CODEGO Risk Management Policy

1.Table of Contents

2.Risk Management

Risk is the potential of gaining or losing something of value. Risk is an event or condition that if it occurs, could have a positive (an opportunity) or negative (a threat) effect on Codego Ltd (“Codego”) (also referred to as “the Company”) objectives.

Risks can be conditionally divided into two types. These are internal and external risks.

Internal risk is the risk arising from the events taking place within the organisation. External risk is outside the control of the Company.

External risks are generally more difficult to predict and control. Factors such as a key partner going bankrupt, economic cataclysm, war, crime, and other events may directly impact the business effectiveness.

The Company sees the risk management process not as a layer of bureaucracy, but rather as a systematic approach to identifying and defining what can go wrong, why and what can be done about it. Risk management is about reducing the impact of risk to an acceptable level.

Risk management is the process of identifying, assessing, responding to, monitoring, and reporting risks. The Company’s Risk Management Plan defines how risks associated with the Company business will be identified, analysed and managed. To manage the risks the Company will perform the qualitative risk analysis. Risk event may be defined as:

Risk Event = Probability x Impact,

where probability is the chance the event may occur, and impact is the effect of that event, if it occurs. The Company will use this Risk Matrix (Figure 1 below) in regular risk assessments.

Impact	1	2	3	4	5
Probability	Negligible	Minor	Moderate	Significant	Severe
(81-100) %	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80) %	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60) %	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40) %	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20) %	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Figure 1: Risk Matrix

A scale of 1-100% will be used for Probability:

- (1-20)% means very low;
- (21-40)% means low;
- (41-60)% means medium;
- (61-80)% means high;
- (81-100)% means it is a fact.

There are number of possible risk management models. The Company model uses a six-step approach. The general process and steps involved in the Company risk management processes are represented in Figure 2 below.

