COMPLIANCE GOVERNANCE

Compliance governance establishes clear accountability for regulatory compliance throughout the Company.

While the Compliance Function provides oversight and guidance, responsibility for compliance remains shared across all organisational levels.

Board of Directors

The Board provides oversight of the Company's compliance framework and receives periodic reporting regarding significant regulatory developments, compliance risks, and material compliance issues.

Senior Management

Senior Management is responsible for ensuring that regulatory obligations are incorporated into operational activities and that adequate resources are available to maintain an effective compliance framework.

Compliance Function

The Compliance Function independently monitors regulatory compliance, provides guidance to business units, supports policy development, conducts reviews, and reports significant compliance matters to Senior Management.

Department Heads

Department Heads are responsible for implementing compliance requirements within their respective business functions and ensuring employees follow approved policies and procedures.

Employees

All employees are responsible for complying with Company policies, reporting compliance concerns, and supporting the Company's commitment to responsible and compliant operations.



4.4 COMPLIANCE FUNCTION

The Compliance Function operates independently from day-to-day operational decision-making and provides objective oversight of the Company's regulatory obligations.

The Compliance Function may perform activities including:

- Regulatory monitoring.
- Compliance risk assessments.
- Policy development and maintenance.
- Internal compliance reviews.
- Advisory support.
- Regulatory reporting.
- Compliance investigations.
- Compliance training.
- Monitoring implementation of corrective actions.
- Supporting regulatory inspections and audits.

Compliance works collaboratively with all departments while maintaining independent oversight responsibilities.

4.5 MONEY LAUNDERING REPORTING OFFICER (MLRO)

The MLRO is responsible for overseeing the Company's AML/CFT framework and ensuring compliance with applicable financial crime legislation and regulatory expectations.

Responsibilities include:

- Oversight of AML/CFT controls.
- Suspicious activity reporting.

- Financial crime investigations.
- Customer risk assessments.
- Transaction monitoring oversight.
- Sanctions and PEP screening.
- AML/CFT training.
- Regulatory liaison where required.

The MLRO works closely with the Compliance Function while maintaining responsibility for financial crime oversight.

4.6 REGULATORY COMPLIANCE OBLIGATIONS

Mirage Corporation N.V. maintains procedures to ensure ongoing compliance with:

- Applicable gaming legislation.
- Licence conditions.
- AML/CFT legislation.
- Data protection requirements.
- Consumer protection obligations.
- Responsible Gaming requirements.
- Financial reporting obligations.
- Information security requirements.
- Corporate governance obligations.
- Internal policies and procedures.

Regulatory developments are monitored on an ongoing basis to ensure timely implementation of new requirements.

4.7 POLICIES AND PROCEDURES

The Company maintains documented policies and procedures covering key operational and regulatory areas.

Policies are designed to provide employees with clear guidance regarding their responsibilities and support consistent application of regulatory requirements.

Policies are periodically reviewed to ensure they remain current, effective, and aligned with changes in legislation, business operations, and industry best practices.

4.8 COMPLIANCE MONITORING AND TESTING

Compliance monitoring forms an essential part of the Company's governance framework.

Monitoring activities may include:

- Compliance reviews.
- File testing.
- Customer account reviews.
- Responsible Gaming monitoring.
- AML/CFT monitoring.
- Transaction sampling.
- Policy compliance testing.
- Incident reviews.
- Complaint analysis.
- Corrective action tracking.
- Third-party oversight reviews.

Monitoring activities are performed using a risk-based approach, with higher-risk areas receiving increased attention and more frequent review.

FIGURE 4.2
COMPLIANCE MONITORING AND REVIEW CYCLE

A continuous cycle that ensures compliance obligations are identified, monitored, evaluated and improved.



4.9 REPORTING AND ESCALATION

Compliance issues are reported through established reporting lines to ensure timely management attention and appropriate corrective action.

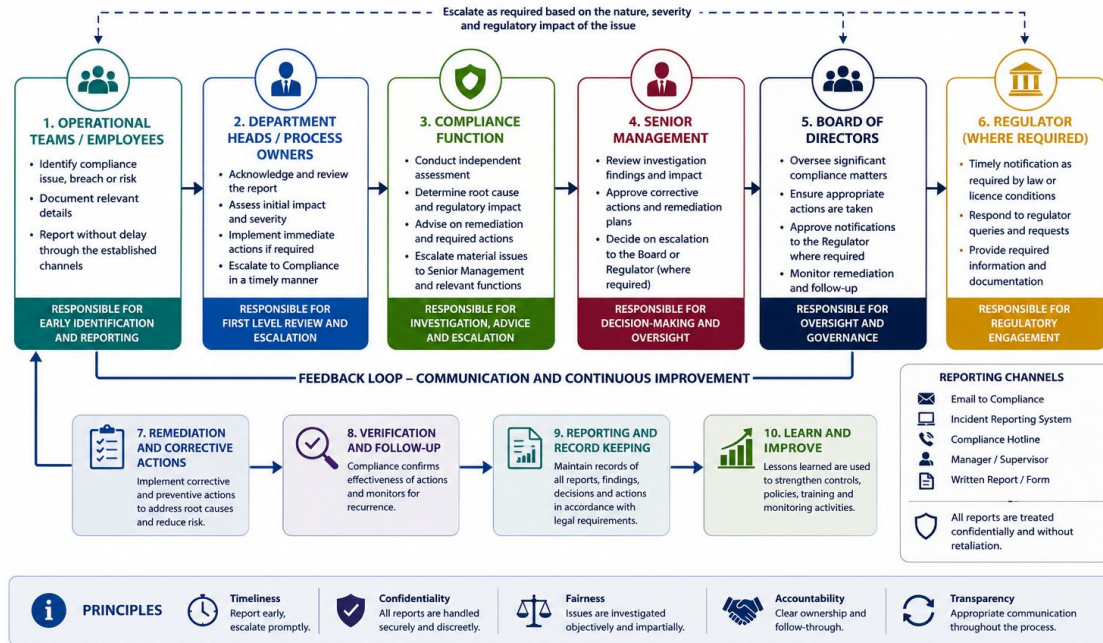
Reportable matters may include:

- Regulatory breaches.
- Policy breaches.
- AML/CFT concerns.
- Responsible Gaming issues.
- Customer protection failures.
- Information security incidents.
- Data protection issues.
- Operational control weaknesses.
- Audit findings.
- Significant customer complaints.

Where necessary, matters are escalated to Senior Management, the MLRO, the Board of Directors, or relevant regulatory authorities in accordance with applicable legal and regulatory requirements.

FIGURE 4.3 COMPLIANCE REPORTING AND ESCALATION WORKFLOW

A clear process for reporting, escalating and resolving compliance issues in a timely and effective manner.



4.10 TRAINING AND AWARENESS

Compliance training forms part of the Company's wider governance framework.

Employees receive training appropriate to their role and responsibilities.

Training may include:

- Regulatory obligations.
- AML/CFT.
- Responsible Gaming.
- Customer protection.
- Data protection.
- Information security.
- Internal policies.
- Incident reporting.
- Fraud awareness.

- Ethics and Code of Conduct.

Training records are maintained by the Company and reviewed periodically.

4.11 RECORD KEEPING

Compliance documentation is retained in accordance with applicable legal, regulatory, and operational requirements.

Records may include:

- Compliance monitoring reports.
- Internal review documentation.
- Regulatory correspondence.
- Training records.
- Risk assessments.
- Policy versions.
- Corrective action registers.
- Audit reports.
- Investigation records.
- Regulatory submissions.

Access to compliance records is restricted to authorised personnel.

4.12 KEY CONTROLS

Control Area	Key Control
Governance	Compliance oversight by Senior Management and Compliance Function
Monitoring	Risk-based compliance monitoring programme
Policies	Periodic review and approval of policies and procedures
Reporting	Escalation of significant compliance matters
Training	Mandatory compliance training for relevant employees
Record Keeping	Secure retention of compliance documentation
Reviews	Internal reviews and testing of key controls
Improvement	Tracking of corrective and preventive actions

4.13 CONTINUOUS IMPROVEMENT

Mirage Corporation N.V. is committed to continuously strengthening its compliance framework through regular review, monitoring, regulatory engagement, internal assessments, audit findings, operational experience, and industry best practices.

Compliance improvements may result from:

- Regulatory changes.
- Internal monitoring.
- Risk assessments.

- Audit recommendations.
- Customer complaints.
- Incident investigations.
- Lessons learned.
- Employee feedback.
- Management review.
- Technological developments.

The Compliance Function monitors the effectiveness of the framework and supports the implementation of improvements designed to strengthen governance, customer protection, and regulatory compliance across the organisation.

AML /CFT FRAMEWORK



5



5. ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING (AML/CFT) FRAMEWORK

5.1 PURPOSE

Mirage Corporation N.V. is committed to preventing its products, services, systems, and infrastructure from being used for money laundering, terrorist financing, fraud, sanctions evasion, or any other form of financial crime.

The Company has implemented an Anti-Money Laundering and Counter Terrorist Financing (AML/CFT) Framework designed to identify, assess, manage, and mitigate financial crime risks associated with its business activities. The framework adopts a risk-based approach consistent with applicable legal and regulatory requirements and industry best practices.

This chapter outlines the Company's AML/CFT governance arrangements, risk management principles, customer due diligence requirements, monitoring activities, reporting obligations, and record-keeping standards.

5.2 AML/CFT OBJECTIVES

The objectives of the AML/CFT Framework are to:

- Prevent the use of the Company's services for money laundering, terrorist financing, fraud, or other financial crime.
- Apply a risk-based approach to customer acceptance and ongoing monitoring.
- Ensure customers are appropriately identified and verified.
- Detect unusual or suspicious transactions.
- Support timely investigation and escalation of financial crime concerns.
- Maintain effective sanctions and PEP screening processes.
- Promote staff awareness through regular AML/CFT training.

- Maintain accurate records in accordance with legal and regulatory requirements.
- Support effective reporting to competent authorities where required.
- Continuously improve financial crime controls through monitoring and review.

5.3 GOVERNANCE AND OVERSIGHT

Board of Directors

The Board of Directors retains ultimate responsibility for oversight of the Company's AML/CFT programme.

The Board shall:

- Approve the AML/CFT Policy.
- Review financial crime risks.
- Ensure adequate resources are allocated to AML/CFT activities.
- Receive periodic reports from the MLRO.
- Review material AML/CFT incidents and emerging risks.

Senior Management

Senior Management is responsible for ensuring the effective implementation of the AML/CFT programme and supporting the Company's financial crime controls.

Money Laundering Reporting Officer (MLRO)

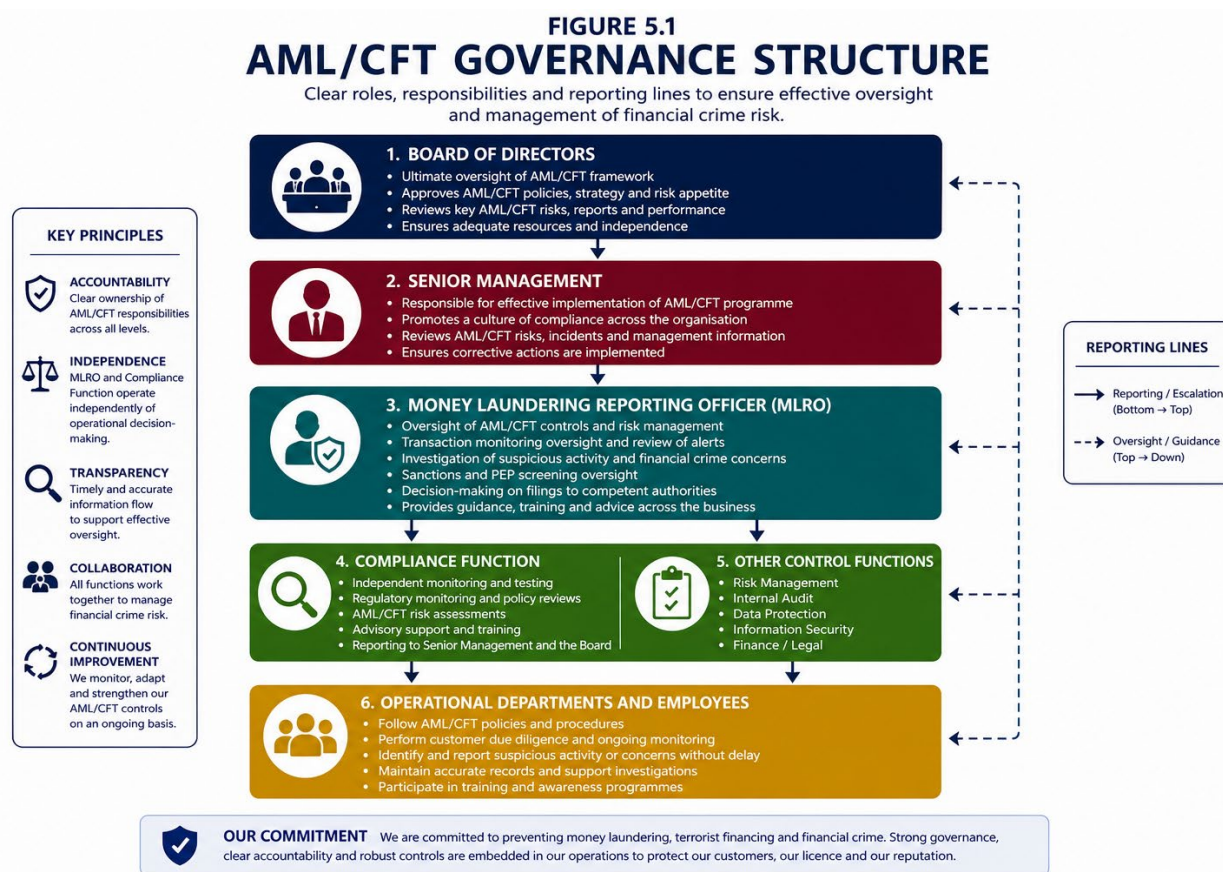
The MLRO is responsible for the day-to-day oversight and management of the AML/CFT programme.

Responsibilities include:

- Monitoring compliance with AML/CFT requirements.
- Conducting financial crime risk assessments.
- Reviewing suspicious activity.
- Managing sanctions and PEP screening processes.

- Maintaining AML/CFT procedures.
- Delivering AML/CFT training.
- Reporting significant AML/CFT matters to Senior Management and the Board.
- Liaising with competent authorities where required.

The MLRO shall have unrestricted access to information necessary to perform their duties effectively.



5.4 RISK-BASED APPROACH

Mirage Corporation N.V. applies a risk-based approach to AML/CFT compliance.

The Company assesses the level of financial crime risk associated with customers, products, services, transactions, geographical locations, and

delivery channels and applies controls proportionate to the level of risk identified.

The risk-based approach allows the Company to focus enhanced controls and monitoring on higher-risk relationships and activities.

5.5 FINANCIAL CRIME RISK ASSESSMENT

The Company periodically assesses its exposure to financial crime by considering:

- Customer risk.
- Geographic risk.
- Product risk.
- Payment risk.
- Delivery channel risk.
- Third-party risk.
- Emerging criminal typologies.

The assessment supports the allocation of monitoring resources and enhancement of internal controls.



Geographical Risk

The Company assesses risks associated with countries and jurisdictions connected to customers, payment methods, and transactions.

Particular attention is given to:

- High-risk jurisdictions.
- Sanctioned countries.
- Countries with weak AML controls.

- Jurisdictions identified by international bodies as presenting elevated financial crime risks.

Product and Transaction Risk

Assessment considers:

- Types of gaming products offered.
- Payment methods used.
- Transaction volumes.
- Transaction frequency.
- Deposit and withdrawal patterns.

Distribution Channel Risk

Risks associated with non-face-to-face relationships, online onboarding, and remote verification processes are assessed and mitigated through enhanced controls where necessary.

5.6 CUSTOMER DUE DILIGENCE

The Company applies Customer Due Diligence (CDD) measures to identify and verify customers before permitting certain activities and transactions.

CDD measures include:

- Identification and verification of customers.
- Verification of age.
- Verification of residential address.
- Screening against sanctions and PEP databases.
- Collection of additional information where necessary

Detailed Customer Due Diligence procedures are contained within Chapter 6 of this Manual.

5.7 ENHANCED DUE DILIGENCE

Enhanced Due Diligence (EDD) shall be applied where higher levels of risk are identified.

EDD measures may include:

- Obtaining additional identity documentation.
- Verification of source of wealth.
- Verification of source of funds.
- Enhanced transaction monitoring.
- Senior management approval.
- Increased review frequency.

EDD shall be applied where required by law, regulation, or internal risk assessments.

5.8 TRANSACTION MONITORING

The Company monitors customer activity to identify unusual, suspicious, or potentially criminal behaviour.

Monitoring activities may include:

- Large deposits.
- Unusual withdrawal patterns.
- Rapid movement of funds.
- Minimal gameplay activity.
- Structuring or smurfing behaviour.
- Use of multiple payment methods.
- Potential coin mixing indicators.
- Activity inconsistent with the customer's profile.

Alerts generated through monitoring systems shall be reviewed and investigated as appropriate.

FIGURE 5.3 TRANSACTION MONITORING WORKFLOW

A risk-based process to detect, review and manage potentially suspicious activity.



5.9 SANCTIONS AND PEP SCREENING

The Company screens customers against applicable sanctions lists and Politically Exposed Person (PEP) databases.

Potential matches shall be reviewed by Compliance or the MLRO prior to account approval or continuation of the customer relationship.

Higher-risk customers may be subject to Enhanced Due Diligence and ongoing monitoring.

5.10 SUSPICIOUS ACTIVITY REPORTING

Mirage Corporation N.V. maintains procedures for the identification, escalation, investigation, and reporting of unusual or suspicious activity in accordance with its AML/CFT obligations.

All employees, contractors, and relevant service providers are required to remain vigilant to indicators of potential money laundering, terrorist financing, fraud, sanctions evasion, identity theft, or other forms of financial crime. Any unusual or suspicious activity identified during the course of business must be reported immediately to the MLRO through the Company's internal reporting channels.

The MLRO shall:

- Review all internal reports of suspicious activity.
- Conduct investigations where necessary.
- Obtain additional information and supporting documentation where appropriate.
- Assess whether the activity presents a reasonable suspicion of money laundering, terrorist financing, fraud, or other criminal conduct.
- Determine whether further action, enhanced monitoring, account restrictions, or external reporting is required.
- Maintain appropriate records of all investigations, findings, decisions, and actions taken.

Employees must not disclose to customers or third parties that a suspicious activity review, investigation, or report has been initiated or is under consideration. Any unauthorised disclosure may constitute tipping-off and may result in disciplinary action and regulatory consequences.

All reports, investigations, and supporting documentation shall be treated as strictly confidential and retained in accordance with the Company's record-keeping requirements.

The detailed Suspicious Activity Reporting (SAR) procedure, including reporting workflows, escalation requirements, investigation methodology, external reporting obligations, confidentiality controls, and record retention standards, is contained within the Company's AML/CFT Policy and associated internal procedures.

FIGURE 5.4 SUSPICIOUS ACTIVITY REPORTING PROCESS

A clear escalation process to ensure timely identification, review and reporting of suspicious activity in accordance with legal and regulatory requirements.



5.11 RECORD KEEPING

The Company shall maintain AML/CFT records sufficient to demonstrate compliance with applicable legal and regulatory requirements.

Records may include:

- Customer identification documents.
- Verification records.
- Risk assessments.
- Monitoring alerts.
- Investigation files.
- Internal reports.
- Training records.

Records shall be retained for a minimum period prescribed by applicable laws and regulations.

5.12 TRAINING AND AWARENESS

All relevant employees shall receive AML/CFT training appropriate to their responsibilities.

Training shall include:

- Money laundering and terrorist financing risks.
- Customer Due Diligence requirements.
- Suspicious activity identification.
- Sanctions compliance.
- Reporting procedures.
- Regulatory obligations.

Training shall be conducted upon commencement of employment and periodically thereafter.

5.13 INDEPENDENT REVIEW AND CONTINUOUS IMPROVEMENT

5.14 Independent Review and Continuous Improvement

Mirage Corporation N.V. is committed to maintaining an effective and proportionate Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Framework through regular review, independent oversight, and continuous enhancement of its financial crime controls.

The effectiveness of the AML/CFT Framework is periodically assessed to ensure that policies, procedures, monitoring systems, and operational controls remain aligned with the Company's business activities, risk profile, applicable legal and regulatory requirements, and recognised industry best practices.

Independent reviews may be conducted through internal compliance assessments, management reviews, external audits, regulatory inspections, or other independent assurance activities, where appropriate. These reviews evaluate the effectiveness of the Company's governance arrangements, customer due diligence processes, transaction monitoring controls, sanctions screening procedures, suspicious activity reporting mechanisms, record-keeping practices, and employee awareness programmes.

Where weaknesses, deficiencies, or opportunities for improvement are identified, appropriate corrective and preventive actions are documented, assigned to responsible owners, and monitored through to completion. Progress is reviewed by the Compliance Function, the Money Laundering Reporting Officer (MLRO), and Senior Management to ensure that remediation measures are implemented effectively and within appropriate timeframes.

Continuous improvement of the AML/CFT Framework may be driven by:

- Regulatory developments and changes in applicable legislation.
- Updates to licence conditions or regulatory guidance.
- Emerging money laundering, terrorist financing, fraud, and sanctions typologies.
- Internal compliance reviews and quality assurance activities.
- External audits and independent assessments.
- Findings arising from transaction monitoring and suspicious activity investigations.
- Risk assessments and periodic business risk reviews.
- Lessons learned from incidents, investigations, or enforcement actions.
- Technological developments that enhance monitoring, screening, or reporting capabilities.
- Employee feedback and operational experience.

