

Risk Management Policy & Framework

The information contained in this document is highly sensitive and is protected by laws and regulations. Unauthorised disclosure or use of this information may result in legal action and other consequences. Employees are expected to maintain the confidentiality of this document and use the information only for legitimate business purposes within the scope of their duties.

Document information

Subject	Risk Management Policy & Framework
Purpose	The Risk Management Policy & Framework ("Policy") provides guidance to the company to be able to identify, assess, and manage its risks to minimize their impact on achieving strategic objectives and ensure the company's resilience and stability.
Involvements	- All departments across the Company are responsible for understanding and managing their risks - The Policy and Framework is managed by the Legal and Compliance function in partnership with the Board of Directors.
Responsibility	Legal and Compliance
Approval	Board of Directors
Review	Normally on an annual basis or earlier as needed
Classification	Confidential

Version history

Date	Version	Summary of changes
July 2024	V1.00	Creation and rollout -

Table of Contents

1. Introduction	4
2. Risk Management Principles	4
3. Three Lines of Defence (3LOD)	5
4. Risk Management Process	6
5. Roles and Responsibilities	9
6. Risk Categories/Taxonomy	10
7. Risk Register	10
8. Training and Awareness	11
9. Monitoring and review	11
10. Appendix	12

1. Introduction

1.1 The purpose of this policy is to create the Risk Management framework and help foster the risk culture of the Company. This policy will outline how the Company will identify, assess, manage and mitigate risks.

1.2 Liquid Entertainment N.V. (hereinafter “Company”) is a company duly incorporated under the laws of Curacao under the register number 153298 with its registered address Zuikertuintjeweg z/n (Zuikertuin Tower), Willemstad, Curaçao. It provides consumer-facing entertainment and gaming products with support of digital, the Company holds a gaming licence issued by the government of Curacao and operates the online casino www.duelbits.com under the licence GLH-OCCHKTW076092020.

1.3 This Policy applies to all employees (whether temporary, fixed-term, or permanent), officers, trustees, board members, consultants, contractors, trainees, seconded staff, remote workers, casual workers, agency staff, volunteers, interns, agents, sponsors, or any other person or persons (collectively the “Representatives”) associated with the Company.

1.4 This policy applies to all teams and departments within the Company and its subsidiaries.

2. Risk Management Principles

2.1 Roles and Responsibilities

The Company operates in a highly regulated industry where risk plays a major role in every aspect of the business. Having an effective and appropriate Risk Management Framework where risks and the controls that mitigate them are documented and regularly monitored is crucial.

A company that is managing its risk effectively is where everyone is aware of the key risks within their department, report their incidents

Whilst risk is a part of every person's role at the Company, the Compliance and Risk Management department's role is to

- create the risk framework
- document the risks across the company
- maintain the risk register
- document and rate the controls
- Assist the teams and departments with managing ongoing remediation items to ensure any gaps in our controls are improved.

The teams and departments across the Company are responsible for mitigating their risks, recording incidents and improving their controls where gaps are identified. Senior Management in each department

are responsible for reporting on their risks and key incidents at the Risk, Audit and Compliance Committee on a quarterly basis.

2.2 Risk Appetite and Tolerance

The risk appetite and risk tolerances of the Company are set and agreed by the Board of Directors. The Risk Appetite Statement is shared across the business and helps to inform all risk based decisions. Any decision or act of the company that falls outside of the agreed risk appetite would be considered a breach of the Risk Framework and may attract disciplinary action.

An incident that occurs outside of the risk appetite is a signal that there are gaps in our control framework and therefore further investigation is required.

2.3 Risk Culture

As a part of a highly regulated industry, a strong and thriving risk culture is one where employees at all levels are encouraged and empowered to identify, assess, and manage risks proactively and transparently. It involves a clear understanding that risk management is everyone's responsibility, with open communication channels for reporting concerns without fear of retribution.