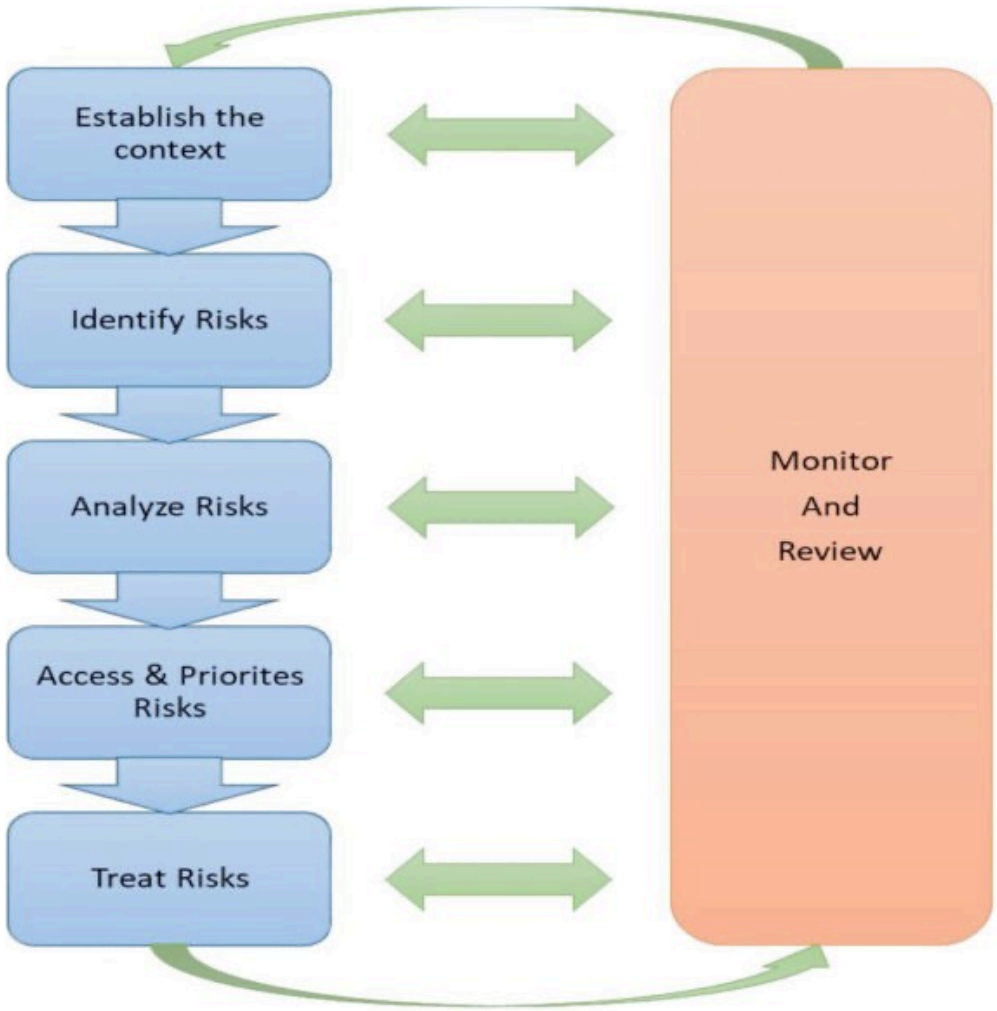

Figure 2: Risk management process

The Company chooses to strike a balance between actively managing the risk by investing in suitable resource and infrastructure, and accepting/transferring the risk by buying a suitable insurance policy. The company is considering having a comprehensive insurance policy covering for its businesses continuity and for issues including: employee theft, fraud and property loss.

2.1. The Company identifies the following low risks

Currency risk is managed by monitoring its daily foreign currency and liquidity risk. Credit risk of the company is limited to the carrying amount of its financial assets exposure. The Company is exposed to interest rate risk by managing cash flows and availing debt.

2.2. The Company identifies the following moderate risks

- Settlement risk
- Counterparty risk
- Liquidity risk
- Market risk

2.2.1. Settlement Risk

Settlement risk is defined as the probability of loss arising from the failure of one counterparty to settle its end of the deal, thus preventing other counterparties from settling their commitments. It arises usually when payments are not exchanged simultaneously.

Examples of settlement risk are advance settlement or cross currency settlement risk: the probability of loss in settlement of foreign exchange contracts arises when a counterparty pays out one currency before receiving a payment of the other, delayed settlement due to time zones. Cross-currency settlement risk that arises where the working hours of inter-bank fund transfer systems do not overlap due to time zone differences.

In this situation, failure by counter-party to settle its side of the deal starts a chain reaction of cross-defaults, this failure causes a string of cascading defaults in a rapid sequence. To limit our exposure to the settlement risk inherent with payment systems, we will establish a profile that does not expose us to non-payment by the providing party. Our business will monitor all transactions on a 6-point system – the check list is as follows:

1. When a transaction is received in the payment system, the transaction is held for review for cleared funds into the client account.
2. Underlying transactions, if any, are identified and checks made to validate the information to ensure correct data has been received.
3. There is verification of cleared funds credited to the client account via online banking with a bank.
4. On receipt of cleared funds, the recipient payment instruction is processed and the onward payment is released.
5. Settlement failure at final stage of a transaction – the Company maintains various relationships that provide the ability to reschedule through alternative methods or providers available.
6. Bank payment system provides live feed information on status against value date monitoring for settlement completion.

2.2.2.Counterparty Risk

This means the probability of loss arising due to the failure of the transmitting party to settle their end of the process: this can occur early within the transaction cycle or prior to the forward date of a settlement agreement.

Counterparty risk is sometimes the hardest to manage against – this is due to the high potential that a transmitting party is unlikely to declare inability to settle. Part of the management of this risk is done as part of the settlement risk process. In addition to this, we use a structured process of credit profiling.

Credit profiling follows three key steps:

1. All new/first time transmitting parties are capped at a low value trading limit – this ensures that over-exposure cannot occur. Prompt settlement is then required.

2. Transaction activity and ongoing monitoring of volumes, settlement speed and credit check monitoring to alert us to changes in financial stability of the transmitting party.

3. Unusual transaction patterns, unexpected increases/decreases in order value that are not market specific and other transmitters are not showing the same patterns emerging.