The Company recognises that financial crime risks continue to evolve and therefore maintains a proactive approach to reviewing and strengthening its AML/CFT controls. Through effective governance, independent oversight, and continuous improvement, Mirage Corporation N.V. seeks to maintain a robust financial crime compliance framework that supports regulatory compliance, protects the integrity of its operations, and safeguards its customers and the wider financial system.



CUSTOMER DUE DILIGENCE (CDD)

KNOW YOUR CUSTOMER (KYC)



6

6. CUSTOMER DUE DILIGENCE (CDD) AND KNOW YOUR CUSTOMER (KYC)

6.1 PURPOSE

Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures form a fundamental component of Mirage Corporation N.V.'s governance, customer protection, and Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) framework.

The purpose of this chapter is to establish the operational controls, responsibilities, and procedures through which customers are identified, verified, risk assessed, and monitored throughout the customer relationship lifecycle.

Effective customer due diligence supports the prevention of money laundering, terrorist financing, fraud, identity theft, underage gambling, sanctions breaches, and other financial crime while promoting responsible gaming and compliance with applicable legal and regulatory requirements.

The Company applies a risk-based approach to customer verification and ongoing monitoring, ensuring that the level of due diligence performed is proportionate to the customer's risk profile and the nature of the business relationship.

6.2 OBJECTIVES

The objectives of the Company's KYC programme are to:

- Verify the identity of customers.
- Prevent underage gambling.
- Identify higher-risk customers.
- Detect suspicious or unusual activity.
- Support AML/CFT compliance obligations.
- Protect the integrity of the Company's gaming operations.
- Ensure compliance with applicable regulatory requirements.

6.3 CUSTOMER IDENTIFICATION REQUIREMENTS

Prior to establishing or continuing a customer relationship, Mirage Corporation N.V. shall collect sufficient information to identify the customer.

Customer information may include:

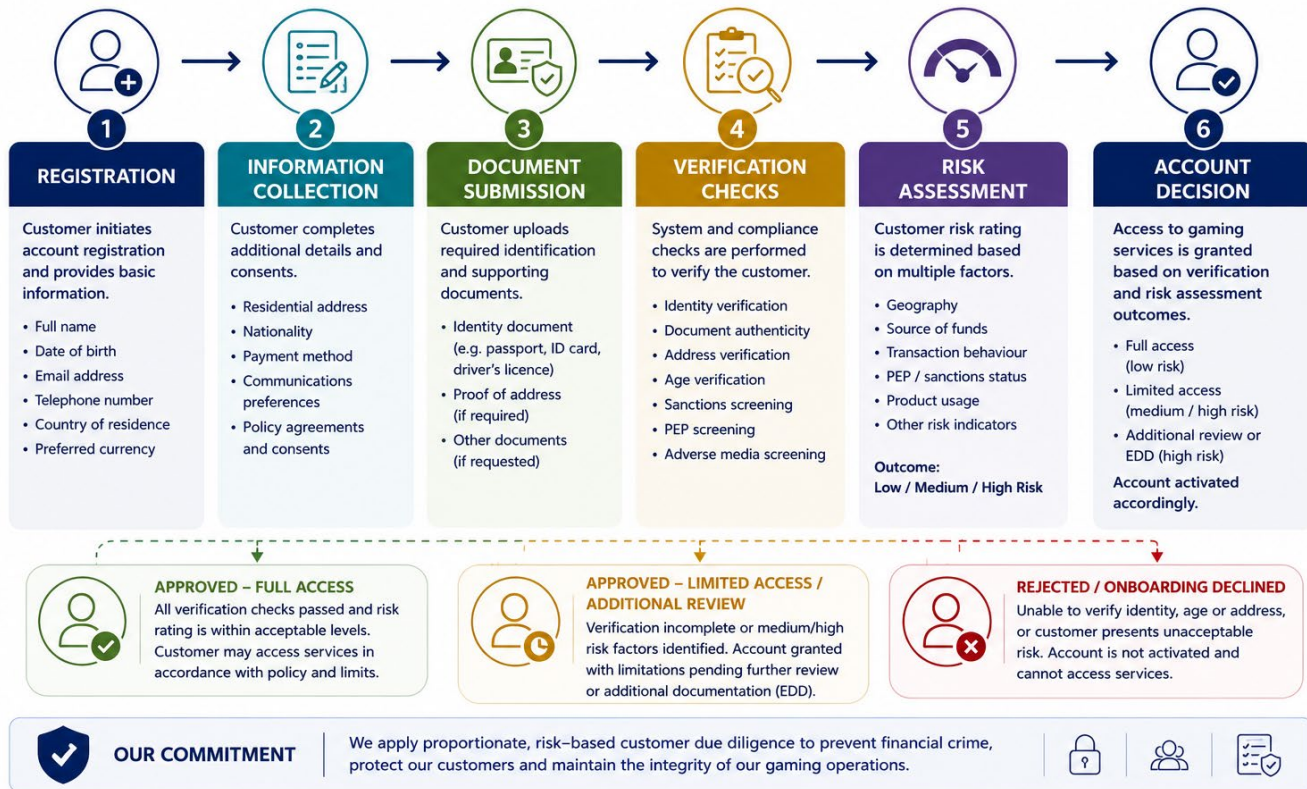
- Full legal name.
- Date of birth.
- Residential address.
- Nationality.
- Email address.
- Telephone number.
- Payment method information.
- Any additional information deemed necessary for risk assessment purposes.

Customer information must be accurate, complete, and capable of independent verification.

Customer information shall be reviewed and updated where changes are identified during the customer relationship or where additional due diligence is required.

FIGURE 6.1 – CUSTOMER ONBOARDING AND VERIFICATION JOURNEY

A structured, risk-based process to identify, verify and approve customers before access to gaming services is granted.



6.4 IDENTITY VERIFICATION

The Company shall take reasonable measures to verify the identity of all customers.

Acceptable identity documents may include:

- Valid passport.
- National identity card.
- Government-issued driver's licence.
- Other government-issued identification documents approved by the Compliance Function.

Verification procedures may include:

- Document verification.
- Electronic verification tools.

- Selfie verification.
- Third-party verification databases.
- Additional verification measures where appropriate.

The Company reserves the right to request additional documentation where there are doubts regarding the authenticity, accuracy, or completeness of information provided.

6.5 ADDRESS VERIFICATION

The Company may require customers to provide proof of residential address.

Acceptable proof of address documents may include:

- Utility bills.
- Bank statements.
- Government-issued correspondence.
- Tax documentation.
- Other reliable and independent documentation.

Proof of address documents should normally be recent and clearly display the customer's name and residential address.

6.6 AGE VERIFICATION

Mirage Corporation N.V. prohibits participation by persons under the age of eighteen (18) years. Age verification controls shall be implemented during customer registration and throughout the customer relationship where necessary.

Where the Company has reason to believe that a customer may be underage:

- The account shall be restricted immediately.
- Additional verification shall be requested.
- Deposits and wagering activity may be suspended.
- Appropriate regulatory and operational actions shall be taken.

Customers who fail age verification checks shall not be permitted to access the Company's services.

6.7 CUSTOMER RISK ASSESSMENT

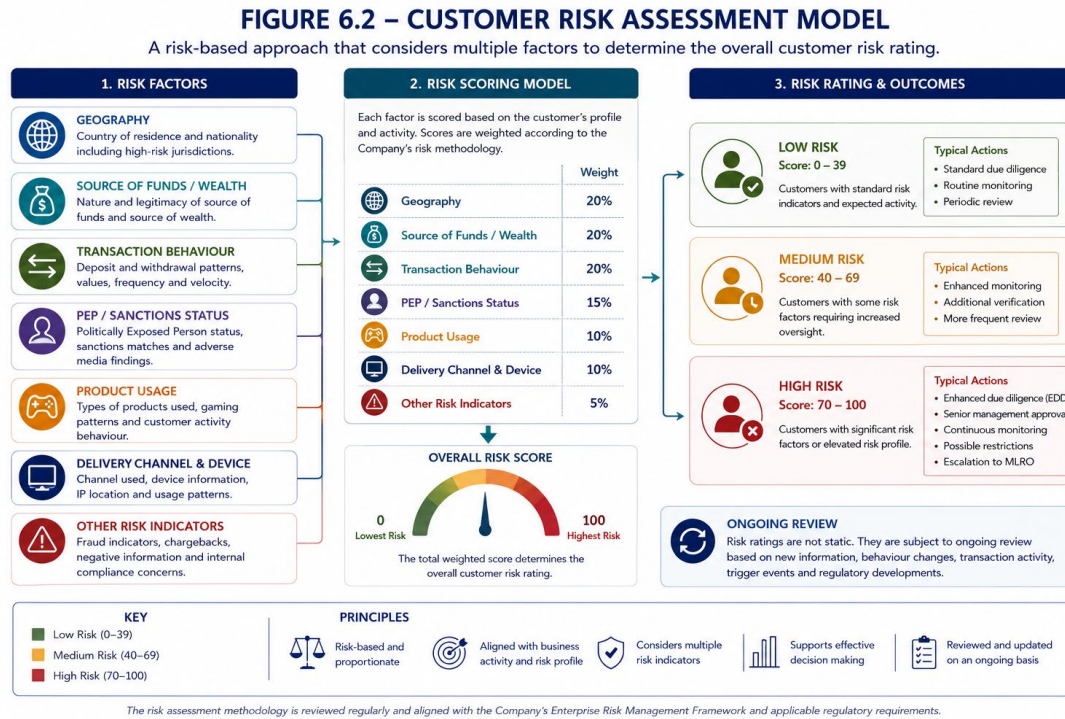
The Company applies a risk-based approach to customer due diligence.

Customers shall be assessed based on factors including:

- Country of residence.
- Nationality.
- Source of funds.
- Transaction behaviour.
- Politically Exposed Person (PEP) status.
- Sanctions screening results.
- Adverse media findings.
- Product usage patterns.
- Other risk indicators identified by the Company.

Customers may be categorised as low, medium, or high risk depending on the outcome of the assessment.

Customer risk ratings are subject to ongoing review and may be revised where new information, behavioural indicators, transaction activity, or regulatory requirements warrant a reassessment of the customer's overall risk profile.



6.8 TRIGGER EVENTS FOR VERIFICATION

Customer verification may be initiated at account registration, during ongoing monitoring activities, or upon the occurrence of specified trigger events.

Verification shall be completed when:

- Cumulative deposits reach or exceed €2,000.
- Unusual or suspicious activity is identified.
- Higher-risk indicators are detected.
- Regulatory requirements require additional verification.
- Compliance or the MLRO determines that further due diligence is necessary.

The Company reserves the right to initiate verification procedures at any time regardless of transaction value.

6.9 ENHANCED DUE DILIGENCE

Enhanced Due Diligence (EDD) measures shall be applied where higher levels of risk are identified.

EDD may be required for:

- Politically Exposed Persons (PEPs).
- Customers connected to higher-risk jurisdictions.
- Customers displaying unusual transaction behaviour.
- Customers subject to adverse media findings.
- Customers identified as presenting elevated money laundering or terrorist financing risks.

EDD measures may include:

- Additional identity verification.
- Source of Funds verification.
- Source of Wealth verification.
- Senior management approval.
- Enhanced transaction monitoring.
- More frequent account reviews.

6.10 ONGOING MONITORING

Mirage Corporation N.V. conducts ongoing monitoring of customer activity throughout the customer relationship.

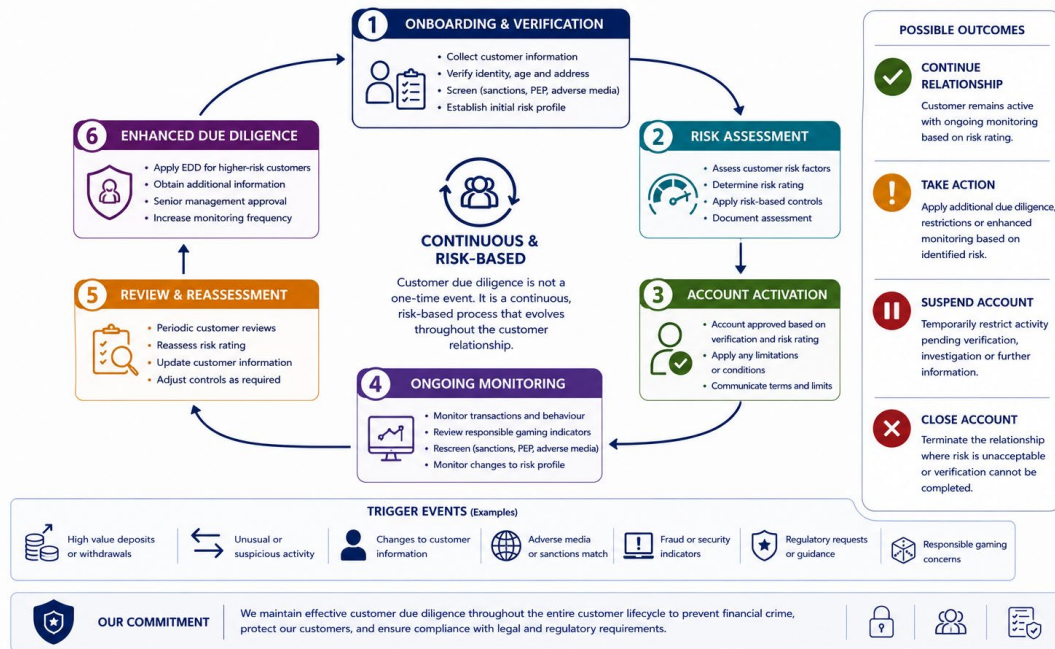
Monitoring activities may include:

- Transaction monitoring.
- Deposit and withdrawal reviews.
- Behavioural analysis.
- Responsible Gaming indicators.
- Changes in customer risk profile.
- Sanctions and PEP rescreening.
- Periodic customer reviews.

Monitoring activities are designed to identify unusual, suspicious, or potentially high-risk behaviour requiring further investigation. Monitoring supports the timely identification of changes in customer behaviour, financial crime indicators, responsible gaming concerns, and other events that may require additional due diligence or escalation to the Compliance Function or MLRO.

FIGURE 6.3 – CUSTOMER DUE DILIGENCE LIFECYCLE

Ongoing customer due diligence is a continuous process throughout the entire customer relationship.



6.11 ACCOUNT RESTRICTIONS AND FAILED VERIFICATION

Where a customer fails to provide requested documentation or where verification cannot be satisfactorily completed, the Company may apply restrictions to the customer account.

Such measures may include:

- Suspension of deposits.
- Suspension of withdrawals.
- Restriction of gameplay.
- Temporary account suspension.
- Account closure.

No withdrawals shall be processed until required verification measures have been completed and approved.

Where requested documentation is not provided within the required timeframe, the Company may close the customer account in accordance with its policies and regulatory obligations.

6.12 RECORD KEEPING

The Company shall maintain records relating to customer identification and verification activities.

Records may include:

- Identity documents.
- Proof of address documents.
- Verification reports.
- Risk assessments.
- Transaction monitoring records.
- Correspondence relating to verification activities.

Customer Due Diligence records shall be retained for a minimum of five (5) years following the end of the customer relationship or such longer period as required by applicable laws or regulatory requirements.

6.13 RESPONSIBILITIES

Compliance Function

The Compliance Function is responsible for:

- Oversees the implementation of the Company's CDD and KYC framework.
- Reviews customer verification procedures.
- Provides regulatory guidance.
- Monitors compliance with internal procedures.

MLRO

The MLRO shall oversee:

- Oversees customer risk assessments.
- Reviews Enhanced Due Diligence.
- Investigates higher-risk customers.
- Reviews suspicious activity.
- Supports financial crime reporting.

Operational Teams

Customer Support, Payments, Compliance, and other operational teams shall support the implementation of KYC procedures and escalate any concerns identified during customer interactions.

Customer Support

- Obtains verification documentation.
- Assists customers during verification.
- Escalates unusual behaviour.

Payments Team

- Reviews payment anomalies.
- Escalates suspicious payment activity.
- Supports transaction investigations.

Technology

- Maintains identity verification integrations.
- Supports automated verification tools.
- Maintains audit logs.

Senior Management

- Provides oversight of the CDD framework.
- Ensures adequate resources.
- Reviews significant customer risk issues.

6.14 KEY CONTROLS

The Company's Customer Due Diligence (CDD) and Know Your Customer (KYC) framework is supported by the following key operational controls:

Control Area	Key Control
Customer Identification	Collection of mandatory customer information during account registration.
Identity Verification	Verification of customer identity using reliable and independent documentation and/or approved electronic verification solutions.
Age Verification	Controls to prevent access to gambling services by persons under the age of eighteen (18) years.
Customer Risk Assessment	Application of a risk-based methodology to classify customers according to their money laundering, fraud, and customer protection risk profile.
Trigger Events	Ongoing monitoring of predefined events that require additional verification, review, or escalation.
Enhanced Due Diligence	Additional due diligence measures applied to higher-risk customers, including PEPs, high-risk jurisdictions, and customers displaying unusual activity.
Ongoing Monitoring	Continuous monitoring of customer transactions, behaviour, responsible gaming indicators, and changes to customer risk profiles throughout the business relationship.
Account Restrictions	Risk-based application of account limitations, suspensions, or closures where verification requirements are not satisfied or regulatory concerns are identified.
Record Keeping	Secure retention of customer identification, verification, risk assessment, and monitoring records in accordance with applicable legal and regulatory requirements.
Escalation & Reporting	Escalation of higher-risk customers, suspicious activity, or verification concerns to the Compliance Function and/or the MLRO for further assessment and action.

The effectiveness of these controls is subject to periodic review through compliance monitoring, internal assessments, audit activities, and management oversight to ensure they remain effective,

proportionate, and aligned with the Company's regulatory obligations and risk profile.

6.15 REVIEW AND CONTINUOUS IMPROVEMENT

Mirage Corporation N.V. shall periodically review its Customer Due Diligence and KYC procedures to ensure that they remain effective, proportionate, and aligned with applicable legal, regulatory, and operational requirements.

Updates may be implemented following regulatory changes, risk assessments, audit findings, operational developments, or emerging financial crime threats.

RESPONSIBLE GAMING



7

7. RESPONSIBLE GAMING

7.1 PURPOSE

Responsible Gaming is a fundamental component of Mirage Corporation N.V.'s customer protection framework and reflects the Company's commitment to providing gambling services in a fair, safe, transparent, and socially responsible manner.

The purpose of this chapter is to establish the governance arrangements, operational controls, customer protection measures, and intervention procedures through which the Company identifies, monitors, supports, and protects customers who may be at risk of experiencing gambling-related harm.

The Company adopts a proactive and risk-based approach to Responsible Gaming by combining behavioural monitoring, customer interactions, automated alerts, responsible gaming tools, and trained personnel to promote informed gambling decisions and minimise the potential for gambling-related harm throughout the customer lifecycle.

7.2 RESPONSIBLE GAMING OBJECTIVES

The Company's Responsible Gaming programme aims to:

- Protect vulnerable persons.
- Prevent underage gambling.
- Promote informed customer decision-making.
- Identify and support customers displaying indicators of gambling-related harm.
- Provide customers with tools to manage their gambling behaviour.
- Ensure compliance with applicable regulatory obligations.
- Promote a safe and sustainable gaming environment.

7.3 GOVERNANCE AND RESPONSIBILITIES

Mirage Corporation N.V. maintains a Responsible Gaming Framework overseen by the Responsible Gaming Officer (RGO) and supported by the Compliance Function and operational teams involved in customer interactions, account monitoring, payments, marketing, and customer support activities.

The Responsible Gaming Officer is responsible for ensuring the effective implementation and ongoing operation of the Company's Responsible Gaming Framework and customer protection measures.

The Responsible Gaming Officer's responsibilities include:

- Monitoring the effectiveness of responsible gaming controls and tools.
- Reviewing responsible gaming alerts and high-risk player cases.
- Assessing indicators of gambling-related harm.
- Coordinating responsible gaming interventions.
- Maintaining the Self-Exclusion Register.
- Monitoring compliance with responsible gaming obligations.
- Supporting responsible gaming training and awareness initiatives.
- Reviewing responsible gaming incidents and customer interactions.
- Reporting significant responsible gaming matters to Senior Management.
- Recommending improvements to the Company's responsible gaming programme.

The Compliance Function shall provide oversight and support to ensure that responsible gaming controls remain aligned with regulatory requirements and industry best practices.