Leadership sets the tone by prioritizing risk management in decision-making, supporting robust processes, and providing the necessary resources for risk identification and mitigation. Additionally, a good risk culture emphasizes learning from past experiences, continuously improving risk management practices, and aligning risk-taking with the company's values and strategic goals.

3. Three Lines of Defence (3LOD)

Duelbits employs the Three Lines of Defence (3LOD) model as the basis of its Risk Management Framework. The Three Lines of Defence model is a way for organizations to clearly identify roles and responsibilities across the Company. The model is in use across the financial sector as well as other gaming operations.

3.1 3LOD Explained (Source: KPMG)

First Line of Defence

The first line of defence consists of the business owners, whose role is to identify risk, as well as execute actions to manage and treat it.

Second Line of Defence

The second line is comprised of the standard setters or risk oversight groups (e.g., compliance functions, legal and enterprise risk management) which are responsible for establishing policies and procedures and serving as the management oversight over the first line (the doers).

Third Line of Defence

The third line is composed of independent assurance providers. These groups report independently to the board or the audit committee and include functions such as internal audit, external auditors, a Chief Risk Officer and special/ad hoc committees.

3.2 3LOD at Duelbits

Risk Governance		
Assurance Providers Internal Audit	3rd Line of Defence	Roles and Responsibilities • Liaise with senior management or board • Rationalize and systematize risk assessment and governance reporting • Provide oversight on risk-management content/processes are adequate and appropriate
Standard Setters Compliance Risk Legal	2nd Line of Defence	Roles and Responsibilities • Establish policy and process for risk management • Strategic link for the enterprise in terms of risk • Provide guidance and coordination among all constituencies • Identify enterprise trends, synergies, and opportunities for change • Initiate change, integration, operationalization of new events • Liaison between third line of defence and first line of defence • Oversight over certain risk areas (e.g AML/CFT) and in terms of certain enterprise objectives (e.g., compliance with regulation)
The Doers Team Leaders Team Members	1st Line of Defence	Roles and Responsibilities • Manage risks/implement actions to manage and treat risk • Comply with risk-management process • Implement risk-management processes where applicable • Execute risk assessments and identify emerging risk

4. Risk Management Process

4.1 Risk Profiling

Risk Identification & Risk Rating

At Duelbits, risk identification is completed via the Risk Profiling process. This process involves the key members of each department identifying all operational risks that may occur within their function. A risk can be easily defined as something that can go wrong or can have a negative impact on the Company's objectives. It can be something that has the potential for loss, harm, or other adverse effects due to uncertain events or conditions. Once identified, each risk is **assigned** an "Inherent Risk" based on the Risk Rating Matrix (please refer to Appendix 1).

Control Identification & Control Rating

Once all risks have been identified and assigned an inherent risk, the controls currently in place are required to be identified. A control can be defined as a measure or action implemented to prevent, detect, mitigate, or correct risks that could negatively impact an organization's objectives.

Controls are designed to manage and reduce the likelihood or impact of risks, ensuring that the organization operates within its risk tolerance levels. They can be policies, procedures, practices, or physical safeguards and are an integral part of a broader risk management framework.

A control can be rated as either “Strong”, “Satisfactory”, “Needs Improvement” or “Unsatisfactory”. For example, a “Strong” control is usually automated and with continuous monitoring enabled, there are no incidents, issues, remediation plan or breach related to the control over a quarter or more. A control can be rated as “Unsatisfactory” if there are known issues or gaps with the control or there have been serious incidents or breaches that show the control as not working or not effective.

Residual Risk

Following the control rating process a “Residual Risk” is assigned to each risk. Generally, If a control is rated as “Strong” or “Satisfactory”, the Residual Risk will reduce as the control will mitigate the risk and reduce the likelihood and impact of the risk occurring.

If the residual risk remains outside of the agreed company risk appetite then a remedial action is required to strengthen the control and reduce the likelihood of and impact of the risk should an incident occur.