2.2.3.Liquidity Risk

Identifying and measuring liquidity risk: Board of Directors of the Company meet quarterly to review liquidity ratio and ensure that the Company is within the limits. The Company must be capable to meet all obligations to customers at any time and, therefore, the active management of its liquidity position is critical. Failure to remain within policy limits will trigger specific action to access secondary sources of liquidity, raise capital, etc.

Monitor and control liquidity risk: the Company intends to monitor its liquidity though frequent monitoring of its transactions and using appropriate financial projection tools.

2.2.4.Market Risk

Market risk encompasses the risk of movements in market prices and results in unexpected losses as the value on settlement post booking could change in a way that cannot be effectively anticipated and guarded against.

To limit this risk, it will be our policy to evaluate whether changes in products, activities, clients or market conditions necessitate activities for adjustment, redevelopment or replacement. Should settlement risk or counterparty risk occur, in consequence of correct positioning within the market, our risk is limited.

Using market trends and historical information, we are able to project an anticipated demand but at the same time, we use negative data allowing unforeseen scenarios. Additional resources used for the provision of up to date market information within management operational environment are Reuters, Bloomberg, BBC Worldwide News and others.

2.3.The Company identifies the following high risks

- Operational and security risk
- Financial crime risk

These risks are specific to the nature of the business of the Company and need special attention.

2.3.1.Operational and security risk

This is the risk resulting from inadequate internal processes or external events affecting availability, confidentiality of information technology (IT) systems and/or information used for payment services. This includes security risks arising from electronic payment, cyber-risks (e.g. risks of cyber-attacks, data theft, cyber fraud, DDOS attack), inadequate physical security.

To response to these risks, the Company implements control mechanisms to prevent, react to and correct the unauthorized use, disclosure, access, and damage or loss of the user's data, sensitive payment data and the personalized security credentials which the Company delivers to the payment service user for the use of a payment instrument.

Security control mechanisms of the Company involve detective and corrective controls designed to:

- recognize and respond to events and incidents,
- minimize adverse impacts,
- gather forensic evidence (where applicable) and
- in due course 'learn the lessons' in terms of prompting improvements to IT systems (e.g. by improving the preventive controls).

Operational or information security incidents commonly involve the exploitation of previously unrecognised and/or uncontrolled vulnerabilities, hence vulnerability management (e.g. applying relevant security patches to IT systems and addressing various control weaknesses in operational and management procedures) is part preventive and part corrective action.

General approach to the operational and security incidents handling is illustrated in Figure 3 below.

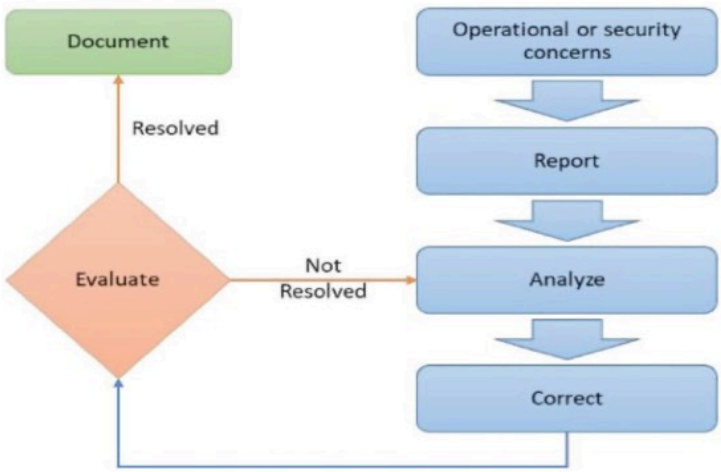

Figure 3 - Operational and security incidents handling

Operational or information security events, incidents and vulnerabilities management process in the Company consists of the six phases:

a. Plan and prepare

The Company is prepared to deal with incidents by establishing appropriate procedures and a competent Incident Response Team headed by the IT Director and IT Security Department. The team is ready to document the investigatory steps they take, what is discovered, and why they chose to take the action they did based on the evidence found.

b. Detection and internal reporting

IT events to be spotted and reported by any staff, but specifically by personnel responsible for operations, customer support and system administrators, as they might be information security incidents. The incident owner provides as much information as possible. Reporting to be done to the IT Director who investigates if the incident is material and reports also to the Risk and Compliance Officer.