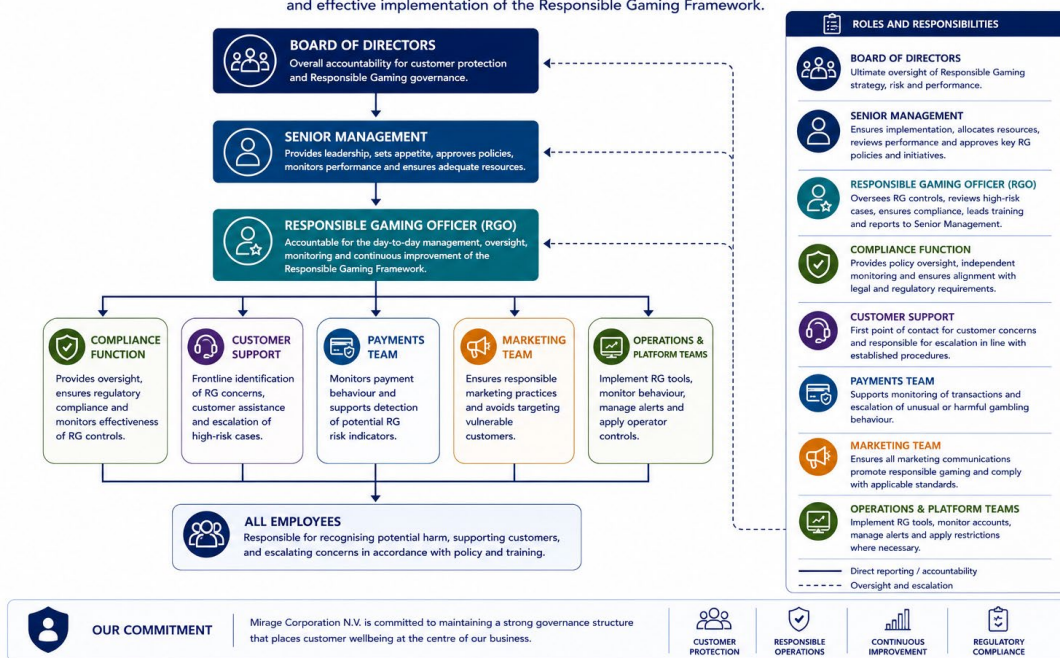
Operational teams, including Customer Support, Payments, VIP Management, Marketing, and Compliance personnel, are responsible

for identifying and escalating potential responsible gaming concerns encountered during customer interactions or account reviews.

All employees have a responsibility to support the Company's commitment to responsible gaming and must promptly escalate any concerns regarding customer welfare, gambling-related harm, or breaches of responsible gaming controls to the Responsible Gaming Officer.

FIGURE 7.1 – RESPONSIBLE GAMING GOVERNANCE FRAMEWORK

A multi-layered governance structure ensuring strong oversight, clear responsibilities and effective implementation of the Responsible Gaming Framework.



7.4 PROTECTION OF VULNERABLE PERSONS

The Company shall take reasonable measures to prevent vulnerable persons from accessing its products and services.

Vulnerable persons may include:

- Individuals under the age of eighteen (18).
- Persons displaying signs of gambling addiction or loss of control.
- Self-excluded individuals.

- Persons prohibited from participating in gaming activities under applicable laws or regulations.

Where indicators of vulnerability are identified, the Company may implement additional monitoring, restrictions, or intervention measures.

7.5 RESPONSIBLE GAMING INFORMATION

Customers shall be provided with clear and accessible information regarding responsible gaming throughout the customer journey.

Information made available to customers may include:

- Responsible Gaming Policy.
- Responsible Gaming tools.
- Self-assessment resources.
- Self-exclusion procedures.
- Cooling-off options.
- Deposit limit functionality.
- Contact information for gambling support organisations.
- Information regarding underage gambling prevention.

Responsible Gaming information shall be accessible through the Company's website and customer interfaces.

7.6 AGE VERIFICATION AND UNDERAGE GAMBLING PREVENTION

Mirage Corporation N.V. prohibits gambling by persons under eighteen (18) years of age.

Age verification controls shall form part of the customer onboarding and verification process.

Where there is reason to believe that a customer may be underage:

- The account shall be reviewed immediately.

- Appropriate verification measures shall be undertaken.
- Gambling activity may be restricted or suspended.
- Regulatory and operational actions shall be taken where necessary.

Customers who fail age verification checks shall not be permitted to use the Company's services.

7.7 BEHAVIOURAL MONITORING

The Company shall monitor customer behaviour to identify indicators of potential gambling-related harm.

Behavioural monitoring may include review of:

- Deposit frequency and amounts.
- Wagering behaviour.
- Session duration.
- Withdrawal reversals.
- Multiple payment methods.
- Attempts to circumvent responsible gaming controls.
- Customer communications.
- Requests for bonuses or incentives.
- Unusual spending patterns.
- Other indicators of potentially harmful gambling behaviour.

Monitoring may be performed through manual reviews, automated systems, platform tools, or a combination of these methods.

FIGURE 7.2 – BEHAVIOURAL MONITORING & EARLY INTERVENTION MODEL

A proactive, risk-based model to identify, assess and respond to potential gambling-related harm.



7.8 RESPONSIBLE GAMING INTERVENTIONS

Where potential gambling-related harm is identified, Mirage Corporation N.V. shall take appropriate action based on the level of risk identified.

Interventions may include:

- Responsible Gaming communications.
- Provision of educational materials.
- Encouragement to use responsible gaming tools.
- Deposit limit recommendations.
- Cooling-off recommendations.
- Temporary restrictions.
- Self-exclusion discussions.
- Operator-initiated restrictions or exclusions.

All interventions shall be documented and maintained within the relevant customer records.

The level of intervention shall be proportionate to the customer's assessed risk profile and may escalate where behavioural indicators continue or where previous interventions have proven ineffective.

7.9 COOLING-OFF PERIODS

Customers may voluntarily suspend their gambling activity by activating a Cooling-Off Period through the Company's Responsible Gaming tools or by contacting Customer Support. Cooling-off periods may include:

- 24 hours.
- 7 days.
- 1 month.
- 3 months.

Once activated:

- The cooling-off period shall take effect immediately.
- Access to relevant gaming activities shall be restricted.
- Customers shall not be encouraged to continue gambling.
- Appropriate account controls shall be applied.

Cooling-off periods shall be made easily accessible and available without unnecessary barriers.

7.10 SELF-EXCLUSION

Mirage Corporation N.V. maintains a self-exclusion programme allowing customers to voluntarily exclude themselves from gaming activities.

Self-exclusion options may include:

- 1 year.

- 3 years.
- 5 years.
- 10 years.
- Lifetime exclusion.

Upon activation of self-exclusion:

- Restrictions shall take effect immediately.
- The customer shall be prevented from participating in gaming activities.
- Marketing communications shall cease.
- Appropriate account restrictions shall be applied.
- Records shall be maintained within the Company's Self-Exclusion Register.

The Company shall take reasonable measures to prevent self-excluded individuals from circumventing restrictions through the creation of new accounts.



7.11 OPERATOR-INITIATED RESTRICTIONS

The Company reserves the right to apply restrictions, suspensions, or exclusions where customer behaviour indicates a significant risk of gambling-related harm or where regulatory obligations require intervention.

Such actions may include:

- Deposit restrictions.
- Account suspension.
- Temporary exclusion.
- Permanent exclusion.

All decisions shall be documented and supported by appropriate evidence.

7.12 DEPOSIT LIMITS AND PLAYER CONTROLS

Mirage Corporation N.V. provides customers with tools designed to assist them in managing their gambling activity.

Customers may establish:

- Daily deposit limits.
- Weekly deposit limits.
- Monthly deposit limits.
- Loss Limits
- Session Limits
- Wager Limits

Requests to reduce limits shall take effect immediately.

Requests to increase limits shall be subject to applicable waiting periods and review processes.

The Company may offer additional responsible gaming controls where appropriate.

7.13 REALITY CHECKS AND SELF-ASSESSMENT TOOLS

The Company may provide customers with responsible gaming tools designed to promote awareness of gambling behaviour.

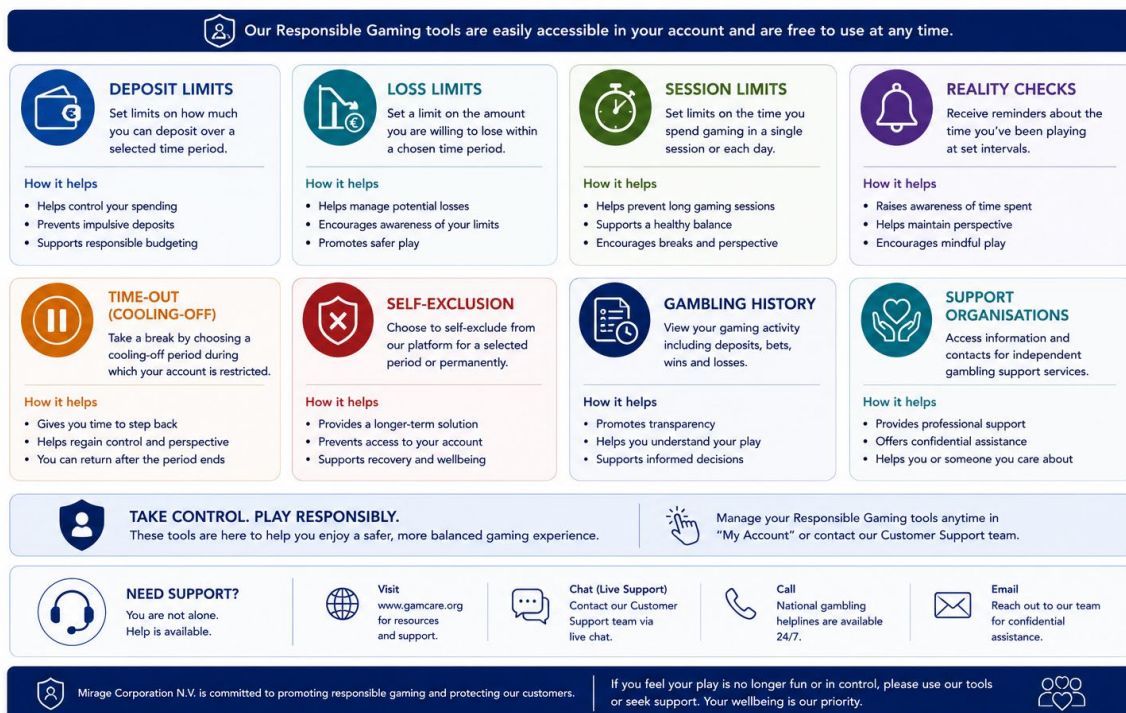
These tools may include:

- Session timers.
- Reality check notifications.
- Gambling history access.
- Self-assessment questionnaires.
- Educational content regarding responsible gaming.
- Links to organisations

Customers shall be encouraged to periodically review their gambling behaviour and utilise available tools where appropriate.

FIGURE 7.4 – RESPONSIBLE GAMING TOOLS OVERVIEW

A suite of tools designed to help customers manage their play, stay in control and make informed choices.



7.14 TRAINING AND AWARENESS

Employees whose duties involve customer interaction, account monitoring, compliance activities, or responsible gaming functions shall receive appropriate Responsible Gaming training.

Training shall include:

- Recognition of gambling-related harm indicators.
- Customer interaction techniques.
- Escalation procedures.
- Responsible Gaming tools.
- Regulatory obligations.
- Documentation requirements.

Training records shall be maintained by the Company.

7.15 RECORD KEEPING

Mirage Corporation N.V. shall maintain records relating to Responsible Gaming activities, including:

- Responsible Gaming interventions.
- Cooling-off requests.
- Self-exclusion requests.
- Operator-initiated exclusions.
- Customer communications.
- Training records.
- Monitoring activities.
- Behavioural monitoring alerts.
- Responsible Gaming assessments.
- Internal escalation records.
- Intervention outcomes.

Records shall be retained in accordance with applicable regulatory and legal requirements.

7.16 KEY CONTROLS

The Company's Responsible Gaming Framework is supported by the following key operational controls designed to promote customer protection, minimise gambling-related harm, and ensure compliance with applicable regulatory requirements:

Control Area	Key Control
Responsible Gaming Governance	Oversight of the Responsible Gaming Framework by the Responsible Gaming Officer (RGO), supported by the Compliance Function and Senior Management.
Behavioural Monitoring	Continuous monitoring of customer behaviour, gambling patterns, transaction activity, and responsible gaming indicators to identify customers who may be at risk of gambling-related harm.
Customer Risk Assessment	Risk-based assessment of customer behaviour and vulnerability to determine the appropriate level of monitoring and intervention.
Customer Interventions	Proportionate responsible gaming interventions, including customer communications, educational guidance, deposit limit recommendations, cooling-off periods, self-exclusion discussions, and operator-initiated measures where appropriate.
Player Protection Tools	Availability of responsible gaming tools including deposit limits, cooling-off periods, self-exclusion, reality checks, session reminders, and access to

	gambling history where supported by the platform.
Underage Gambling Prevention	Identity and age verification controls designed to prevent persons under the age of eighteen (18) from accessing the Company's gambling services.
Escalation and Decision-Making	Escalation of higher-risk customer cases to the Responsible Gaming Officer, Compliance Function, and Senior Management where appropriate to ensure timely and proportionate action.
Employee Training	Mandatory Responsible Gaming training for employees involved in customer interactions, compliance, payments, VIP management, and operational monitoring to ensure effective identification and handling of gambling-related harm indicators.
Record Keeping	Secure maintenance of Responsible Gaming assessments, customer interventions, self-exclusion records, cooling-off requests, operator-initiated restrictions, monitoring activities, and customer communications in accordance with applicable legal and regulatory requirements.
Continuous Monitoring and Review	Regular review of Responsible Gaming controls, customer protection measures, operational effectiveness, and regulatory developments to support continuous improvement of the Company's Responsible Gaming Framework.

The effectiveness of these controls is reviewed periodically through compliance monitoring, operational oversight, internal assessments, audit activities, customer feedback, and regulatory developments to ensure the Company's Responsible Gaming Framework remains effective, proportionate, and aligned with evolving regulatory expectations and industry best practices.

7.17 REVIEW AND CONTINUOUS IMPROVEMENT

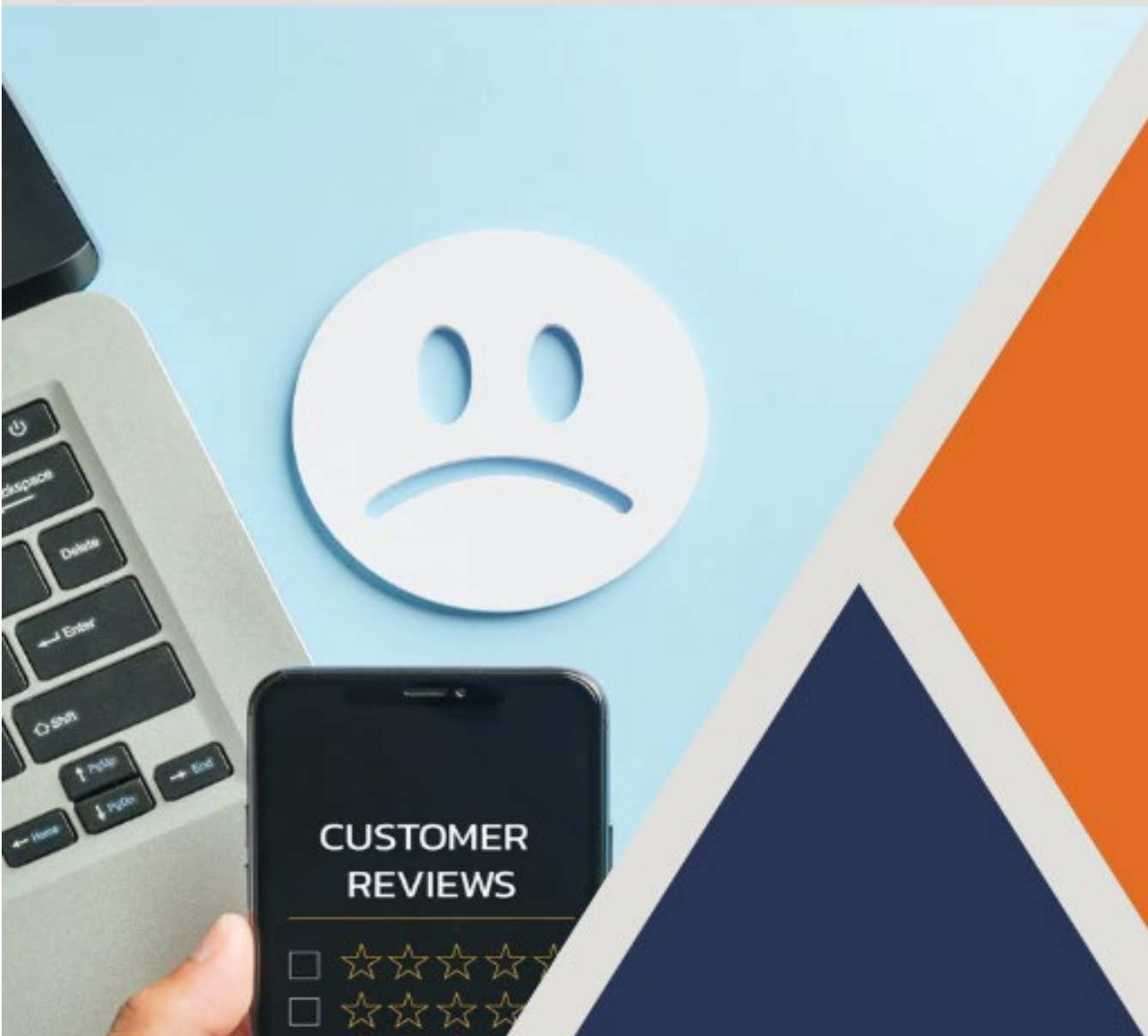
The Responsible Gaming Framework shall be reviewed periodically to ensure its effectiveness and continued alignment with regulatory expectations, operational requirements, and emerging industry best practices.

The Company shall continuously assess and improve its responsible gaming controls based on operational experience, monitoring activities, customer feedback, audit findings, and regulatory developments.



CUSTOMER COMPLAINTS AND DISPUTE RESOLUTION

8



8. CUSTOMER COMPLAINTS AND DISPUTE RESOLUTION

8.1 PURPOSE

Mirage Corporation N.V. is committed to providing customers with a fair, transparent, accessible, and efficient process for raising complaints, disputes, and service-related concerns.

The purpose of this chapter is to establish the governance arrangements, operational procedures, escalation mechanisms, and reporting requirements through which customer complaints are received, investigated, resolved, documented, and, where appropriate, escalated to an independent Alternative Dispute Resolution (ADR) provider.

An effective complaint management framework supports customer protection, promotes fair outcomes, strengthens operational controls, contributes to continuous improvement, and demonstrates the Company's commitment to regulatory compliance and high standards of customer service.

8.2 COMPLAINT MANAGEMENT PRINCIPLES

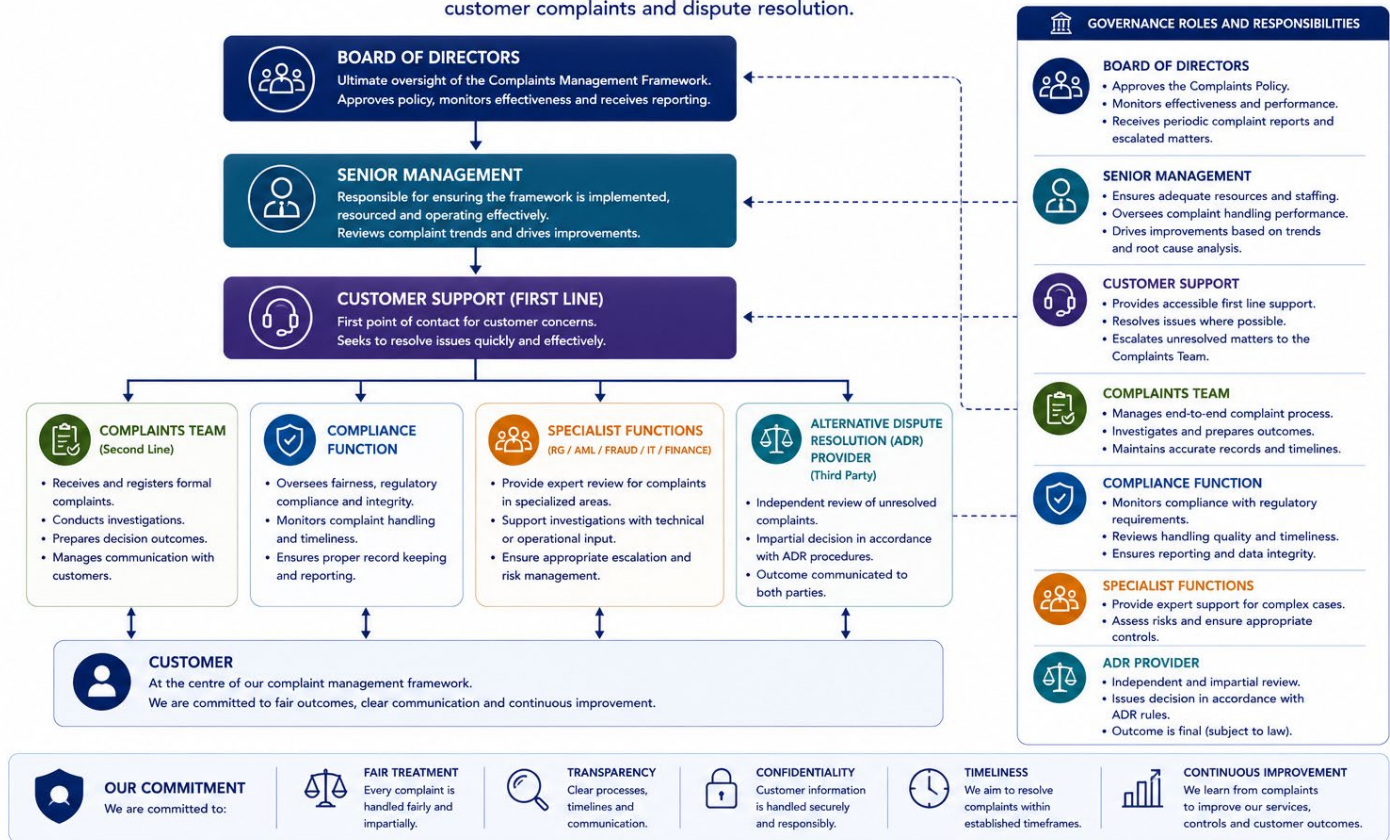
Mirage Corporation N.V. shall ensure that all complaints are handled in accordance with the following principles:

- Fairness.
- Transparency.
- Independency.
- Confidentiality.
- Objectivity.
- Timeliness.
- Consistency.
- Good faith resolution.