4.2 Business Risk Assessment

Once the risk profiling process has been completed, all profiles are maintained within the Business Risk Assessment document which is presented to and approved by Senior Management. The Business Risk Assessment document will be reviewed on a regular basis, especially following new incidents or material changes

4.3 Technology Risk Assessment

Duelbits’ risk management team plays a critical role in partnership with the technology team in guiding the process to ensure that new apps, services or technological solutions are evaluated thoroughly for potential risks and opportunities. The risk management team will perform the following tasks before new technology is brought in:

Identify Emerging Risks: Assess new and evolving technologies to identify potential risks associated with their implementation, including security vulnerabilities, compliance issues, and integration challenges.

Evaluate Risk Impact and Likelihood: Analyze the potential impact of identified risks on the organization’s operations, data, and strategic objectives, as well as the likelihood of these risks occurring.

Develop Mitigation Strategies: Create and implement strategies to manage or mitigate identified risks, such as developing robust security protocols, establishing contingency plans, and ensuring compliance with relevant regulations.

Ensure Alignment with Business Objectives: Ensure that risk management strategies are aligned with the organization's overall business objectives and technological goals, balancing risk with potential benefits.

Facilitate Informed Decision-Making: Provide insights and recommendations to support decision-making processes, helping stakeholders understand the risk implications of technological investments and innovations.

Monitor and Review: Continuously monitor the risks associated with technological developments and review risk management practices to adapt to new threats and changes in technology.

4.4 Remediation Plans

Any control that is determined as “Weak” or “Needs Improvement” requires a remediation plan to be put in place to resolve any issues identified by the risk owner. The remediation plan needs to have a due date, and directly address the control weakness and agreed to by the risk owner. Depending on the severity or likelihood of the risk occurring the due date may need to

4.5 Control Testing

On a periodic basis, the Risk Management function will test the effectiveness of a selection of “Key Controls”, especially those where high risk incidents have occurred in the previous 6-12 months.

In the context of risk management, a control is a measure or action implemented to prevent, detect, mitigate, or correct risks that could negatively impact an organization's objectives. Controls are designed to manage and reduce the likelihood or impact of risks, ensuring that the organization operates within its risk tolerance levels. They can be policies, procedures, practices, or physical safeguards and are an integral part of a broader risk management framework.

A risk is the possibility of something happening that could have a negative impact on an organization's objectives. It represents the potential for loss, harm, or other adverse effects due to uncertain events or conditions.

Control testing involves evaluating the effectiveness of an organization's controls to ensure they are properly designed and functioning as intended to manage and mitigate risks. The process typically includes the following steps:

Planning and Scoping: Identify the specific controls to be tested based on the risks they address and the objectives they support. Define the scope, objectives, and criteria for testing.

Test Design: Develop testing procedures and determine the methods to be used, such as walkthroughs, inspection, observation, or re-performance. Select the appropriate sample size for testing.

Execution: Perform the tests according to the designed procedures. This may involve reviewing documents, observing processes, interviewing personnel, and re-performing control activities.

Documentation: Record the results of the tests, noting whether the controls are operating effectively or if there are any deficiencies or exceptions.

Evaluation and Analysis: Analyze the test results to assess the overall effectiveness of the controls. Determine if any weaknesses or gaps need to be addressed.

Reporting: Summarize the findings in a report, highlighting any issues and providing recommendations for improvement. Communicate the results to relevant stakeholders.

Follow-up: Monitor the implementation of corrective actions and re-test controls if necessary to ensure deficiencies are resolved.

The results of the control testing will be shared with senior management via the Risk, Audit and Compliance Committee.

5. Roles and Responsibilities

Role	Responsibility
Board of Directors	Oversight and approval of risk management framework including the Risk Appetite Statement
Executive Management	Implementation and enforcement of the policy.
Risk Management Committee	Coordination and guidance on risk-related activities.
Risk Owners	Identification and management/mitigation of specific risks.
All Employees	Adherence to risk management procedures and reporting of risks and incidents.