An incident may be material if it:

- results in significant loss of data, or the availability or control of the Company IT systems
- affects a large number of customers
- results in authorised access to the Company information and communication systems.

c. Assessment and decision

IT Director must assess the situation to determine whether it is in fact a security incident. IT Director makes decision about how they are to be addressed e.g. patch things up and get back to business quickly, or collect forensic evidence even if it delays resolving the issues.

d. Respond to incident

The incident must be contained, resolved by the IT Director and forensically analysed, where appropriate.

If the Company receives any security-related customer complaint, the response with additional information is given to the customer at this stage in accordance with the Complaints Handling Procedure. A full response to the customer complaint is provided maximum within 15 days.

e. Learn the lessons

Simply identifying the things that might have been done better is not enough. IT Director must make systematic changes that improve the process as a consequence of incidents experienced. IT Director reports to the Risk and Compliance Officer all the incidents and remediation activities.

f. Training

The IT Director and Incident Response Team are in charge of creation of information security incident awareness within the Company and appropriate employees training, including: incident examples and lessons learnt.

External reporting

If the IT Director of the Company becomes aware of a material operational or security incident, he immediately reports the incident to the Risk and Compliance Officer who notifies the Authority as soon as possible. This notification must be done in such form and manner as the Authority may direct. All changes in reporting standards should be followed up by the Risk and Compliance Director at: https://www.fca.org.uk/firms/cyber-resilience

If the incident has or may have an impact on the financial interests of the e-wallet holders, the Company, without undue delay, informs its e-wallet holders of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

Physical security

To address physical security risk, the Board ensures that appropriate practical measures are taken, that includes:

- video monitoring on the premises of the Company
- monitoring of the staff processing transactions,
- physical access to the systems is limited to authorised personnel only and regularly reviewed,
- auditing of transactions on daily basis,
- disciplinary procedures in place to address any fraudulent activity attempts undertaken by employees.

The CEO also ensures that Business Continuity Plan of the Company has been updated and enables the sustained execution of mission critical activities for the Company following a severe unexpected event that prevents service delivery under normal operating conditions.

Personal data

The Company ensures that in accordance with its Data Protection Policy personal data cannot be accessed, processed or retained for the provision of payment services unless the payment service user provided the explicit consent to do so.

3.Financial crime risk and money laundering controls

Financial crime is an increasing concern for all financial institutions. The Company is looking at financial crime prevention as a lifecycle with seven discreet pieces: compliance, prevention, detection, investigation, remediation, monitoring and testing. Preventing and detecting financial crime is rapidly evolving to be one of the biggest challenges, the impact of which extends well beyond monetary losses to reputation and brand, employee morale, business relations, as well as regulatory censure. In recent years financial institutions have been the subject of dramatic increases in fines for regulatory violations imposed by authorities. The Company focuses on key financial crime risks which the Company recognises are specific to the business model it operates and therefore the following controls are necessary to be implemented:

- anti-money laundering and counter-terrorist financing (AML/CTF)
- anti-bribery and corruption
- financial sanctions control
- data security
- fraud prevention.

In practical terms, all these controls can be characterised as individual components of AML programme. The Company studied the FCA “Financial crime: a guide for firms” and builds an efficient programme to mitigate the risk of financial crime. For this purpose the Company developed the AML Manual where customer on-boarding, KYC standards, monitoring and reporting processes are described. The programme includes the following steps the Company takes to prevent financial crime:

- introduction and renewal of AML Manual accessed and understood by all staff,
- having an organisational structure that includes AML employees directly supervised by the Risk and Compliance Officer and that has a Monitoring role responsible for KYC, transactional activity monitoring and suspicious/ fraudulent activity identification,
- direct reporting of MLRO to the Board of Directors; the MLRO has oversight of all high-risk relationships, keeping the copies or references to the evidence of the customer’s identity for five years after the business relationship ended; and transactional documents for five years from the completion of the transaction,
- employment of skilled staff and review employees’ competence to ensure they remain competent for their role, employees training,
- tests to ensure that controls are proportionate and effective.