Customers shall not be disadvantaged for submitting a complaint and all complaints shall be reviewed impartially.

FIGURE 8.1 – CUSTOMER COMPLAINTS GOVERNANCE FRAMEWORK

A robust governance structure that ensures fair, transparent and effective handling of customer complaints and dispute resolution.



8.3 FIRST LINE RESOLUTION

Customer Support serves as the first point of contact for customers experiencing issues relating to their account, transactions, gameplay, promotions, verification requirements, or other operational matters.

Customer Support personnel shall make reasonable efforts to resolve customer concerns through available support channels before the matter enters the formal complaint process.

Customers may contact Customer Support through:

- Live Chat.
- Email.
- Website contact channels.

- Other approved customer communication channels.

Where a satisfactory resolution cannot be achieved, customers may submit a formal complaint in accordance with the procedures outlined below.

8.4 FORMAL COMPLAINT SUBMISSION

Customers who remain dissatisfied following interaction with Customer Support may submit a formal complaint.

Complaints should be submitted within six (6) months of the relevant incident or event giving rise to the complaint.

Formal complaints may be submitted through:

- The Company's online complaints form.
- Email using the prescribed complaint form.
- Other approved complaint submission channels made available by the Company.

Customers are encouraged to provide all relevant information and supporting documentation to facilitate investigation and resolution.

8.5 COMPLAINT REGISTRATION

Upon receipt of a formal complaint, the Company shall:

- Register the complaint within the Complaints Register.
- Assign a unique reference number.
- Categorise the complaint.
- Assign responsibility for investigation.
- Determine the complaint priority and applicable response timeframe
- Record all supporting information and communications.

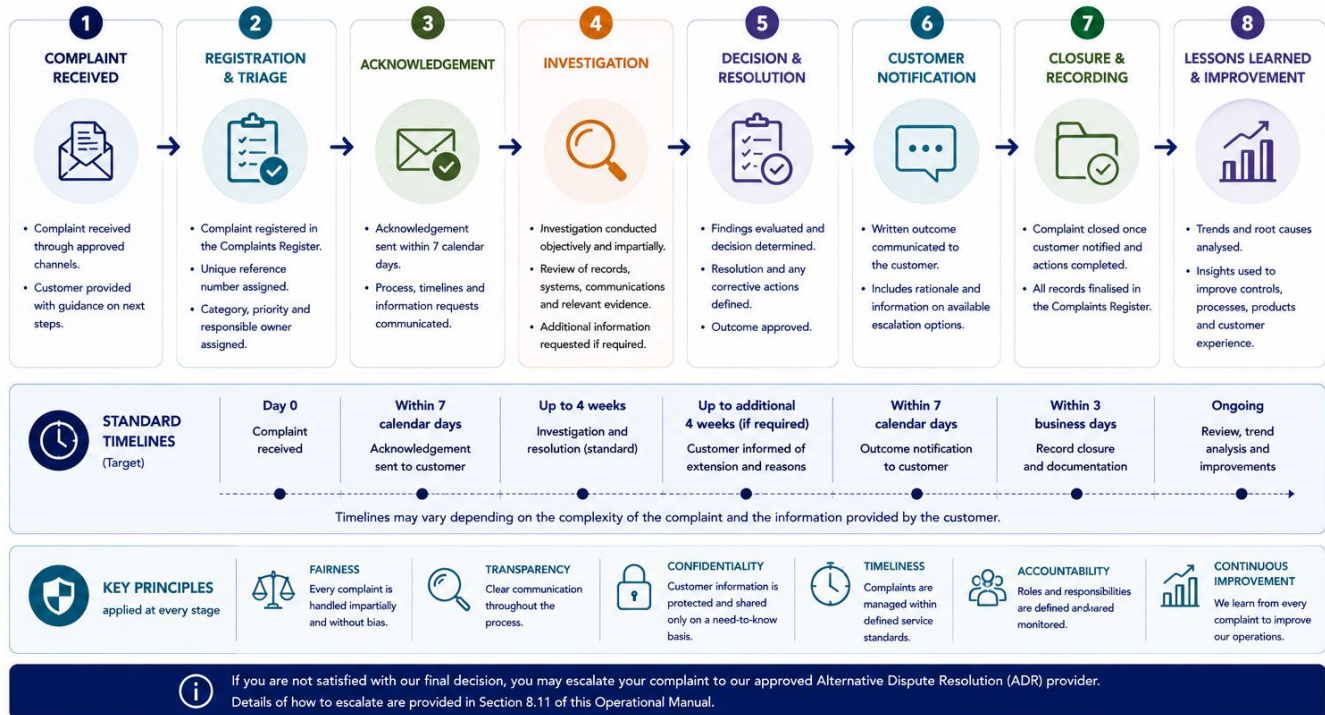
Each complaint shall be tracked from receipt through to closure.

FIGURE 8.2 – COMPLAINT HANDLING LIFECYCLE

A structured, fair and transparent process for managing customer complaints from receipt to closure.



Our commitment: Every complaint is handled fairly, objectively and in a timely manner, with the goal of achieving a fair outcome and continuous improvement.



8.6 COMPLAINT ACKNOWLEDGEMENT

The Company shall acknowledge receipt of a complaint within seven (7) calendar days of receipt.

The acknowledgement shall include:

- Confirmation that the complaint has been received.
- Information regarding the complaint handling process.
- Expected timelines for investigation and resolution.
- Any additional information required from the customer.

8.7 INVESTIGATION PROCESS

All complaints shall be investigated fairly, objectively, and in accordance with applicable policies and procedures.

Investigations may include:

- Review of account records.
- Review of transaction history.
- Review of gameplay records.
- Review of audit logs where applicable.
- Review of system records and platform logs.
- Review of customer communications.
- Review of promotional terms and conditions.
- Consultation with operational departments.
- Consultation with Compliance, AML, Responsible Gaming, or other relevant functions.

The Company may request additional information from the customer where necessary to complete the investigation.

Failure to provide requested information may result in the complaint being rejected or closed where the Company is unable to reasonably assess the matter.

8.8 COMPLAINT RESOLUTION

Mirage Corporation N.V. aims to resolve complaints within four (4) weeks of receipt.

Where a complaint is particularly complex, the Company may extend the investigation period by up to an additional four (4) weeks.

Where an extension is required:

- The customer shall be informed in writing.
- Reasons for the extension shall be provided.
- An updated estimated resolution date shall be communicated.

At the conclusion of the investigation, the customer shall receive a written decision outlining:

- The outcome of the complaint.

- Supporting reasoning.
- Any corrective actions taken.
- Available escalation options where applicable.

Where appropriate, remedial actions, goodwill gestures, refunds, account corrections, or operational improvements may be implemented following the outcome of the investigation.

8.9 RESPONSIBLE GAMING COMPLAINTS

Complaints relating to Responsible Gaming matters shall receive priority handling.

The Company aims to resolve Responsible Gaming complaints within five (5) business days and no later than two (2) weeks from receipt.

Where appropriate, Responsible Gaming complaints may be referred to the Responsible Gaming Officer for review and investigation.

8.10 COMPLAINT CATEGORIES

Complaints shall be classified according to the nature of the issue.

Categories may include:

1. Deposit or withdrawal issues.
2. Bonus disputes.
3. Account restrictions or account closures.
4. Game errors or game fairness concerns.
5. Responsible Gaming matters.
6. Player balance disputes.
7. KYC and verification concerns.
8. Data protection and privacy concerns.

9. Technical or software issues.
10. AML/CFT related concerns.
11. Underage gambling concerns.
12. Fraud-related matters.
13. Regulatory or licensing concerns.

The Company may create additional categories where necessary to support effective reporting and trend analysis.

8.11 ALTERNATIVE DISPUTE RESOLUTION (ADR)

Where a complaint cannot be resolved internally, the customer may escalate the matter to the Company's approved Alternative Dispute Resolution (ADR) provider.

The ADR process shall:

- Be available free of charge to customers.
- Be conducted independently of the Company.
- Provide impartial review of the complaint.
- Follow the procedures established by the appointed ADR provider.

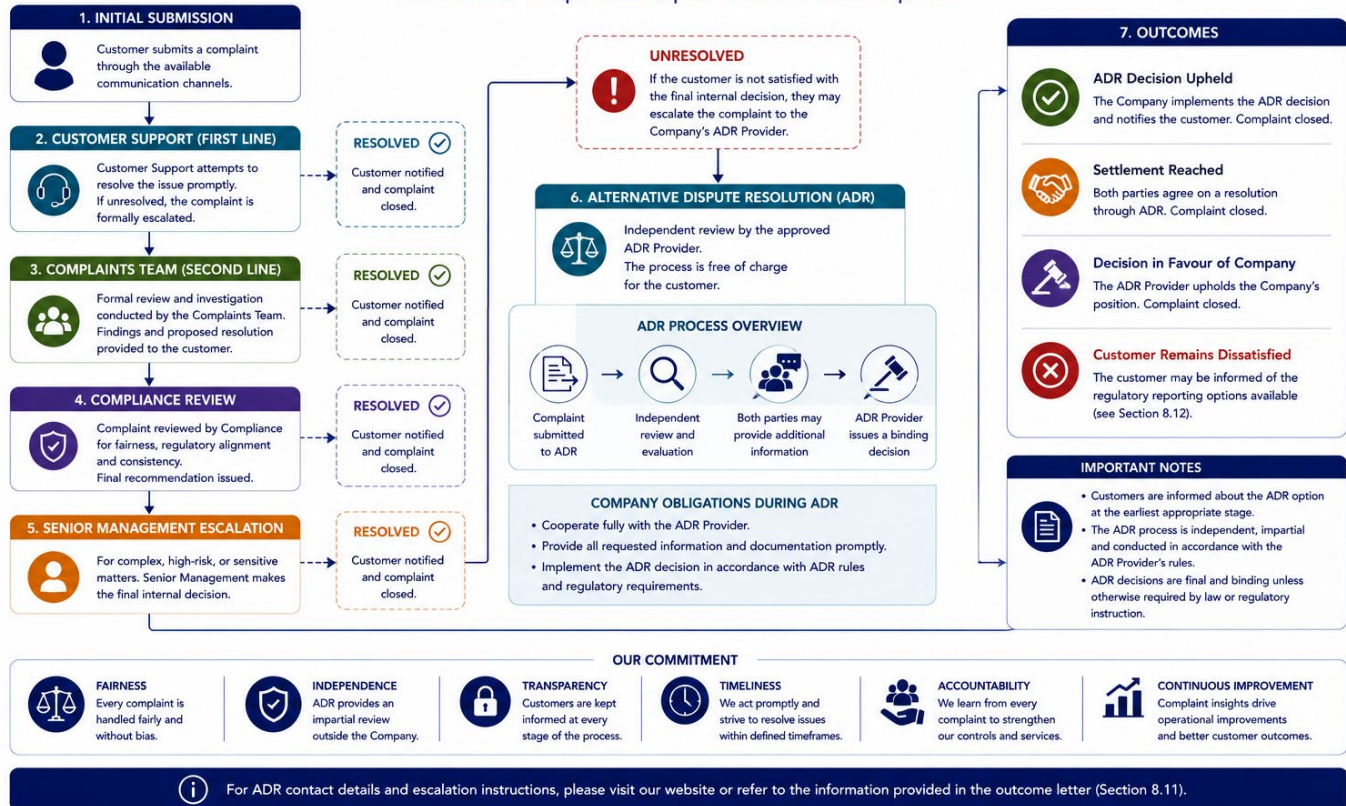
Customers shall be provided with ADR contact information and instructions regarding the escalation process.

While a complaint is under review by the ADR provider, the Company shall cooperate with the ADR process and provide relevant information as required.

The outcome issued by the ADR provider shall be treated as final unless otherwise required by law or regulatory instruction.

FIGURE 8.3 – COMPLAINT ESCALATION & ADR PROCESS

Clear escalation pathways ensure that every complaint receives appropriate review and access to independent dispute resolution when required.



8.12 REGULATORY ESCALATION

Customers may be informed that the Curaçao Gaming Authority does not generally intervene in individual gambling disputes.

Where a customer believes that the Company has breached regulatory obligations, the customer may be directed to the appropriate regulatory reporting channels maintained by the Curaçao Gaming Authority.

8.13 COMPLAINTS REGISTER

Mirage Corporation N.V. shall maintain a Complaints Register containing:

- Complaint reference number.
- Date received.
- Customer details.
- Complaint category.
- Investigation status.
- Resolution date.
- Outcome.
- ADR referrals where applicable.
- Any legal proceedings associated with the complaint.

The Complaints Register shall be reviewed periodically to identify recurring issues, operational weaknesses, and opportunities for improvement.

8.14 RECORD KEEPING

The Company shall retain complaint records for a minimum period of five (5) years.

Records shall include:

- Complaint submissions.
- Supporting documentation.
- Investigation records.
- Internal communications.
- Customer communications.
- ADR decisions.
- Legal correspondence where applicable.

Records shall be maintained securely and made available to competent authorities upon lawful request.

8.15 REPORTING

The Company shall prepare complaint management reports for regulatory and management purposes.

Reports may include:

- Total number of complaints received.
- Number of complaints by category.
- Number of complaints resolved.
- Number of complaints pending.
- Number of complaints referred to ADR.
- ADR outcomes.
- Complaint trends and root cause analysis.
- Legal proceedings arising from complaints.
- Average response time.
- Average resolution time.

Where required by applicable regulations, complaint reports shall be submitted to the Curaçao Gaming Authority within prescribed reporting periods.

8.16 KEY CONTROLS

The Company's Customer Complaints and Dispute Resolution Framework is supported by the following key operational controls:

Control Area	Key Control
Complaint Accessibility	Multiple communication channels are available to enable customers to submit complaints easily and without unnecessary barriers.
Complaint Registration	All formal complaints are assigned a unique reference number, categorised, recorded in the Complaints Register, and tracked throughout their lifecycle.
Investigation Process	Complaints are investigated objectively using customer records, transaction history, gameplay logs,

	communications, and other relevant operational information.
Escalation Procedures	Higher-risk, complex, Responsible Gaming, AML/CFT, fraud, or regulatory complaints are escalated to the appropriate specialist functions for review.
Resolution Management	Complaints are resolved within established service standards wherever possible, with customers receiving clear explanations and information regarding available escalation options.
Alternative Dispute Resolution (ADR)	Customers who remain dissatisfied following the Company's internal complaint process may refer their complaint to the approved ADR provider for independent review.
Reporting and Trend Analysis	Complaint data is analysed to identify recurring issues, operational weaknesses, emerging risks, and opportunities for continuous improvement.
Record Keeping	Complaint records, supporting documentation, communications, investigations, ADR decisions, and related evidence are securely maintained in accordance with applicable legal and regulatory requirements.
Management Oversight	Senior Management receives periodic reporting on complaint volumes, resolution performance, complaint trends, and significant customer protection issues.
Continuous Improvement	Findings arising from complaints, customer feedback, audit activities, regulatory developments, and ADR

	outcomes are used to strengthen operational processes, controls, and customer experience.
--	---

The effectiveness of these controls is reviewed periodically through compliance monitoring, internal assessments, management oversight, and audit activities to ensure that the Company's complaint handling framework remains fair, transparent, efficient, and aligned with applicable regulatory requirements and industry best practices.

8.17 REVIEW AND CONTINUOUS IMPROVEMENT

Mirage Corporation N.V. shall periodically review its complaint handling framework to ensure ongoing effectiveness, fairness, and regulatory compliance.

Lessons learned from complaints, ADR decisions, customer feedback, audit findings, and regulatory developments shall be used to improve products, services, controls, and customer outcomes.



PAYMENT OPERATIONS AND FINANCIAL CONTROLS

9



9. PAYMENT OPERATIONS AND FINANCIAL CONTROLS

9.1 PURPOSE

The Payments Department is responsible for managing all monetary transactions between customers and Mirage Corporation N.V., ensuring secure payment processing, compliance with regulatory obligations, fraud prevention, transaction monitoring, and operational efficiency across all payment channels.

The department oversees deposit and withdrawal processing, payment method verification, transaction monitoring, fraud detection, payment service provider (PSP) management, chargeback handling, reconciliation activities, and financial crime escalation procedures.

The Payments Department operates as a key operational control function and forms part of the Company's first line of defence against financial crime, fraud, and payment-related risks.

9.2 DEPARTMENT STRUCTURE AND RESPONSIBILITIES

The Payments Department operates under the supervision of the Head of Payments and consists of Payments Associates responsible for daily payment operations and transaction monitoring activities.

The department's responsibilities include:

- Deposit processing.
- Withdrawal processing.
- Payment method verification.
- Fraud prevention and detection.
- Transaction monitoring.
- PSP management.
- Chargeback management.
- Reconciliation activities.
- AML and financial crime escalation.
- Operational reporting and analytics.

The Payments Department works closely with Compliance, AML, Responsible Gaming, Customer Support, Finance, and external PSPs to ensure secure and compliant payment operations.

9.3 OPERATIONAL SYSTEMS AND MONITORING INFRASTRUCTURE

Mirage Corporation N.V. utilises a combination of payment orchestration platforms, PSP back-office systems, fraud monitoring tools, business intelligence dashboards, and internal operational systems to manage payment activities.

The primary systems utilised by the Payments Department include:

PaymentIQ

PaymentIQ serves as the Company's primary payment orchestration and transaction monitoring platform and supports:

- Deposit processing.
- Withdrawal processing.
- Risk scoring.
- Transaction routing.
- PSP integrations.
- Fraud detection.
- Velocity monitoring.
- Transaction monitoring.

SumSub

SumSub supports:

- Identity verification.
- Document verification.
- Liveness verification.
- AML screening.
- PEP screening.

- Sanctions screening.

Internal Back Office

The Internal Back Office provides operational access to:

- Customer accounts.
- Transaction histories.
- Payment records.
- Internal notes.
- Risk indicators.
- AML reviews.
- Customer activity.

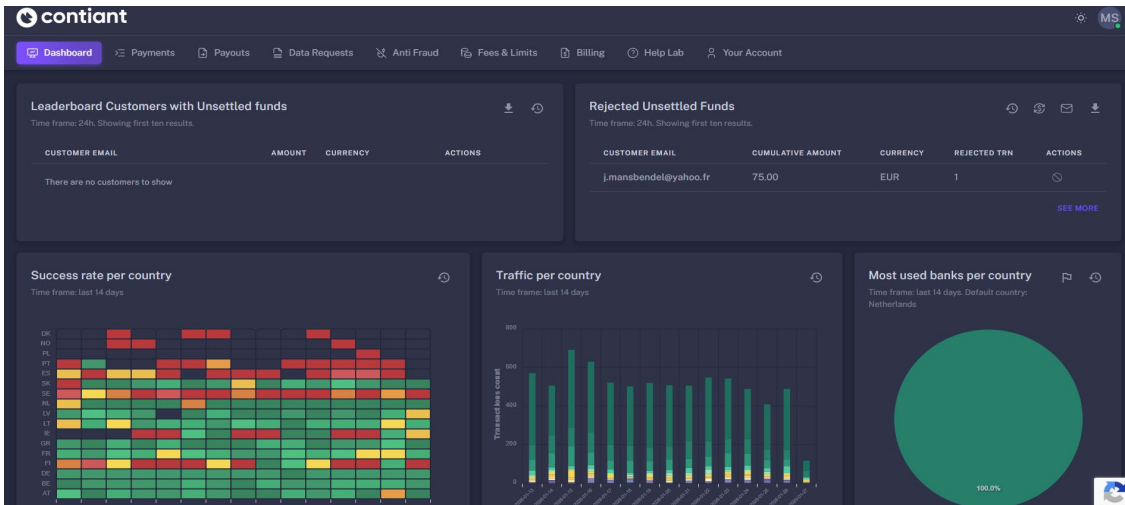
PSP Dashboards

PSP dashboards are utilised for:

- Transaction verification.
- Settlement monitoring.
- Chargeback management.
- Reconciliation activities.
- Transaction investigations.

Business Intelligence and Reporting Tools

The Payments Department utilises operational dashboards and analytics platforms to monitor transaction performance, payment success rates, PSP performance, fraud indicators, operational KPIs, and financial reporting metrics.



9.4 DEPOSIT PROCESSING

All customer deposits are processed through approved payment methods and PSPs.

Deposit Workflow

Step 1 – Deposit Initiation

The customer selects a payment method and initiates a transaction through the cashier interface.

The payment system identifies:

- Payment method.
- Currency.
- Applicable routing logic.
- Jurisdictional requirements.

Step 2 – PSP Processing

The transaction is routed to the relevant PSP for authorisation and processing.

The PSP returns a transaction status of:

- Approved.

- Declined.
- Pending.

Step 3 – Automated Risk Assessment

All deposits undergo automated risk assessment.

Risk controls include:

- Velocity monitoring.
- Device fingerprinting.
- IP analysis.
- BIN analysis.
- Country risk checks.
- Transaction threshold reviews.
- Wallet validation.
- Payment method ownership consistency checks.

Step 4 – Review and Decision

Transactions are processed according to risk profile:

- Low-risk transactions may be approved automatically.
- Medium-risk transactions may require review.
- High-risk transactions may be rejected or escalated.

Step 5 – Crediting of Funds

Approved deposits are credited to the customer's account balance.