6. Risk Categories/Taxonomy

Every risk must meet a certain category and must be defined within the risk register.

Risk Category	Description
---------------	-------------

Strategic Risks	Risks affecting the achievement of strategic goals such as competition, regulatory changes, economic downturn, potential M&A and expansion
Operational Risks	Risks arising from day-to-day operations, e.g technology failures, health and safety incidents, natural disasters, serious fraud/theft, talent risks e.g. challenges in recruiting, retaining or managing skilled employees.
Financial Risks	Risks related to financial loss, liquidity or instability, market risk or increases in operational costs, taxation or
Compliance Risks	Risks of legal or regulatory non-compliance, data privacy violations, AML violations, employment law breaches, bribery and corruption, licence risks.
Reputational Risks	Risks affecting the organization's reputation, e.g. significant data breaches, executive misconduct, negative media coverage or social media missteps.

7. Risk Register

Once the risk profiling process has been completed, all risks that have been identified are to be recorded in a central risk register.

The risk register should capture all relevant risk information, for example:

- Risk Title and Description
- Risk Category
- Risk Owner
- Department
- Inherent Risk Rating
- Consolidated Control Rating
- Residual Risk Rating
- Recent Incident Details

The risk register is to be maintained by the Risk Management team and made available to senior management at any time. The risk register should be reviewed monthly for accuracy and relevance and if any material incident occurs that may impact a risk or control effectiveness rating.

8. Training and Awareness

8.1 Risk Management Training Programs

All members of staff are required to complete some form of training on Risk Management and the Company framework depending on their type of role.

For example, operational team members may require general training on Risk Management theories and how to identify and log a risk incident. More senior members of the team, from team leaders to senior management would require training on how to monitor risks within the team, maintain and improve the controls in use in the team to mitigate risks and how to resolve incidents.

8.2 Awareness Campaigns

From time to time, the Learning and Development team, in consultation with the Risk Management team will create company wide awareness campaigns to uplift the understanding and importance of risk. Company wide emails, Slack messages and or “Lunch and Learn” events can assist the function to improve the risk culture across the company.

9. Monitoring and review

The Company’s Risk Management policy and procedures are subject to regular external and internal audits to ensure that they are effective in practice.

The employees or Representatives of the Company are responsible for the success of this Policy. They are invited to comment on this Policy and suggest ways in which it might be improved. Comments, suggestions, and queries should be addressed to the Legal and Compliance Team.

The Policy will be reviewed and approved by the Board on an annual basis at minimum, or in case significant changes are done at a level which warrants a Board approval.

Any amendment of the Policy shall, as soon as is reasonably practicable, be distributed or informed to employees or Representatives within the scope of the Policy for information of the amendment.

Appendix 1:

Example of Business Risk Assessment:

Risk Summary (1/8)

1. Operational Risk		Inherent Rating ^a				Residual Rating ^b		
#	AML/TF Type Behaviour	Likelihood	Impact	Rating	Consolidated Controls	Likelihood	Impact	Rating
1	Non-KYC Customers An account may be opened using false information or by someone other than the registered individual for the purpose of carrying out ML/TF activity.	(5) Almost Certain	(4) Major	Critical	Satisfactory	(3) Possible	(4) Major	High
2	Unidentified PEPs and HIOs Accounts being funded by the proceeds of crime by individuals who have a high political profile or have held public office (past or present).	(5) Almost Certain	(4) Major	Critical	Satisfactory	(3) Possible	(4) Major	High
3	Potential ML/TF depositing and betting activity Funds deposited into betting accounts are from an illicit source, whether the proceeds of crime or for the purpose of financing terrorism.	(5) Almost Certain	(4) Major	Critical	Satisfactory	(3) Possible	(4) Major	High
4	Drastic changes in betting behaviour May indicate that the account is now being used, by the customer or by someone on whose behalf the customer is acting, for money laundering purposes.	(4) Likely	(4) Major	High	Satisfactory	(2) Unlikely	(4) Major	Moderate