The Company realises that the size and global nature of the UK financial industry mean that money laundering presents a significant risk to the industry and the Company, so we consider AML/CTF as one of our key priorities. The Company understands its obligations under the legislation, incl. The Fourth Money Laundering Directive 2015/849, The Money Laundering Regulations 2017, the Proceeds of Crime Act 2002, and insures that its AML controls will be proportionate to the business model it operates (size, products, geography).

Overall responsibility for AML systems and controls is given to the Risk and Compliance Officer, this person appointed as a Money Laundering Reporting Officer (MLRO) to supervise the Company’s compliance with its AML/ financial crime prevention obligations.

The Company aims to maintain the highest industry standards in terms of regulatory and compliance requirements. The Company’s strategy to meet its AML obligations is to keep up-to-date risk assessment of the business of the Company, thus developing effective and proportionate risk-based

money laundering and fraud prevention processes. They include not only collection of identification and know-your-customer documentation, but also transaction monitoring where the Company will monitor transactions made into/out of the payment accounts and ensure that due diligence procedures are followed and transactions supporting documentation/ explanations are provided.

The Company will devote adequate resources to AML and financial crime prevention, both human and technical. The Company sets a high priority on the development and use of technology able to help manage its obligations. From the perspective of the compliance function, a robust technological infrastructure is essential to properly monitor transactions and to build a comprehensive profile on clients. Successfully establishing a sustainable and cost-effective process for on-going compliance requires leveraging technology to achieve efficiency and effectiveness. The Company is using client application software with integrated KYC, AML/fraud checks and card risk management based on solution FinMatic (https://finmatic.net/modular-architecture/) to manage financial crime risk and to ensures statistics collection on various parameters for defined period of time.

The Company is also working on commissioning specialised applications and AML intelligent solutions by regtech providers (like Thomson Reuters World-Check, Accuity and others for screening transactions and customers against Politically Exposed Persons, consolidated list of EU financial sanctions and persons, OFAC SDN List and other relevant information) to be integrated to manage compliance risks.

Training is another essential part of the AML programme to make sure that employees of the Company understand and comply with the procedures. As new information comes to light or new legislation is enacted, all employees will be briefed as soon as possible. Staff will be trained upon commencement of duties before dealing with the public and will have training updates every 12 months.

3.1.Payments Fraud detection and internal reporting

Payments fraud incidents to be spotted and reported by any staff, but specifically by personnel responsible for operations, customer support and system administrators. The incident owner provides as much information as possible. Reporting to be done to the Risk and Compliance Officer who documents the investigatory steps taken, what is discovered, and why they chose to take the action they did based on the evidence found.

Payments Fraud incident is any payment transaction that the Company has executed or acquired and that are subject to one of the following fraud types:

- Manipulation of the payer to issue a payment order
- Issuance of a payment order by the fraudster
- Modification of a payment order by the fraudster
- Account takeover
- Lost and stolen card fraud
- 'Card Not Received' fraud
- Counterfeit card fraud
- Theft of card details

If a payment transaction meets the conditions above, the Risk and Compliance Officer records it as a fraudulent transaction to be reported to the FCA (as and when required) irrespective of whether the fraud is committed by the first party (e-wallet holder) or by the third party (person with whom the Company doesn't have a contractual relationship).

3.2.Payments Fraud external reporting

Codego is required under the Payment Services Regulations 2017 to provide the FCA with the Payments Fraud (information on fraud relating to different means of payment). The Risk and Compliance Officer accumulates statistical data on the Payments Fraud and provides Payments Fraud Report (statistical data on fraud) to the FCA annually, within one month of the reporting end date. The Risk and Compliance Officer will follow the instructions on the Gabriel online system for collecting and storing regulatory data to submit the report electronically, using the format of the report set out at:

https://www.handbook.fca.org.uk/form/sup/SUP_16_ann_27E_REP017_20190914.pdf

The Risk and Compliance Officer will also use Gabriel system to view a tailored schedule of the reporting requirements of the Company – and use the guidance notes for the completion of the report as set out at:

https://www.handbook.fca.org.uk/handbook/SUP/16/Annex27F.html#D100000287