Payments

Customers

Balances

Pay-ins

Payouts

Search

Transaction ID

Reference

Customer ID

Searchable text

Filter

Date: 01/01/2026 - 27/01/2026

+ Add filter

Clear all

Apply

Learn more about payment statuses

Export CSV

Date	Transaction ID	Customer ID	Reference	Bank	Status	Amount	Searchable text
27 Jan 2026, 11:05:46	58bcb5df-3dc0-bc35-fdf3-4852ce	5973803	3248322656		Completed	20,00 €	
27 Jan 2026, 11:00:58	4a89f5a5-1869-c9fd-e014-e9c569	5973803	3248315870		Completed	20,00 €	
27 Jan 2026, 10:59:20	bc5f62ec-32d2-17c8-90e3-f60314	10740417	3248313787	N26	Completed	400,00 €	
27 Jan 2026, 10:59:05	ad4b8697-fdb7-288e-09b2-4aa27b	10002757	3248313414		Completed	100,00 €	
27 Jan 2026, 10:59:04	72451229-41a7-9341-740d-4085a2	5973803	3248313398		Completed	20,00 €	
27 Jan 2026, 10:57:59	9ab25d59-a9e0-31fa-d399-f659a2	11624631	3248311909	Revolut	Completed	50,00 €	
27 Jan 2026, 10:52:36	0a27ba85-5ba9-409e-ee77-44d9f7	4945525	3248304431		Pending ASPSP acceptance	25,00 €	
27 Jan 2026, 10:51:07	836326cd-df60-bc14-3479-d0b764	5764529	3248302416		Completed	100,00 €	
27 Jan 2026, 10:50:00	80104ebc-14b0-8745-bd6b-666bd	1963445	3248300884		Completed	20,00 €	
27 Jan 2026, 10:48:17	9a5ebd9f-0793-0d4d-c86d-862749	10031917	3248298338		Completed	55,00 €	
27 Jan 2026, 10:45:26	b7b3a720-9fda-ea48-05af-1d7109	11624631	3248294569	Revolut	Completed	50,00 €	

Rows per page: 50

1-50 of 6344

Provide feedback

Settings

Legal Hub

YASPA © 2026 - ALL RIGHTS RESERVED.

9.5 WITHDRAWAL PROCESSING

All withdrawal requests are subject to operational, AML, fraud prevention, and KYC controls before approval.

Withdrawal Review Controls

Prior to approval, the following checks may be conducted:

- Identity verification.
- Address verification.
- Liveness verification.
- Payment method ownership validation.
- Transaction history review.
- Source of Funds review.
- Fraud indicators.
- AML risk indicators.

Where risk indicators are identified, withdrawals may be subject to manual review and escalation.

The Payments Department aims to process withdrawals efficiently while ensuring regulatory compliance and customer protection.

9.6 FRAUD PREVENTION AND TRANSACTION MONITORING

The Payments Department performs continuous monitoring of customer payment activity to identify fraud, financial crime, operational risk, and unusual transaction behaviour.

Monitoring activities include:

Automated Monitoring

- Velocity monitoring.
- Device and IP fingerprinting.
- BIN checks.
- Country mismatch reviews.
- Payment method ownership reviews.
- Repeated failed deposits.
- High-value transaction alerts.

Behavioural Monitoring

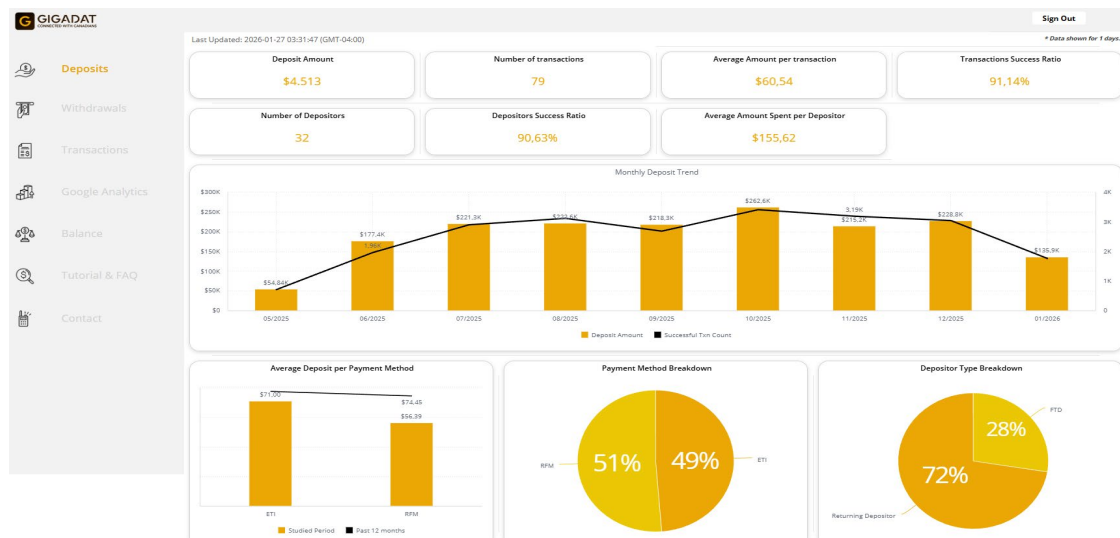
- Deposit-withdrawal cycling.
- Minimal gameplay following deposits.
- Shared devices.
- Multiple payment methods.
- Abnormal transaction patterns.
- Sudden behavioural changes.

Manual Monitoring

Payments personnel review:

- Flagged transactions.
- High-risk withdrawals.
- AML alerts.
- Fraud alerts.
- Operational exceptions.

Transactions may be restricted pending investigation where concerns are identified.



9.7 AML AND FINANCIAL CRIME ESCALATION

The Payments Department acts as a first-line control function in the identification and escalation of financial crime risks.

Transactions shall be escalated where:

- Velocity alerts are triggered.
- Source of Funds concerns arise.
- Behaviour is inconsistent with customer profiles.
- High-risk payment methods are identified.
- Transaction activity appears suspicious.
- Blacklist matches occur.

Escalated cases shall be reviewed by AML and Compliance personnel and, where necessary, referred to the MLRO.

All investigations, findings, and decisions shall be documented within the Company's AML monitoring systems.

9.8 CHARGEBACKS AND DISPUTES

The Payments Department manages the full lifecycle of chargebacks and PSP disputes.

Activities include:

- Receiving chargeback notifications.
- Gathering supporting evidence.
- Reviewing KYC documentation.
- Reviewing transaction records.
- Reviewing gameplay history.
- Reviewing customer communications.
- Submitting representment documentation.
- Monitoring outcomes.

Chargeback trends are monitored regularly to ensure compliance with PSP and acquiring bank requirements.

9.9 PSP RECONCILIATION

Mirage Corporation N.V. performs regular reconciliation activities to ensure transaction accuracy and completeness.

Reconciliation activities include:

- Deposit verification.
- Withdrawal verification.
- Settlement verification.
- Fee verification.
- Review of cancelled transactions.
- Review of reversed transactions.
- Investigation of discrepancies.

Monthly reconciliation reports are provided to the Finance Department and retained for audit and regulatory review.



Dashboard
Orders
Shops
Reports
Staff
Balance

Transaction list

Search by transaction data

Transaction UID

Tracking ID

Payment description

Bank ID

Amount

Currency

RRN

Transaction type

Status

Recurring type

Payment method

Provider

Select a status

Select a recurring type

Select a payment method

Select a provider

Processor account number

Shop

Select a shop

Search by bank card data

Search by client data

Search by date

From

To

Date range on trx

Time zone

2025-10-30 00:00:00

2026-01-27 23:59:59

Creation date

(GMT+00:00) UTC

Search for a fraud operation

Find

Reset fields

Test transactions

Transaction	Date	Payment method	Customer	Shop	Description

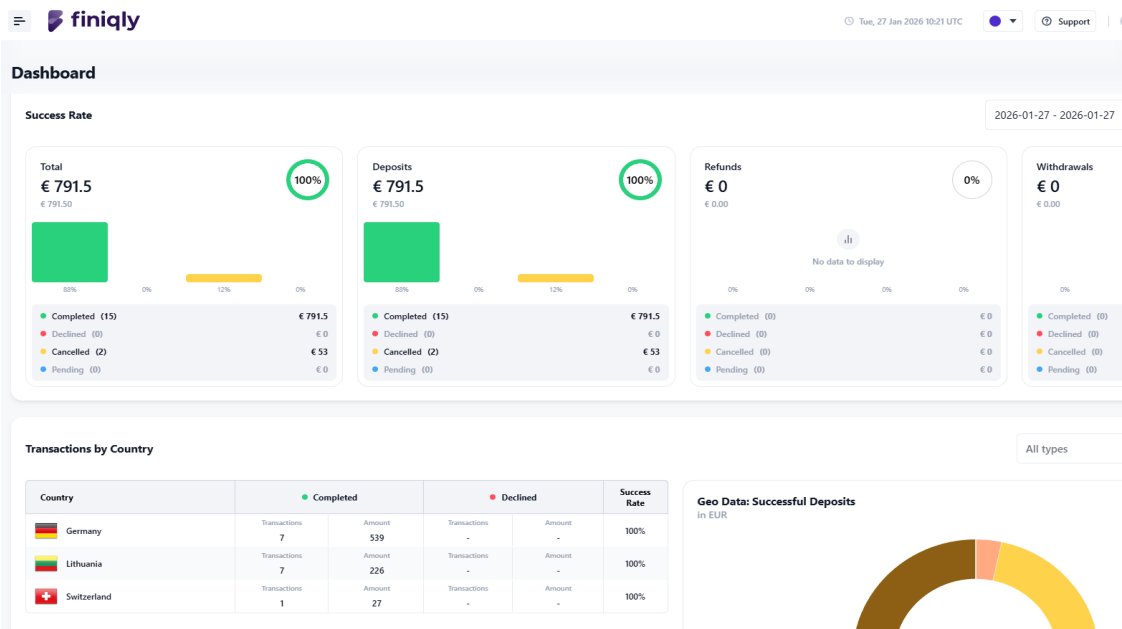
© 2019 - 2026 Paysage.io

The Payments Department maintains a data-driven approach to payment operations through operational dashboards, reporting tools, and business intelligence platforms.

- Deposit performance analysis.
- Withdrawal performance analysis.
- PSP approval and decline monitoring.
- Country performance reviews.

- Payment method performance reviews.
- Fraud trend analysis.
- Chargeback monitoring.
- Operational KPI tracking.

Management reviews operational reports periodically to identify trends, operational risks, and opportunities for process improvement.



9.11 KEY PERFORMANCE INDICATORS (KPIs)

The Payments Department monitors operational performance through established KPIs.

Withdrawal Processing

- 90% of withdrawals processed within 12 hours.
- 100% processed within 24 hours.

Transaction Performance

- PSP approval rates monitored daily.
- Significant reductions in approval rates investigated.
- Manual review rates monitored continuously.

Chargeback Management

- Chargeback ratios monitored by PSP and acquirer.
- Chargeback responses submitted within required deadlines.

Reconciliation Accuracy

- Reconciliation discrepancies investigated promptly.
- Settlement files reconciled within operational targets.

AML and Fraud Monitoring

- High-risk alerts reviewed within established timeframes.
- Financial crime escalations handled in accordance with AML procedures.

9.12 RECORD KEEPING

The Company shall maintain records relating to:

- Deposits.
- Withdrawals.
- Payment investigations.
- Chargebacks.
- Reconciliation activities.
- Fraud reviews.
- AML escalations.
- Source of Funds reviews.
- PSP communications.

Records shall be retained in accordance with applicable legal, regulatory, and operational requirements.

9.13 KEY CONTROLS

The Company's Payment Operations and Financial Controls Framework is supported by the following key operational controls

designed to ensure secure payment processing, regulatory compliance, financial integrity, and protection against fraud and financial crime.

Control Area	Key Control
Payment Governance	Payment operations are managed by the Payments Department under the supervision of the Head of Payments, with defined responsibilities, segregation of duties, and oversight by Senior Management.
Deposit Controls	All customer deposits are processed through approved Payment Service Providers (PSPs) and are subject to automated validation, transaction routing, and risk-based monitoring prior to acceptance.
Withdrawal Controls	Withdrawal requests are subject to identity verification, KYC status checks, payment method ownership validation, AML/CFT reviews, fraud screening, and manual approval where risk indicators are identified.
Transaction Monitoring	Customer payment activity is continuously monitored through automated and manual controls to identify unusual behaviour, fraud indicators, financial crime risks, and operational anomalies.
Fraud Prevention	Risk-based fraud detection measures, including velocity monitoring, device fingerprinting, IP analysis, BIN verification, country risk assessment, behavioural monitoring, and payment ownership checks, are applied throughout the payment lifecycle.
AML/CFT Escalation	Transactions presenting indicators of money laundering, terrorist financing, sanctions exposure, or

	other financial crime risks are promptly escalated to the Compliance Function and the Money Laundering Reporting Officer (MLRO) for investigation and further action where appropriate.
Chargeback Management	Chargebacks and payment disputes are investigated, documented, and managed in accordance with PSP requirements, card scheme rules, and internal procedures to minimise financial loss and operational risk.
Reconciliation and Financial Controls	Regular reconciliation of deposits, withdrawals, settlements, fees, reversals, and PSP balances is performed to ensure transaction accuracy, financial integrity, and timely identification of discrepancies.
Reporting and Performance Monitoring	Operational reporting, management information, and Key Performance Indicators (KPIs) are monitored to assess payment performance, fraud trends, PSP effectiveness, reconciliation accuracy, and compliance with operational service standards.
Record Keeping	Payment records, investigations, reconciliations, fraud reviews, AML escalations, PSP communications, and supporting documentation are securely maintained in accordance with applicable legal, regulatory, and operational requirements.

The effectiveness of these controls is reviewed periodically through operational monitoring, compliance oversight, internal audits, reconciliation activities, fraud trend analysis, regulatory developments, and management review to ensure that the Company's payment

operations remain secure, efficient, resilient, and aligned with applicable legal and regulatory obligations.

9.14 REVIEW AND CONTINUOUS IMPROVEMENT

The Payments Department shall periodically review its systems, procedures, controls, monitoring activities, and performance metrics to ensure ongoing effectiveness, operational efficiency, regulatory compliance, and protection against financial crime and fraud.

Findings arising from audits, fraud reviews, reconciliations, incidents, chargebacks, operational reporting, and regulatory developments shall be incorporated into the Company's continuous improvement programme.

INFORMATION SECURITY AND DATA PROTECTION



10



10. INFORMATION SECURITY AND DATA PROTECTION

10.1 PURPOSE

Mirage Corporation N.V. is committed to protecting the confidentiality, integrity, availability, and security of its information assets, systems, networks, and personal data.

The purpose of this chapter is to establish the framework through which the Company protects customer information, business data, technology infrastructure, and personal information while ensuring compliance with applicable legal, regulatory, and contractual obligations.

This framework supports the Company's obligations under data protection legislation, the General Data Protection Regulation (GDPR), Curaçao Gaming Authority requirements, and industry best practices.

10.2 INFORMATION SECURITY OBJECTIVES

The Company's Information Security and Data Protection Framework is designed to:

- Protect customer and company information from unauthorised access.
- Maintain the confidentiality, integrity, and availability of information assets.
- Protect personal data throughout its lifecycle.
- Prevent data breaches, cyber-attacks, and information security incidents.
- Ensure compliance with regulatory and legal requirements.
- Support secure gaming operations and payment processing.
- Promote security awareness across the organisation.
- Support business continuity and operational resilience.

10.3 GOVERNANCE AND RESPONSIBILITIES

Mirage Corporation N.V. maintains an Information Security and Data Protection Framework supported by management oversight, operational controls, and clearly defined responsibilities.

Board of Directors

The Board is ultimately responsible for ensuring that adequate information security and data protection controls are maintained throughout the organisation.

Senior Management

Senior Management is responsible for implementing and supporting the Information Security Framework and ensuring that sufficient resources are available to maintain appropriate security controls.

Data Protection Officer (DPO)

The Data Protection Officer oversees compliance with applicable data protection and privacy obligations.

The DPO's responsibilities include:

- Monitoring compliance with data protection requirements.
- Advising on privacy matters.
- Conducting Data Protection Impact Assessments (DPIAs).
- Managing data subject requests.
- Coordinating data breach responses.
- Acting as the primary contact for supervisory authorities.
- Supporting employee awareness and training.

Information Technology Function

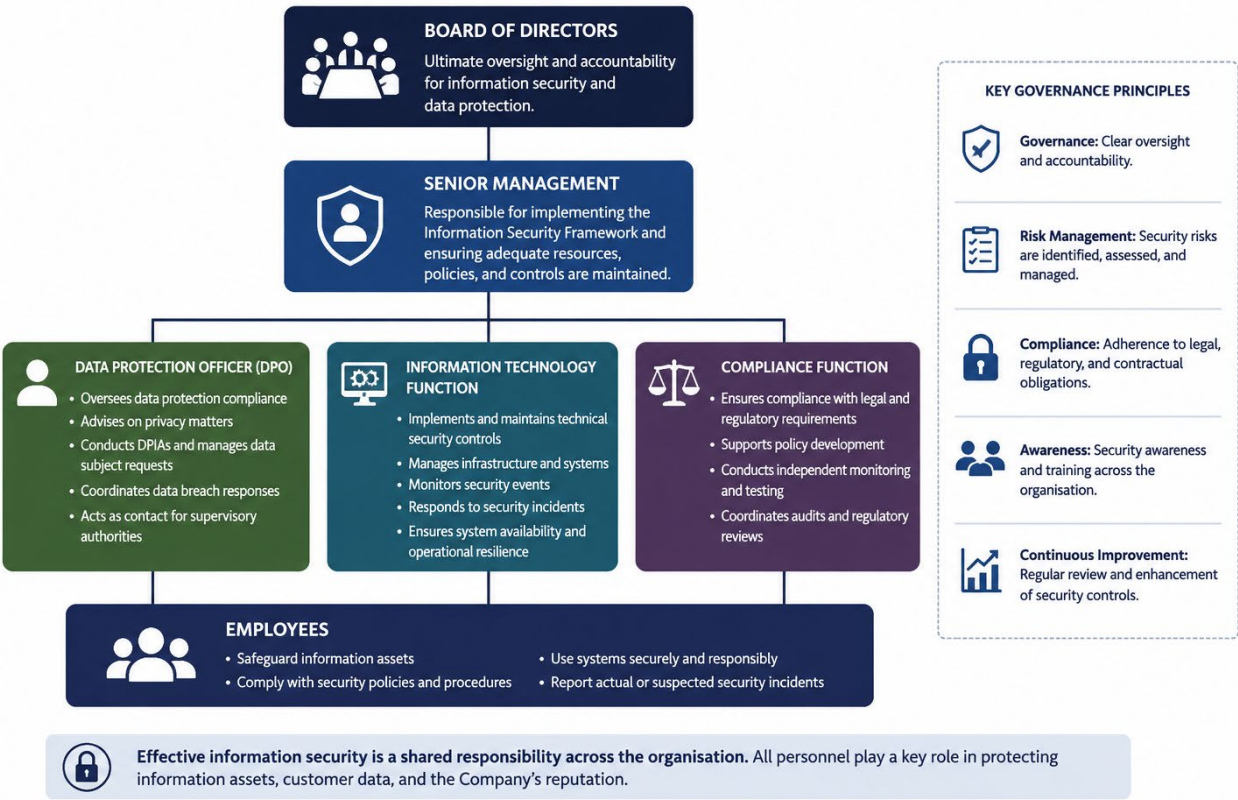
The Information Technology Function is responsible for implementing and maintaining technical security controls, monitoring system

security, managing infrastructure, and responding to information security incidents.

Employees

All employees are responsible for safeguarding information assets, complying with security requirements, and reporting actual or suspected security incidents.

Figure 10.1 – Information Security Governance Framework



10.4 INFORMATION SECURITY PRINCIPLES

Mirage Corporation N.V. adopts the following core security principles:

Confidentiality

Information shall only be accessible to authorised individuals with a legitimate business need.

Integrity

Information shall be protected against unauthorised modification, corruption, or destruction.

Availability

Systems, applications, and data shall remain available to authorised users when required for business operations.

Accountability

All users are accountable for activities performed under their assigned accounts and access privileges.

Compliance

Information shall be managed in accordance with legal, regulatory, contractual, and internal policy requirements.

10.5 DATA PROTECTION AND PRIVACY

Mirage Corporation N.V. processes personal data in a lawful, fair, transparent, and secure manner.

Personal data may include:

- Customer identification information.
- Contact details.
- Account information.
- Payment and transaction data.
- Gaming activity records.
- Responsible Gaming records.
- Customer communications.
- Employee information.
- Supplier and business partner information.

The Company shall process personal data only where a lawful basis exists and only for legitimate business purposes.

10.6 DATA CLASSIFICATION

Information assets shall be classified according to their sensitivity and business importance.

Data classifications may include:

Public

Information approved for public disclosure.

Internal

Information intended for internal business use.

Confidential

Sensitive business information requiring restricted access.

Restricted

Highly sensitive information requiring enhanced protection and strict access controls.

Data classification determines the applicable handling, storage, transmission, and retention requirements.

Figure 10.2 – Data Classification Model

	CLASSIFICATION LEVEL	DESCRIPTION	EXAMPLES OF DATA	HANDLING REQUIREMENTS	ACCESS
	RESTRICTED Highly sensitive information requiring enhanced protection and strict access controls.	Information where unauthorised access, disclosure, alteration or loss could cause severe damage to the Company, customers, or regulatory compliance.	- Customer identification documents - Payment card details - Account credentials - AML/KYC documents - Source of Funds information - Security keys and certificates - System configuration files	- Encrypted at rest and in transit - Access on a need-to-know basis - Strong authentication (MFA) required - Activity logging and monitoring - Secure storage and disposal	 Restricted access to authorised personnel only.
	CONFIDENTIAL Sensitive business information requiring restricted access.	Information that is important to the Company and could cause significant harm if accessed or disclosed inappropriately.	- Business strategies - Financial information - Customer data (non-payment) - Internal reports and analytics - Contracts and agreements - Employee personal data	- Access restricted to authorised roles - Stored in secure systems - Monitoring and audit trails - Shared only via approved channels	 Access limited to authorised employees and third parties.
	INTERNAL Information intended for internal business use.	Information that supports day-to-day operations and is not intended for public disclosure.	- Internal policies and procedures - Meeting minutes - Operational documentation - Training materials - Internal communications - Non-sensitive customer data	- Stored on internal systems - Access based on job role - Regular backup - Protect from unauthorised disclosure	 Access granted to employees based on role requirements.
	PUBLIC Information approved for public disclosure.	Information that is publicly available or intended for distribution to external parties.	- Website content - Press releases - Marketing materials - Public company information - General promotional content	- No special handling required - Reviewed and approved for release - Can be shared publicly	 Access available to anyone.



All information must be classified, handled, stored, transmitted, and disposed of in accordance with its classification level to ensure appropriate protection and compliance.



When in doubt, classify at the highest appropriate level.

10.7 ACCESS CONTROL

Access to systems, applications, networks, and data shall be controlled through documented access management procedures.

The Company applies Role-Based Access Control (RBAC) principles to ensure access rights are aligned with job responsibilities

Access control measures include:

- User account management.
- Role-based permissions.
- Multi-factor authentication (MFA).
- Password complexity requirements.
- Periodic access reviews.
- Access logging and monitoring.
- Privileged account management.

Access shall be granted according to the principle of least privilege and revoked promptly when no longer required.

Figure 10.3 – Access Control & Identity Management Workflow

Access is granted based on business need, monitored continuously, and revoked when no longer required.



10.8 PERSONAL DATA PROTECTION

Mirage Corporation N.V. implements technical and organisational measures to protect personal data.

Measures include:

- Access controls.
- Encryption.
- Data minimisation.
- Secure storage.
- Secure transmission.
- Monitoring and logging.

- Retention controls.
- Data disposal procedures.

Personal data shall only be accessed by authorised personnel for legitimate business purposes.

10.9 DATA SUBJECT RIGHTS

The Company recognises and supports the rights of individuals regarding their personal data.

Subject to applicable legal and regulatory requirements, individuals may exercise rights including:

- Right of access.
- Right to rectification.
- Right to erasure.
- Right to restriction of processing.
- Right to object.
- Right to data portability.
- Right to withdraw consent where applicable.

Players may submit data protection requests or enquiries by contacting the designated Data Protection Officer (DPO) directly via email or through the Company's Customer Support channels.

Upon receipt of a request, the DPO shall assess the nature of the request and verify the identity of the data subject before any personal data is disclosed, modified, restricted, or erased.

Identity verification shall normally be conducted through the email address registered on the customer's account. The data subject may also be required to answer security questions and provide additional information or documentation to enable the Company to reasonably verify their identity.

The DPO shall exercise discretion in determining the level of verification required based on the nature of the request, the sensitivity of the information involved, and the risk of unauthorised disclosure.

Once identity verification has been successfully completed, the DPO shall process and respond to the request in accordance with applicable legal and regulatory requirements and within the statutory timeframes prescribed by data protection legislation.

10.10 DATA RETENTION AND DISPOSAL

Mirage Corporation N.V. retains information only for as long as necessary to fulfil legal, regulatory, contractual, and operational requirements.

Retention periods are determined based on:

- Regulatory requirements.
- AML obligations.
- KYC obligations.
- Financial reporting requirements.
- Data protection obligations.
- Business needs.

Upon expiry of retention periods, information shall be securely deleted, anonymised, or destroyed using approved methods.

10.11 ENCRYPTION AND SECURE DATA STORAGE

Sensitive information and personal data shall be protected through encryption and secure storage controls.

Security measures include:

- Encryption of data in transit.
- Encryption of data at rest.
- Secure key management.
- Secure backup procedures.

- Segregated storage environments.
- Access restrictions for sensitive information.

The Company applies appropriate encryption standards to protect customer information, financial data, and business-critical information.

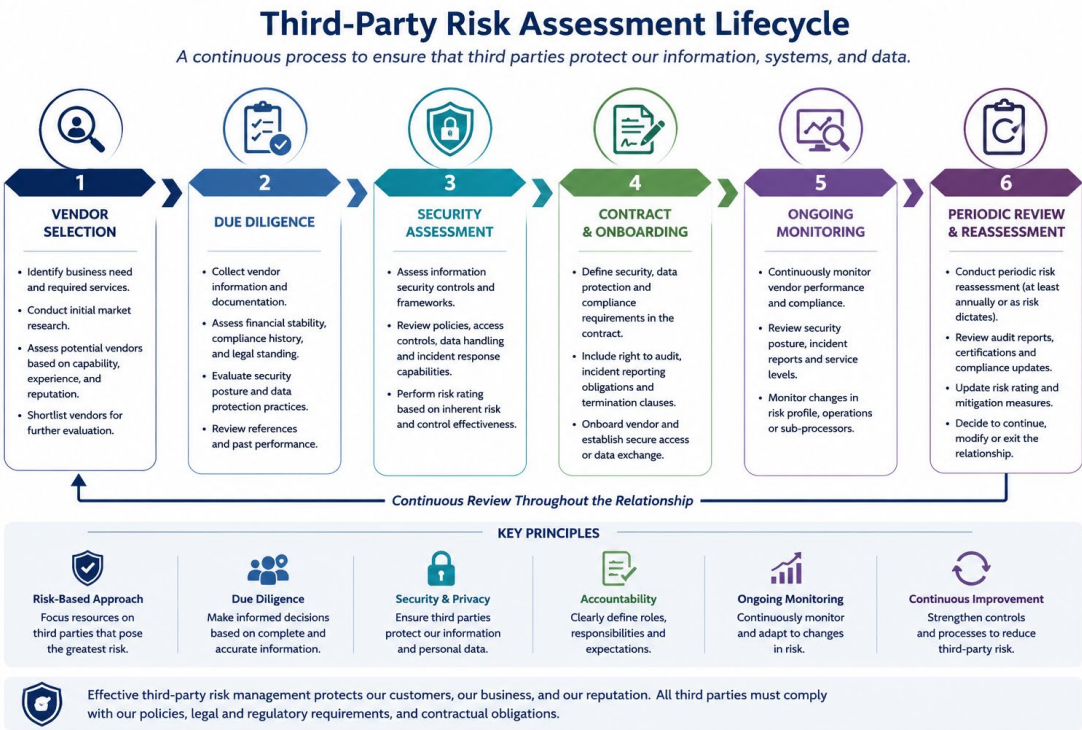
10.12 THIRD-PARTY AND VENDOR SECURITY

Third-party service providers with access to Company systems or customer data shall be subject to security and privacy assessments.

Third-party controls may include:

- Due diligence reviews.
- Security assessments.
- Data Processing Agreements.
- Contractual security obligations.
- Ongoing monitoring and review.

Third-party access shall be restricted to authorised activities and reviewed periodically.



10.13 SECURITY AWARENESS AND TRAINING

Mirage Corporation N.V. maintains a security awareness programme to ensure that employees understand their security and data protection responsibilities.

Training may include:

- Information security awareness.
- Data protection and privacy obligations.
- Password security.
- Social engineering awareness.
- Phishing awareness.
- Incident reporting procedures.
- Data handling requirements.

Training shall be provided during onboarding and periodically thereafter.

10.14 INFORMATION SECURITY INCIDENT MANAGEMENT

Employees must immediately report any actual or suspected information security incidents.

Examples include:

- Unauthorised access attempts.
- Malware infections.
- Data breaches.
- System compromise.
- Lost or stolen devices.
- Suspicious emails or phishing attempts.
- Accidental disclosure of confidential information.

Reported incidents shall be investigated, documented, and managed in accordance with the Company's Incident Response procedures.

Where required, regulatory authorities and affected individuals shall be notified in accordance with applicable legal obligations.

Figure 10.4 – Information Security Incident Response Process

A structured approach to detect, respond to, and recover from information security incidents.



10.15 COMPLIANCE MONITORING AND AUDIT

Mirage Corporation N.V. conducts periodic reviews and audits of information security and data protection controls.

Audit activities may include:

- Access reviews.
- Security assessments.
- Vulnerability reviews.
- Compliance testing.
- Data protection reviews.
- Third-party assessments.
- Incident reviews.

Findings shall be documented and corrective actions implemented where necessary.

10.16 KEY CONTROLS

The Company's Information Security and Data Protection Framework is supported by the following key operational controls designed to protect information assets, maintain the confidentiality, integrity, and availability of data, and ensure compliance with applicable legal and regulatory requirements.

Control Area	Key Control
Information Security Governance	Information security responsibilities are clearly defined and overseen by Senior Management, with security requirements integrated into the Company's governance and risk management framework.
Access Management	Role-based access controls, user authentication, periodic access reviews, and the principle of least privilege are implemented to prevent unauthorised access to systems and information.
Data Protection	Personal and confidential information is protected through data classification, secure storage, encryption, controlled access, and appropriate retention and disposal procedures.
Infrastructure and Network Security	Security measures, including firewalls, endpoint protection, secure configurations, vulnerability management, and system monitoring, are implemented to protect the Company's technology infrastructure.
Third-Party Security	Third-party service providers are subject to appropriate due diligence, contractual security

	requirements, and ongoing monitoring where they have access to Company systems or information.
Security Monitoring and Incident Management	Information security events are continuously monitored, investigated, and managed through established incident response procedures to minimise operational disruption and protect Company assets.
Employee Awareness	Employees receive mandatory information security and data protection training to promote awareness of cyber security risks, phishing threats, data handling responsibilities, and reporting obligations.
Record Keeping	Security logs, incident records, audit findings, access reviews, and related documentation are securely maintained in accordance with applicable legal, regulatory, and operational requirements.
Continuous Risk Assessment	Information security risks are assessed periodically to identify emerging threats, evaluate existing controls, and implement appropriate mitigation measures.
Continuous Improvement	Security controls, policies, and procedures are regularly reviewed and enhanced in response to audit findings, regulatory developments, technological advancements, and the evolving cyber threat landscape.

The effectiveness of these controls is reviewed periodically through security monitoring, internal assessments, compliance oversight, vulnerability testing, audit activities, and management review to ensure that the Company's Information Security and Data Protection Framework remains effective, resilient, and aligned with applicable legal, regulatory, and industry best practices.

10.17 CONTINUOUS IMPROVEMENT

The Information Security and Data Protection Framework shall be reviewed periodically to ensure ongoing effectiveness, regulatory compliance, and alignment with emerging threats, technological developments, and industry best practices.

Lessons learned from incidents, audits, risk assessments, regulatory developments, and operational reviews shall be incorporated into the Company's continuous improvement programme.

BUSINESS CONTINUITY IT AND INCIDENT MANAGEMENT



11



11. IT OPERATIONS, INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

11.1 PURPOSE

Mirage Corporation N.V. relies on secure, resilient, and continuously available technology systems to support gaming operations, customer services, payment processing, regulatory compliance, and business activities.

The purpose of this chapter is to establish the framework through which the Company manages IT operations, responds to incidents, maintains service availability, and ensures business continuity in the event of operational disruptions, security incidents, or system failures.

The framework is designed to minimise operational disruption, protect customers and business assets, and support compliance with regulatory requirements.

11.2 OBJECTIVES

The objectives of the IT Operations and Business Continuity Framework are to:

- Maintain stable and reliable technology services.
- Minimise disruption to customers and business operations.
- Ensure timely identification and resolution of incidents.
- Protect critical systems and information assets.
- Support operational resilience and recovery.
- Ensure effective communication during incidents.
- Meet regulatory and contractual obligations.
- Promote continuous improvement of operational processes.

11.3 GOVERNANCE AND RESPONSIBILITIES

Senior Management

Senior Management is responsible for ensuring that adequate resources, systems, and procedures are maintained to support business continuity and incident management activities.

Information Technology Function

The Information Technology Function is responsible for:

- Monitoring systems and infrastructure.
- Managing operational incidents.
- Maintaining technology platforms.
- Supporting service restoration activities.
- Maintaining business continuity procedures.
- Coordinating technical recovery activities.

Incident Response Team (IRT)

Mirage Corporation N.V. maintains an Incident Response Team (IRT) consisting of representatives from Information Technology, Compliance, Legal, and other relevant departments.

The Incident Response Team is responsible for:

- Incident assessment and classification.
- Escalation and communication.
- Incident containment.
- Recovery coordination.
- Regulatory notification support.
- Incident documentation.
- Post-incident review activities.

Operational Departments

Operational teams shall cooperate with incident response activities and provide support where incidents affect their respective functions.

11.4 IT OPERATIONS MANAGEMENT

Mirage Corporation N.V. maintains operational controls designed to support the ongoing availability, reliability, and performance of its technology infrastructure.

Operational activities include:

- Infrastructure monitoring.
- Application monitoring.
- Network monitoring.
- Capacity management.
- Performance monitoring.
- Vendor coordination.
- Change management.
- Patch management.
- Backup monitoring.

Technology systems are monitored continuously to identify operational issues, service degradation, security threats, and potential disruptions.

11.5 INCIDENT MANAGEMENT FRAMEWORK

All operational, technical, and security incidents shall be managed through a structured incident management process.

The incident management process includes:

1. Incident identification.
2. Incident reporting.
3. Incident classification.

4. Investigation and assessment.
5. Escalation where required.
6. Resolution and recovery.
7. Post-incident review.
8. Documentation and reporting.

All incidents shall be recorded and tracked through appropriate incident management procedures.

Figure 11.2 – Incident Management Lifecycle

A structured and continuous process to detect, respond to, and learn from incidents.



11.6 INCIDENT REPORTING

Employees are required to report any actual or suspected operational, technical, or security incident immediately upon discovery.

Examples of reportable incidents include:

- System outages.

- Application failures.
- Gameplay disruptions.
- Payment system failures.
- Cybersecurity incidents.
- Data breaches.
- Infrastructure failures.
- Third-party service disruptions.
- Network connectivity issues.

Incident reports shall be escalated to the Information Technology Function and Incident Response Team where appropriate.

11.7 INCIDENT CLASSIFICATION

Mirage Corporation N.V. classifies incidents according to operational impact and urgency.

Priority 1 – Critical Impact

Priority 1 incidents involve total or near-total service failure and have a significant impact on customers, gameplay, revenue generation, or business operations.

Examples include:

- Core platform outages.
- Aggregation API failures.
- Widespread game unavailability.
- Incorrect balance calculations.
- Jackpot system failures.
- Critical payment system outages.

Target Resolution Time:

- Resolution target: 2 hours.
- Status updates: Hourly.

Priority 2 – Significant Impact

Priority 2 incidents significantly affect customer experience or operational performance but do not result in a complete service outage.

Examples include:

- Major game availability issues.
- Bonus functionality failures.
- Session management issues.
- High-impact customer issues.
- Significant payment disruptions.

Target Resolution Time:

- Resolution target: 24 hours.
- Status updates: Every 4 hours.

Priority 3 – Low Impact

Priority 3 incidents affect individual users or non-critical functionality and have limited operational impact.

Examples include:

- Individual player issues.
- Isolated game launch failures.
- Game categorisation errors.
- Cosmetic display issues.
- Minor operational requests.

Target Resolution Time:

- Resolution target: 48 hours.
- Status updates: Daily.

Figure 11.3 – Incident Classification Matrix

Incidents are classified based on impact, urgency and business criticality to ensure appropriate response and escalation.

CRITERIA	 PRIORITY 1 CRITICAL IMPACT	 PRIORITY 2 SIGNIFICANT IMPACT	 PRIORITY 3 LOW IMPACT	 PRIORITY 4 INFORMATIONAL
 DEFINITION	Total or near-total service failure with critical impact on customers, revenue, or core business operations.	Significant impact on customer experience or operations but no complete service outage.	Limited impact affecting individual users or non-critical functionality with minimal operational impact.	Informational or routine requests with no operational impact.
 IMPACT ON BUSINESS	 Severe – Core services affected, major revenue or regulatory risk.	 High – Noticeable impact on customers or operations.	 Low – Minor impact, workarounds available.	 None – No impact on services or customers.
 EXAMPLES	- Core platform outages - Aggregation API failures - Widespread game unavailability - Incorrect balance calculations - Jackpot system failures - Critical payment system outages	- Major game availability issues - Bonus functionality failures - Session management issues - High-impact customer issues - Significant payment disruptions	- Individual player issues - Isolated game launch failures - Game categorisation errors - Cosmetic display issues - Minor operational requests	- General enquiries - Enhancement requests - Information requests - Routine data updates
 TARGET RESPONSE TIME (ACKNOWLEDGE)	 15 minutes	 1 hour	 4 hours	 1 business day
 TARGET RESOLUTION TIME	 2 hours	 24 hours	 48 hours	 5 business days
 ESCALATION PATH	 IRT Lead → Head of IT → Senior Management → Compliance / Legal (if required)	 IRT Lead → Head of IT → Relevant Department Head → Compliance (if required)	 Service Desk Lead → Relevant Team Lead → Head of IT (if required)	 Service Desk / Assigned Team

 Incident priority may be adjusted as new information becomes available. All incidents must be recorded, tracked and managed in accordance with the Incident Management Framework.

 **KEY FACTORS CONSIDERED:**

- Impact on customers
- Scope of outage
- Financial impact
- Business criticality
- Regulatory risk
- Security risk

 Timely classification and escalation ensure that the right resources are engaged quickly to minimise disruption, protect customers and assets, and maintain regulatory compliance.

11.8 INCIDENT RESPONSE PROCEDURES

Upon identification of an incident, the Incident Response Team shall:

- Assess the severity of the incident.
- Determine potential impact.
- Assign ownership and responsibilities.
- Implement containment measures.
- Coordinate resolution efforts.
- Monitor progress until closure.
- Communicate updates to relevant stakeholders.

Where external suppliers or service providers are involved, the relevant vendor shall be engaged immediately.

11.9 REGULATORY AND CUSTOMER COMMUNICATIONS

Where incidents affect customers, regulatory obligations, or critical operations, appropriate communication procedures shall be followed.

Communication activities may include:

- Internal management notifications.
- Customer communications.
- Supplier notifications.
- Regulatory notifications.
- Incident status updates.

Where required by law or regulation, the Company shall notify competent authorities and affected customers within applicable timeframes.

11.10 BUSINESS CONTINUITY PLANNING

Mirage Corporation N.V. maintains a Business Continuity Framework designed to ensure the continuation of critical business functions during disruptive events.

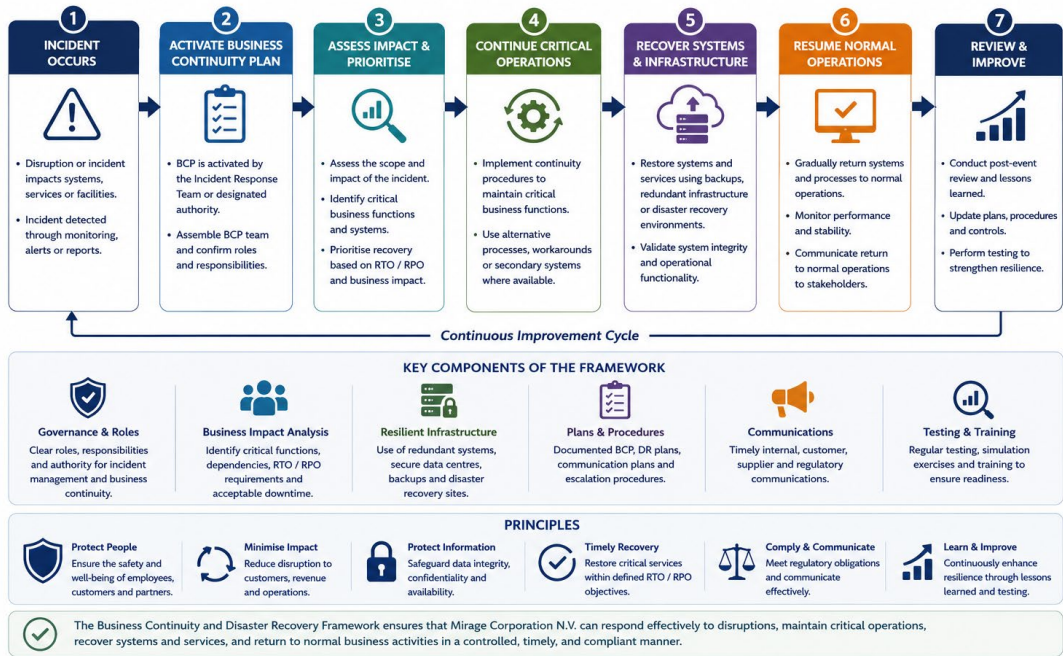
The Business Continuity Framework aims to:

- Minimise service disruption.
- Protect customers and assets.
- Maintain critical operations.
- Facilitate recovery of systems and services.
- Support regulatory compliance.
- Protect the Company's reputation.

Business continuity planning applies to technology systems, operational processes, third-party dependencies, personnel, and facilities.

Figure 11.4 – Business Continuity & Disaster Recovery Framework

A structured framework to ensure the continuation of critical operations and the timely recovery of systems and services.



11.11 CONTINUITY AND RECOVERY MEASURES

The Company maintains measures designed to support operational resilience and recovery.

Such measures may include:

- Redundant infrastructure.
- System backups.
- Disaster recovery procedures.
- Vendor contingency arrangements.
- Alternative communication channels.
- Incident escalation procedures.
- Recovery testing activities.

Critical systems shall be prioritised during recovery efforts to minimise customer impact and operational disruption.

11.12 POST-INCIDENT REVIEWS

Following resolution of significant incidents, Mirage Corporation N.V. shall conduct a post-incident review.

The review may include:

- Root cause analysis.
- Assessment of response effectiveness.
- Identification of control weaknesses.
- Evaluation of communication effectiveness.
- Review of recovery activities.
- Recommendations for improvement.

Findings shall be documented and tracked to completion.

11.13 RECORD KEEPING

The Company shall maintain records relating to:

- Incident reports.
- Incident investigations.
- Recovery activities.
- Root cause analyses.
- Business continuity testing.
- Vendor incidents.
- Regulatory notifications.
- Improvement plans.

Records shall be retained in accordance with applicable legal, regulatory, and operational requirements.

11.14 KEY CONTROLS

The Company's IT Operations, Incident Management and Business Continuity Framework is supported by the following key operational controls designed to maintain the availability, resilience, security, and continuity of critical technology services while minimising operational

disruption and ensuring compliance with applicable legal and regulatory requirements.

Control Area	Key Control
IT Governance	Information Technology operations are managed under a clearly defined governance structure with assigned responsibilities, management oversight, and documented operational procedures.
Infrastructure Monitoring	Critical infrastructure, applications, networks, databases, and supporting services are continuously monitored to identify performance degradation, system failures, security threats, and operational anomalies.
Incident Detection and Management	Operational, technical, and information security incidents are promptly identified, recorded, classified, investigated, and managed through the Company's Incident Management Framework.
Incident Escalation	Incidents are escalated to the Incident Response Team (IRT), Senior Management, Compliance, and other relevant stakeholders according to their severity, operational impact, and regulatory significance.
Business Continuity Planning	Business Continuity Plans are maintained to ensure the continued operation and timely recovery of critical business functions during disruptive events affecting technology,

	personnel, facilities, or third-party service providers.
Disaster Recovery	Backup procedures, redundant infrastructure, recovery plans, and disaster recovery testing support the restoration of critical systems and services within defined operational objectives.
Change and Vendor Management	System changes, software updates, infrastructure modifications, and critical third-party service providers are managed through documented approval, testing, monitoring, and review procedures to minimise operational risk.
Communication and Regulatory Reporting	Internal communications, customer notifications, supplier engagement, and regulatory reporting are coordinated in accordance with established incident response procedures and applicable legal and regulatory obligations.
Post-Incident Review	Significant incidents are subject to formal root cause analysis, lessons learned, and corrective action plans to strengthen operational resilience, improve response effectiveness, and reduce the likelihood of recurrence.
Record Keeping	Incident reports, investigations, recovery activities, business continuity testing, disaster recovery exercises, vendor incidents, regulatory notifications, and corrective action records are securely maintained in accordance

	with applicable legal, regulatory, and operational requirements.
--	--

The effectiveness of these controls is reviewed periodically through operational monitoring, incident simulations, business continuity testing, disaster recovery exercises, internal audits, management oversight, and continuous improvement initiatives to ensure that the Company's IT Operations, Incident Management and Business Continuity Framework remains effective, resilient, and aligned with applicable legal, regulatory, and industry best practices.

11.15 CONTINUOUS IMPROVEMENT

Mirage Corporation N.V. is committed to continuously improving its operational resilience, incident management capabilities, and business continuity arrangements.

Lessons learned from incidents, audits, testing activities, vendor reviews, customer feedback, and regulatory developments shall be incorporated into ongoing operational improvements.

Where service level targets are repeatedly missed, management shall implement corrective actions, improvement plans, and additional controls to restore expected performance levels.

CUSTOMER & TECHNICAL SUPPORT



12



CHAPTER 12 – CUSTOMER SUPPORT AND TECHNICAL SUPPORT OPERATIONS

12.1 PURPOSE

Mirage Corporation N.V. is committed to delivering efficient, professional, and customer-focused support services to customers, business partners, and internal stakeholders.

The purpose of this chapter is to establish the operational framework governing Customer Support and Technical Support activities, including issue resolution, escalation procedures, complaint handling, incident reporting, and service management.

The Company recognises that effective support operations are essential for maintaining customer satisfaction, operational stability, regulatory compliance, and business continuity.

12.2 SUPPORT FUNCTION STRUCTURE

The Support Function consists of two distinct operational teams:

CUSTOMER SUPPORT TEAM

The Customer Support Team serves as the primary point of contact for customers and is responsible for handling customer enquiries, account-related issues, technical assistance, and general support requests.

The team operates under the supervision of the Customer Support Team Lead and consists of approximately ten (10) support specialists operating on a 24/7 basis.

Customer Support operates as a critical operational function within Mirage Corporation N.V., acting as the first line of interaction between customers and the Company and serving as an intake point for complaints, Responsible Gaming requests, data protection enquiries, account-related concerns, and other regulated customer interactions.

The primary objective of the Customer Support Team is to provide timely, accurate, professional, and customer-focused assistance while ensuring that customer issues are resolved efficiently and in accordance with the Company's operational, regulatory, and compliance requirements.

The Customer Support Team is responsible for:

- Responding to customer enquiries across approved communication channels.
- Providing account-related assistance and general customer support.
- Assisting with payment-related enquiries and transaction status requests.
- Providing first-line troubleshooting for technical and gameplay-related issues.
- Identifying and escalating Responsible Gaming concerns.
- Receiving and escalating formal customer complaints.
- Receiving and routing data protection and privacy-related requests.
- Supporting AML, Compliance, Payments, and other operational departments through appropriate referrals and escalations.
- Maintaining accurate records of customer interactions and support activities.
- Monitoring customer issues through to resolution and closure.

The Customer Support Team contributes directly to customer satisfaction, customer retention, operational efficiency, and regulatory compliance. Performance is monitored through a combination of service quality metrics, response times, ticket resolution effectiveness, escalation management, complaint handling outcomes, and customer satisfaction indicators.

Key performance objectives include:

- Timely response to customer enquiries.
- Efficient resolution of customer issues at first point of contact where possible.
- Accurate classification and escalation of issues requiring specialist review.
- High levels of customer satisfaction and service quality.
- Effective handling of complaints and regulated customer requests.
- Consistent adherence to internal procedures and service standards.
- Continuous contribution to operational improvements and internal knowledge resources.
- Professional, accurate, and transparent communication with customers.

The Customer Support Team Lead is responsible for monitoring operational performance, ticket volumes, response times, escalation trends, complaint statistics, customer feedback, and quality assurance outcomes to identify opportunities for service improvement, staff development, and operational enhancement.

TECHNICAL SUPPORT TEAM

The Technical Support Team provides technical, operational, and integration support to business partners, service providers, and internal departments. The team plays a critical role in maintaining platform stability, supporting client integrations, coordinating technical investigations, and ensuring the efficient resolution of operational and system-related issues.

The team operates under the supervision of the Technical Support Team Lead and consists of two (2) specialists responsible for platform

integrations, technical troubleshooting, testing support, monitoring activities, and issue resolution.

The Technical Support Team does not communicate directly with players and primarily supports B2B clients, third-party providers, and internal stakeholders. Communication is conducted through approved business channels including email, Jira Service Desk, Microsoft Teams, Slack, and other operational communication platforms.

The primary objective of the Technical Support Team is to ensure the stable operation of the Company's technology environment while supporting client onboarding, technical integrations, product deployments, and incident resolution activities.

The Technical Support Team is responsible for:

- Supporting B2B client integrations and onboarding activities.
- Assisting with API configuration and technical setup requirements.
- Providing technical support to business partners and service providers.
- Investigating platform, game, payment, and integration-related issues.
- Monitoring operational systems and identifying service disruptions.
- Coordinating issue resolution with Development, Product, Payments, and external providers.
- Supporting testing, validation, and deployment of new features and configurations.
- Assisting with root cause investigations and technical incident analysis.
- Maintaining technical documentation and operational knowledge resources.
- Escalating issues requiring development or infrastructure intervention.

- Supporting internal departments with technical troubleshooting and operational requests.

The Technical Support Team serves as a key coordination point between business operations and technology functions, ensuring that technical issues are investigated, documented, prioritised, and resolved efficiently.

Performance is monitored through a combination of operational KPIs, service quality indicators, issue resolution effectiveness, testing accuracy, integration support performance, and stakeholder satisfaction measures.

Key performance objectives include:

- Accuracy and consistency of testing and validation activities.
- Efficient resolution of client and internal technical issues.
- Timely support of client onboarding and integration projects.
- Effective monitoring and escalation of operational incidents.
- High-quality technical documentation and knowledge sharing.
- Responsiveness and communication effectiveness during incidents.
- Ownership and accountability for assigned tasks and investigations.
- Continuous contribution to process improvements and operational stability.

The Technical Support Team Lead is responsible for monitoring workload distribution, ticket volumes, integration activities, incident trends, testing outcomes, and overall service performance to ensure operational effectiveness and continuous improvement.

12.3 CUSTOMER SUPPORT OPERATIONS

The Customer Support Team is responsible for ensuring a positive customer experience through timely, accurate, and professional assistance.

Primary responsibilities include:

- Customer enquiries.
- Account assistance.
- Gameplay enquiries.
- Bonus enquiries.
- Payment-related enquiries.
- Technical troubleshooting.
- Complaint intake.
- Escalation management.
- Responsible Gaming referrals.
- Compliance referrals.
- Fraud and AML referrals.

The Customer Support Team acts as the first point of contact for customers and seeks to resolve issues at the earliest possible stage.

12.4 CUSTOMER COMMUNICATION CHANNELS

Customers may contact the Company through approved support channels including:

- Live Chat.
- Email.
- Contact forms.
- Website support portals.

Customer interactions are recorded and retained within the Company's support management systems in accordance with record retention requirements.

12.4 CUSTOMER COMMUNICATION CHANNELS

Customers may contact the Company through approved support channels.

 LIVE CHAT Real-time assistance via the website or platform live chat function. USED FOR: ✓ Account assistance ✓ General enquiries ✓ Payment queries ✓ Technical issues ✓ Responsible Gaming support AVAILABLE: 24/7	 EMAIL Secure email communication for non-urgent or detailed support requests. USED FOR: ✓ Account & verification requests ✓ Payment & transaction issues ✓ Document submissions ✓ Complaints ✓ Data protection requests RESPONSE TARGET: Within 24 hours	 CONTACT FORMS Online forms available on the website for structured submissions. USED FOR: ✓ General enquiries ✓ Account registration issues ✓ Responsible Gaming requests ✓ Complaints ✓ Partnership or business enquiries AVAILABLE: 24/7 via Website	 WEBSITE SUPPORT PORTALS Self-service help centre and support portal for guides, FAQs and ticket submission. USED FOR: ✓ FAQs & guides ✓ Troubleshooting ✓ Submit support tickets ✓ Track ticket status ✓ Policy & document access AVAILABLE: 24/7 via Customer Portal
---	--	--	---

 RECORDING & RETENTION All customer interactions across the above channels are automatically recorded, tracked and retained within the Company's support management systems.	 CENTRALISED RECTENTING All communications are logged in a secure, centralised system for full traceability.	 DATA SECURITY Customer data is protected in accordance with applicable privacy and data protection requirements.	 RECORD RETENTION Records are retained in accordance with the Company's record retention policy and legal obligations.	 ACCESS CONTROL Access to customer records is restricted to authorised personnel on a strict need-to-know basis.
---	---	--	---	---



We are committed to providing accessible, reliable and secure communication channels to ensure excellent customer service and regulatory compliance.



12.5 SERVICE STANDARDS

Mirage Corporation N.V. aims to provide prompt and professional support services.

Service standards include:

Live Chat

- Initial response target of one (1) hour during operational periods.
- Immediate response where possible.

Email Support

- First response target within eight (8) hours.

Escalated Cases

- Managed according to priority and severity.

- Subject to internal escalation procedures.

Service performance is monitored through operational reporting and quality assurance activities.

12.6 CUSTOMER SUPPORT WORKFLOW

Step 1 – Issue Identification

All incoming enquiries are reviewed and categorised according to:

- Issue type.
- Severity.
- Operational impact.
- Regulatory implications.
- Resolution complexity.

Step 2 – First-Line Resolution

Customer Support personnel attempt to resolve issues using:

- Available knowledge bases.
- Standard Operating Procedures (SOPs).
- Internal guidance materials.
- Existing operational tools.

Step 3 – Escalation Assessment

Where an issue cannot be resolved at first contact, or where the matter falls within a predefined operational or regulatory process, Customer Support shall assess the appropriate escalation pathway.

Escalation may be required where:

- Specialist knowledge or intervention is required.
- Technical investigation is necessary.
- The matter relates to payment processing or transaction reviews.

- A formal player complaint has been submitted.
- A data protection request has been received.
- Responsible Gaming concerns have been identified.
- AML or financial crime concerns have been identified.
- Legal or regulatory review is required.
- The issue affects multiple customers or critical business operations.

Customer Support shall ensure that all escalated matters are documented appropriately and transferred to the relevant department, officer, or process owner for investigation and resolution.

Step 4 – Escalation

Escalated cases shall be formally documented and transferred to the appropriate department, function, or designated officer for investigation and resolution. Prior to escalation, Customer Support shall ensure that all relevant information has been collected and recorded, including customer details, account information, transaction references, communication history, supporting evidence, and a summary of the issue. Depending on the nature of the matter, cases may be escalated to the Payments Department, Compliance Function, AML Function, Responsible Gaming Officer, Technical Support Team, Product Department, Development Teams, Legal Department, Data Protection Officer, or other appropriate stakeholders.

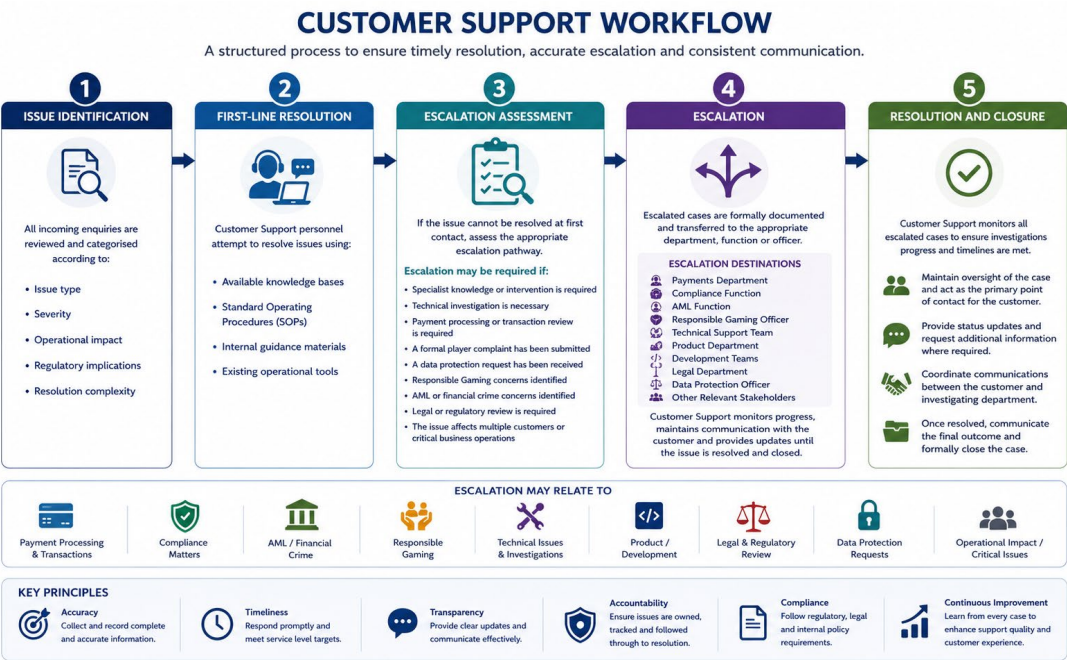
Upon escalation, the receiving department shall assume responsibility for investigating and resolving the matter. Customer Support shall remain responsible for monitoring the progress of the case, maintaining communication with the customer, and providing updates where appropriate until the issue has been resolved and formally closed. All escalation activities, actions taken, findings, and final

outcomes shall be documented and retained in accordance with the Company's record-keeping requirements.

Step 5 – Resolution and Closure

Customer Support shall monitor the progress of all escalated cases to ensure that investigations are progressing appropriately and that agreed service levels and response timelines are maintained. The team shall maintain oversight of the case throughout its lifecycle and act as the primary point of contact for the customer unless responsibility for communications has been formally transferred to another department.

Where appropriate, Customer Support shall provide customers with status updates regarding the progress of their case and any additional information requests. Customer Support shall continue to coordinate communications between the customer and the investigating department until the matter has been resolved, a final outcome has been communicated, and the case has been formally closed.



12.7 ESCALATION FRAMEWORK

Issues may be escalated where:

- Specialist knowledge is required.
- Technical investigation is necessary.
- Compliance review is required.
- Responsible Gaming intervention is required.
- AML review is required.
- Payment review is required.
- Legal review is required.

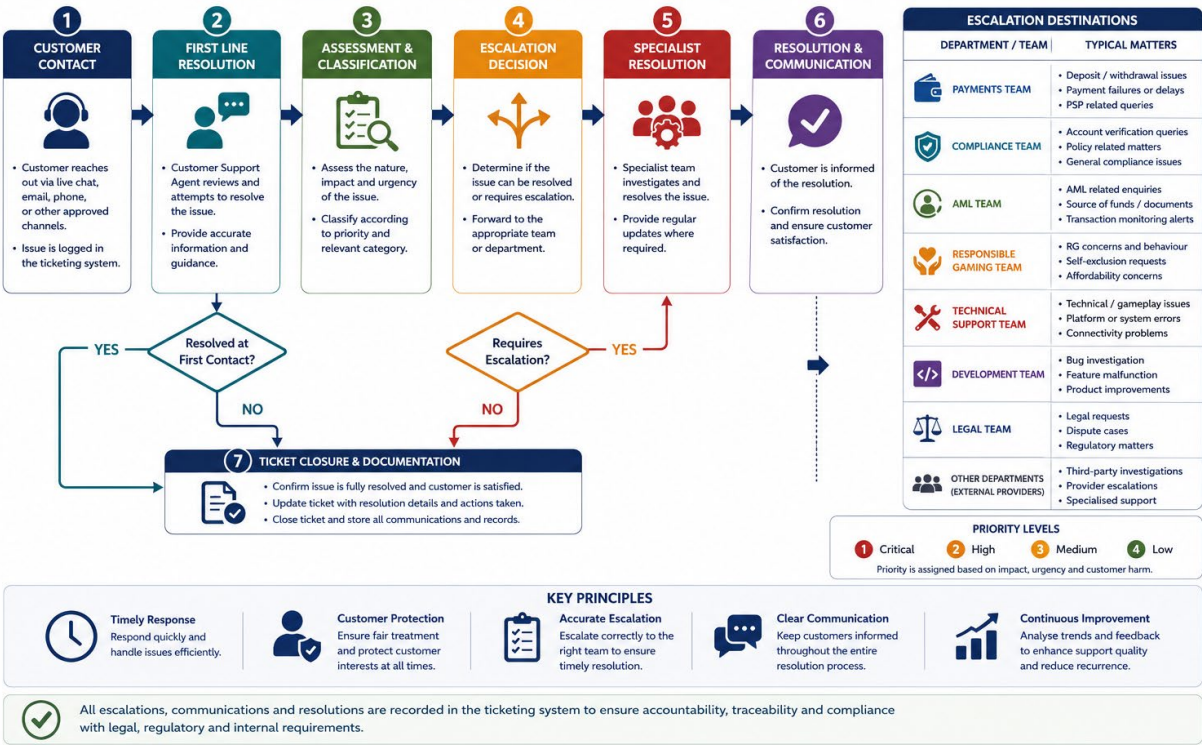
Escalations may be directed to:

- Payments Department.
- Compliance Department.
- AML Function.
- Responsible Gaming Officer.
- Technical Support Team.
- Product Department.
- Development Teams.
- Legal Department.
- External providers.

All escalations shall be documented within the Company's ticketing systems.

Figure 12.1 – Customer Support Escalation Framework

A structured escalation process to ensure timely resolution, regulatory compliance and customer protection.



12.8 COMPLAINT HANDLING

Customer Support serves as the first point of contact for customer complaints and is responsible for identifying, documenting, and escalating complaints in accordance with the Company's Complaints and Alternative Dispute Resolution (ADR) Framework.

Where a customer expresses dissatisfaction regarding a product, service, decision, transaction, account action, or any aspect of the Company's operations, Customer Support shall make reasonable efforts to understand the concern and seek an appropriate resolution through normal support channels. Where the matter cannot be resolved immediately, or where the customer requests a formal review, the issue shall enter the formal complaints process.

COMPLAINT HANDLING PROCESS

Step 1 – Receipt of Complaint

Customer Support shall receive the complaint through an approved communication channel, such as email, live chat, contact form, or support ticket. The complaint shall be reviewed to determine whether it constitutes a formal complaint or a general customer enquiry.

Step 2 – Complaint Registration

Where the matter meets the definition of a complaint, Customer Support shall record the complaint and collect all relevant information, including customer details, account information, transaction references, supporting documentation, and previous communications relating to the matter.

Complaints should be submitted by the customer within six (6) months of the incident or event giving rise to the complaint.

Step 3 – Acknowledgement of Complaint

Customer Support shall ensure that receipt of the complaint is acknowledged within seven (7) calendar days.

The acknowledgement shall include:

- Confirmation that the complaint has been received.
- Information regarding the complaint handling process.
- Expected investigation and resolution timelines.
- Any additional information required from the customer.

Step 4 – Initial Assessment and Escalation

Customer Support shall assess the nature of the complaint and determine the appropriate escalation path. The complaint shall be assigned to the appropriate department or designated complaint owner for investigation.

Depending on the nature of the complaint, matters may be referred to the Payments Department, Compliance Function, AML Function, Responsible Gaming Officer, Technical Support Team, Data Protection Officer, Legal Department, or other relevant stakeholders.

Step 5 – Investigation and Customer Communication

The investigating department shall review the complaint and gather all relevant information required to reach a determination.

Customer Support shall remain responsible for monitoring the progress of the complaint, maintaining communication with the customer, and providing updates where appropriate throughout the investigation process.

Step 6 – Resolution

Mirage Corporation N.V. aims to resolve complaints within four (4) weeks of receipt.

Where a complaint is particularly complex and additional investigation is required, the Company may extend the investigation period by up to an additional four (4) weeks. In such cases, the customer shall be informed of the reasons for the delay and provided with an updated estimated resolution date.

Responsible Gaming complaints shall receive priority handling and should normally be resolved within five (5) business days and no later than two (2) weeks from receipt.

Step 7 – Outcome and Closure

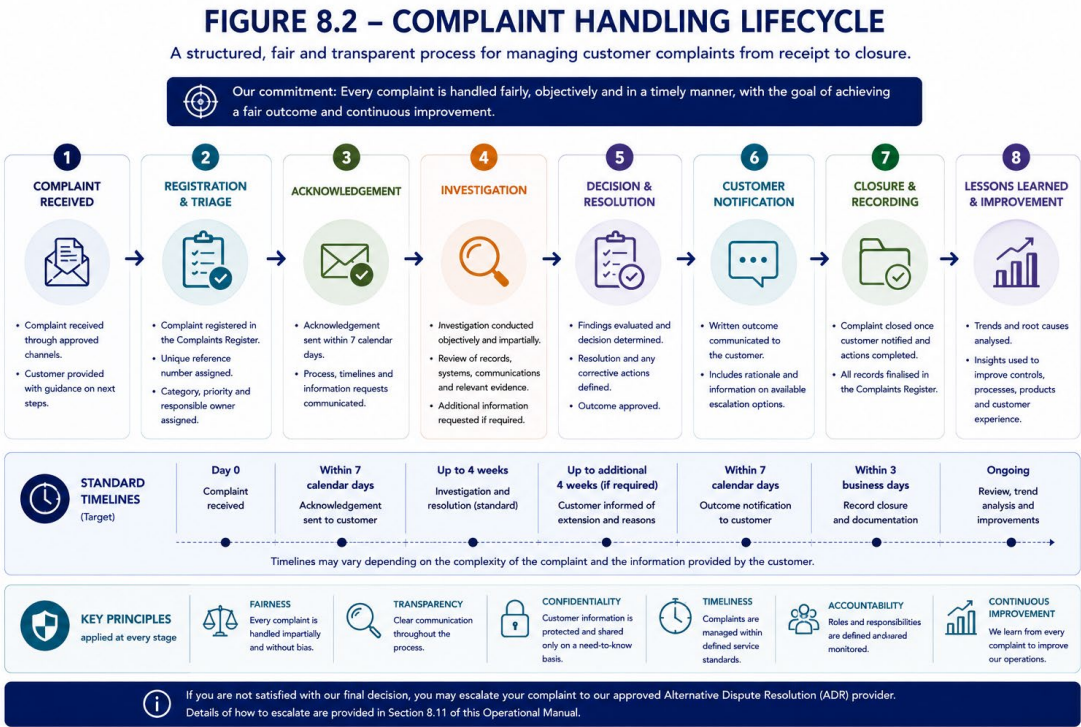
Once the investigation has been completed, the outcome shall be communicated to the customer in writing. Customer Support shall ensure that the complaint record is updated, all relevant documentation is retained, and the matter is formally closed.

Where a customer remains dissatisfied following the Company's final response, information regarding the Alternative Dispute Resolution (ADR) process shall be provided in accordance with the Company's Complaints and ADR Framework.

Customer Support responsibilities include:

- Receiving and identifying customer complaints.
- Recording complaints within the appropriate systems and registers.
- Collecting relevant information and supporting documentation.
- Acknowledging complaints within required timeframes.
- Providing customers with information regarding the complaints process.
- Escalating formal complaints to the appropriate department or complaint owner.
- Monitoring complaint progress and maintaining communication with the customer.
- Supporting complaint investigations by providing records, communications, and operational information where required.
- Assisting with ADR referrals where applicable.

Formal complaint investigations, determinations, and ADR referrals remain subject to the Company's Complaints and ADR Framework as described in Chapter 8.



12.9 Responsible Gaming And Compliance Escalations

Customer Support personnel play a key role in the Company's Responsible Gaming Framework by acting as the first line of interaction with customers. Through regular customer contact, support personnel may identify behavioural indicators suggesting that a customer is experiencing gambling-related harm or may require additional support or intervention.

To ensure concerns are identified promptly and managed consistently, all Customer Support personnel receive initial and ongoing Responsible Gaming training. Training programmes are designed to enable employees to recognise behavioural indicators of gambling-related harm, respond appropriately to customer interactions, and escalate concerns in accordance with the Company's Responsible Gaming Policy and internal procedures.

Where customer interactions indicate potential Responsible Gaming concerns, Customer Support personnel shall escalate the matter to the Responsible Gaming Officer without undue delay.

Responsible Gaming indicators may include, but are not limited to:

- Expressions of financial hardship or difficulty paying essential living expenses.
- Statements suggesting gambling is being used as a means of earning income rather than for entertainment.
- Repeated requests for bonuses, free bets, or promotional credits following significant losses.
- Evidence of frequent or unusually large deposits that may indicate attempts to recover previous losses ("chasing losses").
- Signs of distress, agitation, frustration, desperation, or aggressive behaviour during live chat, email, or other customer communications.
- Customers expressing that they are unable to stop gambling or feel they have lost control over their gambling behaviour.
- Repeated requests to reverse withdrawals or cancel withdrawal requests without a legitimate operational reason.
- Customers spending prolonged periods gambling without appropriate breaks or displaying patterns of continuous play where such information is available.
- Any other behavioural indicators that reasonably suggest the customer may be experiencing gambling-related harm.

Customer Support personnel are not expected to diagnose gambling-related harm or make clinical assessments. Their responsibility is to identify potential warning signs, document relevant observations, and

escalate concerns to the Responsible Gaming Officer for further review and, where appropriate, intervention.

Similarly, where customer interactions identify potential compliance, fraud, money laundering, terrorist financing, sanctions, or other regulatory concerns, the matter shall be escalated promptly to the appropriate Compliance Function or Money Laundering Reporting Officer (MLRO) in accordance with the Company's AML/CFT and Compliance Frameworks.

All Responsible Gaming and Compliance escalations shall be documented within the Company's customer support and case management systems, together with the actions taken, referrals made, and any subsequent outcomes, in accordance with the Company's record-keeping requirements.

12.10 OPERATIONAL SYSTEMS AND TOOLS

Customer Support and Technical Support utilise a range of operational systems and collaboration tools.

These include:

- Jira.
- Microsoft Teams.
- Slack.
- Internal Back Office.
- Confluence.
- Microsoft Office.
- DbVisualizer.
- Zabbix.
- Grafana.
- ExpressVPN.
- Internal monitoring platforms.

These systems support:

- Ticket management.
- Customer communication.
- Escalation management.
- Technical investigations.
- Operational reporting.
- Internal collaboration.
- System monitoring.

Jira

Log in to continue

Email *

Enter your email

Manage Passwords

Continue

Or continue with:

Google

Microsoft

Apple

Slack

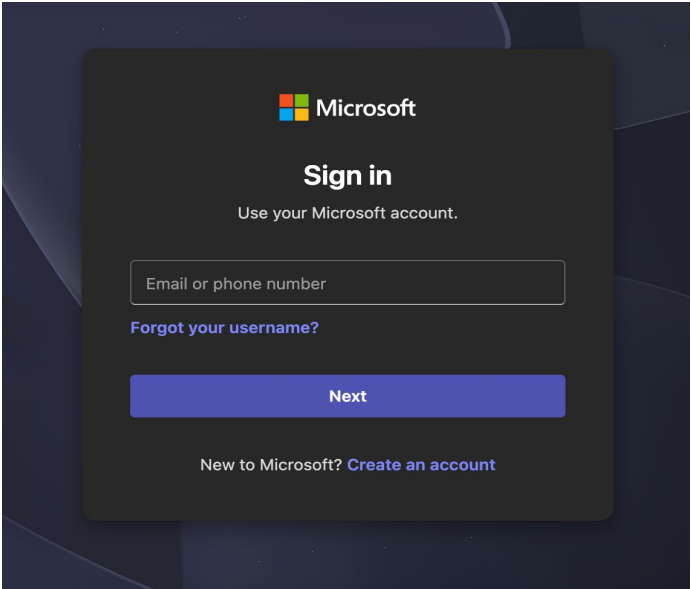
[Can't log in?](#) • [Create an account](#)

ATLASSIAN

One account for Jira, Confluence, Trello and [more](#)

[Privacy Policy](#) • [User Notice](#)

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.



Back Office:

Player: rokiy... 01 (N/A)

Set as handled

Switch to player

Go

DASHBOARD

EDIT PROFILE

PLAYER MANAGEMENT

NOTES

GAME REPORT

BONUSES

USB

SPLAYERS

AUDIT LOG

HISTORY

EVENTS

IP HISTORY

FRAUD

OPEN ROUNDS

DEVICE MANAGEMENT

TOP GAMES

MANAGE TAGS

PLAYER JOURNEY

LOYALTY

Agent

Email

Email self-excluded

Status

KYC verification status

Member since

Balance

Vip level

Player notes

Player interventions / complaints

Total deposits

Total withdrawals

Number of deposits

Deposits

No deposits

Withdrawals Pending

No pending withdrawals

Withdrawals

No withdrawals

Bonus currently not active

Last 5 player free spins

Created	Games	Bet level	Valid From - To	Received	Activated	Win	Used / Available	Completed
No Data Available								

Last 5 player feature buys

Created	Games	Bet level	Valid From - To	Received	Activated	Win	Used / Available	Completed
No Data Available								

Fund Transfer / Bonus Activation

Free Rounds

12.11 TECHNICAL SUPPORT OPERATIONS

The Technical Support Team provides technical support to B2B clients and internal departments.

Primary responsibilities include:

- Integration support.
- API configuration support.
- Technical troubleshooting.
- Platform issue investigation.
- Testing support.
- Monitoring and diagnostics.
- Provider issue coordination.
- Internal technical assistance.

The Technical Support Team works closely with Development, Product, Payments, and external providers to resolve technical issues.

12.12 TECHNICAL INCIDENT MANAGEMENT

Technical Support is responsible for investigating and coordinating resolution of:

- Integration failures.
- Provider connectivity issues.
- API issues.
- Configuration issues.
- Technical defects.
- Performance issues.
- Monitoring alerts.

Where development intervention is required, incidents are escalated through Jira and tracked until resolution.

Communication with B2B clients occurs through:

- Email.
- Microsoft Teams.
- Slack.
- Jira Service Desk.

12.13 KNOWLEDGE MANAGEMENT

The Support Function maintains internal documentation and operational knowledge repositories to support efficient issue resolution.

Documentation may include:

- Standard Operating Procedures.
- Product Guides.
- Troubleshooting Guides.
- Incident Reports.
- Escalation Procedures.
- Regulatory Guidance.

Knowledge repositories are reviewed and updated periodically.

12.14 PERFORMANCE MONITORING AND KPIS

Support performance is monitored through operational metrics and service quality indicators.

Customer Support KPIs may include:

- First response times.
- Resolution times.
- Ticket volumes.
- Escalation rates.
- Customer satisfaction scores.
- Complaint volumes.

Technical Support KPIs may include:

- Resolution efficiency.
- Testing accuracy.
- Integration support effectiveness.
- Ticket closure rates.
- Internal stakeholder satisfaction.

12.15 RECORD KEEPING

The Company maintains records relating to:

- Customer enquiries.
- Support tickets.
- Technical incidents.
- Escalations.
- Complaint referrals.
- Customer communications.
- Resolution records.

Records are retained in accordance with applicable legal, regulatory, and operational requirements.

12.16 KEY CONTROLS

The Customer Support and Technical Support Framework is supported by the following operational controls designed to ensure efficient customer service, timely issue resolution, regulatory compliance, and continuous operational improvement.

Control Area	Key Control
Governance	Customer Support and Technical Support operate under clearly defined responsibilities, reporting lines, and management oversight.
Customer Communication	Customer enquiries are managed through approved communication channels using documented procedures and service standards.
Ticket Management	All customer enquiries, incidents, complaints, and technical issues are recorded, categorised, prioritised, and tracked until formal resolution and closure.
Escalation Procedures	Matters requiring specialist review are escalated to the appropriate operational department, including Payments, Compliance, AML, Responsible Gaming, Technical Support, Development, Legal, or external providers.
Complaint Handling	Formal complaints are managed in accordance with the Company's Customer Complaints and Dispute Resolution Framework to ensure fair, timely, and transparent resolution.
Responsible Gaming & Compliance	Customer Support personnel identify potential Responsible Gaming concerns, AML indicators, fraud risks, and compliance matters and escalate them in accordance with established procedures.

Technical Support	Technical issues, integrations, platform incidents, and provider connectivity problems are investigated, documented, monitored, and resolved through structured incident management processes.
Knowledge Management	Standard Operating Procedures, troubleshooting guides, technical documentation, and operational knowledge bases are maintained and reviewed to support consistent service delivery.
Performance Monitoring	Operational performance is measured through defined KPIs, service quality reviews, ticket analytics, customer satisfaction indicators, and management reporting.
Record Keeping	Support tickets, customer communications, complaints, technical investigations, escalation records, and resolution outcomes are securely maintained in accordance with legal, regulatory, and operational requirements.

The effectiveness of these controls is reviewed periodically through quality assurance activities, performance reporting, management oversight, customer feedback, operational audits, and continuous improvement initiatives to ensure that Customer Support and Technical Support operations remain effective, customer-focused, and aligned with applicable legal, regulatory, and operational requirements.

12.17 CONTINUOUS IMPROVEMENT

The Customer Support and Technical Support functions shall periodically review operational performance, service quality,

escalation trends, customer feedback, incident data, and complaint outcomes.

Lessons learned shall be incorporated into updated procedures, training programmes, and operational improvements to enhance customer experience and operational effectiveness.

OPERATIONAL MANUAL **GOVERNANCE** **AND REVIEW**



13



13. DOCUMENT CONTROL AND VERSION MANAGEMENT

13.1 PURPOSE

This Operational Manual is a controlled document maintained by Mirage Corporation N.V. to support the effective governance, operation, and compliance of its online gaming activities.

The purpose of this chapter is to establish the framework governing the creation, approval, distribution, review, amendment, and retention of this Manual to ensure that it remains accurate, current, and aligned with the Company's operational practices and applicable legal and regulatory requirements.

Document control supports effective governance, accountability, regulatory compliance, and the consistent application of operational procedures throughout the organisation.

13.2 SCOPE

This chapter applies to this Operational Manual and any future revisions issued by Mirage Corporation N.V.

It governs:

- Document creation and approval.
- Version control.
- Document review and amendment.
- Distribution and accessibility.
- Record retention.
- Document ownership.
- Change management.

13.3 DOCUMENT OWNERSHIP

Overall responsibility for this Operational Manual rests with Senior Management.

The Compliance Function shall coordinate the review and maintenance of the Manual and ensure that updates are implemented where required.

Department Heads are responsible for ensuring that procedures relating to their respective operational areas remain accurate and are reviewed periodically.

All employees are responsible for complying with the procedures described within this Manual and for reporting any inaccuracies or operational changes requiring document updates.

13.4 VERSION CONTROL

Each version of this Manual shall contain appropriate document control information, including:

- Version number.
- Date.
- Description of amendments.
- Version amendment author

Only the most recent approved version shall be regarded as the official operational manual.

Superseded versions shall be archived and retained in accordance with the Company's document retention procedures.

13.5 REVIEW AND APPROVAL PROCESS

This Manual shall be reviewed periodically and whenever significant operational or regulatory changes occur.

Reviews may be initiated following:

- Regulatory or legislative changes.
- Internal audits.
- External audits.
- Compliance monitoring.
- Risk assessments.
- Operational incidents.
- Business process changes.
- Introduction of new products or services.
- Recommendations arising from management reviews.

Any amendments shall be reviewed by the relevant department owners before submission to Senior Management for approval.

13.6 DISTRIBUTION AND ACCESSIBILITY

The current approved version of this Manual shall be made available to relevant personnel through the Company's approved document management systems.

Access shall be restricted according to business need and information security requirements.

Employees shall be informed of material updates affecting their responsibilities and, where appropriate, receive additional guidance or training.

13.7 CHANGE MANAGEMENT

All proposed amendments shall be documented and assessed to determine their operational, legal, regulatory, and compliance impact.

Changes shall be implemented through the Company's governance and approval processes to ensure that procedures remain consistent across all operational departments.

Where significant amendments are introduced, related policies, procedures, training materials, and operational documentation shall be updated accordingly.

13.8 RECORD RETENTION

Current and historical versions of this Manual shall be retained securely in accordance with the Company's document retention requirements.

Document records shall include:

- Previous versions.
- Approval records.
- Change history.
- Review dates.
- Supporting documentation where applicable.

Archived versions shall remain accessible for audit, regulatory inspection, and historical reference.

13.9 KEY CONTROLS

The Company's Document Control and Version Management Framework is supported by the following key controls to ensure the integrity, accuracy, and effective governance of controlled documentation.

Control Area	Key Control
Document Ownership	A designated document owner is responsible for maintaining the Manual and coordinating periodic reviews.
Version Control	All revisions are assigned a unique version number, approval date, effective date, and change description.
Review Process	The Manual is reviewed periodically and following significant operational, regulatory, or organisational changes.
Approval	Amendments require review by relevant department owners and formal approval by Senior Management prior to implementation.
Distribution	Only the latest approved version is distributed and made available to authorised personnel.
Change Management	Proposed amendments are documented, assessed, approved, and implemented through controlled governance procedures.
Record Retention	Current and archived versions, approval records, and change histories are securely maintained in accordance with record retention requirements.
Continuous Compliance	Document reviews incorporate regulatory developments, audit findings, operational improvements, and lessons learned to ensure ongoing compliance and effectiveness.

The effectiveness of these controls is reviewed periodically through compliance oversight, internal audits, management review, and document governance activities to ensure that this Operational Manual remains accurate, controlled, and aligned with the Company's operational and regulatory obligations.

13.10 CONTINUOUS IMPROVEMENT

Mirage Corporation N.V. is committed to maintaining this Operational Manual as a living document that evolves alongside the Company's business activities, regulatory obligations, and operational environment.

Feedback from employees, audit findings, regulatory inspections, operational incidents, customer outcomes, and business improvements shall be considered during periodic reviews to ensure that the Manual continues to reflect current practices and supports the Company's commitment to effective governance, operational excellence, and regulatory compliance.

DOCUMENT VERSION CONTROL

Version	Date	Author	Purpose
1.0	20/11/2025	Mirage Corporation N.V - Compliance	Compilation of this document
1.0	22/06/2026	Mirage Corporation N.V - Compliance	Revision

CONCLUSION

This Operational Manual establishes the governance, operational frameworks, internal controls, and procedures through which Mirage Corporation N.V. conducts its online gaming activities in a secure, responsible, and compliant manner.

The Manual reflects the Company's commitment to maintaining the highest standards of operational integrity, regulatory compliance, customer protection, information security, financial crime prevention, and responsible gaming. It provides a structured framework for the management of key operational functions, including corporate governance, risk management, compliance, anti-money laundering and counter-terrorist financing, customer due diligence, payment operations, information security, business continuity, customer support, and technical operations.

Mirage Corporation N.V. recognises that effective governance extends beyond documented procedures. It requires a culture of accountability, transparency, continuous learning, and collaboration across all areas of the organisation. Accordingly, all employees, officers, and service providers are expected to understand and fulfil their respective responsibilities while operating in accordance with applicable laws, regulatory requirements, internal policies, and recognised industry standards.

The Company remains committed to protecting its customers by promoting responsible gaming, safeguarding customer funds and personal information, preventing financial crime, and maintaining fair, transparent, and secure gaming operations. Robust internal controls, ongoing monitoring, regular training, and independent oversight form an integral part of the Company's operational framework and support the effective management of emerging risks.

Mirage Corporation N.V. acknowledges that the regulatory and technological landscape continues to evolve. For this reason, this Operational Manual shall remain a living document, subject to periodic review and amendment to reflect regulatory developments, operational enhancements, technological advancements, audit findings, lessons learned, and evolving industry best practices.

Through the implementation of the policies, procedures, and controls described within this Manual, Mirage Corporation N.V. aims to maintain a resilient, customer-focused, and well-governed operation that supports sustainable business growth while meeting its obligations to customers, business partners, employees, regulators, and other stakeholders.

Senior Management is responsible for ensuring that this Operational Manual remains effective, current, and consistently applied throughout the organisation. All personnel are expected to comply with its provisions and to contribute actively to the continuous improvement of the Company's governance, operational resilience, and regulatory compliance framework.

This Operational Manual shall be read in conjunction with the Company's supporting policies, procedures, and operational documentation and shall serve as the principal reference document governing the day-to-day operation of Mirage Corporation N.V.'s licensed online gaming activities.

END OF DOCUMENT

Mirage Corporation Operational Manual

Version 1.0

2025