C-ISMS-DOC-08-1

[Internal]

Information Security Risk Assessment and Treatment Process

Version 1.0

7th February 2025

CBL Information Security Risk Assessment and Treatment Process

[Internal]

Document Reference

Document Code:	C-ISMS-DOC-08-1
Document title:	CBL Information Security Risk Assessment and Treatment Process
Filename:	C-ISMS-DOC- 08-1 CBL Information Security Risk Assessment and Treatment Process
Author:	Consultant
Owner:	CBL
Date:	7th February 2025
Version:	1.0
Status:	Final

Revision Record

Version	Date	Summary of Changes	Revision Author
1.0	7th February 2025	Establishment of Information Security Risk Assessment and Treatment Process.	Consultant
	6th February 2026	Next Version	

Distribution

Name	Title
Alex Iwobi	Chairman
Francisca Ordega	Chief Executive Officer
Sopade Adeola	Chief Information Security Officer
Ngozi Okobi	Chief Technology Officer
Rasheedat Ajibade	ISMS Manager

Approval

Name	**Position**	**Signature**	**Date**
Alex Iwobi	Chairman		11 February, 2025
Sopade Adeola	Chief Information Security Officer		11 February, 2025

Contents

1. Purpose, Scope, and Users

CBL recognises information security as a critical business requirement for managing risk, protecting information assets, and safeguarding its reputation.

To strengthen its security posture and adopt a more proactive, structured approach, CBL has implemented an information security risk assessment and treatment process aligned with recognised industry best practices.

ISO/IEC 27001 provides the international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). As part of its security maturity journey, CBL has committed to adopting ISO/IEC 27001 and pursuing full certification to demonstrate the effective and consistent application of information security controls, validated through independent external assessment.

This document applies to all information assets, business processes, and personnel within the scope of the ISMS and is intended for use by management, risk owners, and staff involved in information security risk management activities.

2. Risk Assessment and Treatment Process

Risk is defined as the effect of uncertainty on business objectives, arising from the occurrence of an unwanted event or the failure of a desired event to occur. Risk materialises where:

- Business objectives are not achieved.
- Information and other assets are not adequately protected.
- There is non-compliance with internal policies or applicable legal, regulatory, or contractual obligations.
- Business resources are not used efficiently or effectively.
- The confidentiality, integrity, or availability of information is compromised.

CBL operates a structured information security risk assessment and treatment process to identify, analyse, and manage risks before they result in a material impact. Where risks cannot be prevented, appropriate treatment measures are defined to reduce the likelihood and/or impact to acceptable levels.

The process is designed to be repeatable, consistent, and auditable, ensuring that risk assessments produce valid and comparable results regardless of who performs them. This supports informed decision-making, accountability of risk owners, and continual improvement of the ISMS.

2.1 Criteria for Performing Information Security Risk Assessments

Information security risk assessments shall be performed whenever changes or events may impact the confidentiality, integrity, or availability of information or information assets. The scope and depth of each assessment will vary depending on the nature and scale of the change.

Risk assessments shall be conducted in the following circumstances:

- During initial implementation of the ISMS, covering all relevant information assets.
- As part of management review activities, to reflect changes in assets, threats, vulnerabilities, or risk levels.
- For projects involving significant changes to the organisation, systems, processes, or information assets.
- As part of the change management process, to support informed approval decisions.
- Following major external changes that may affect information security, such as new or amended legal or regulatory requirements.

Where there is uncertainty as to whether an information security risk assessment is required, CBL shall adopt a precautionary approach and perform the assessment.

2.2 Process Diagram

The process of risk assessment and treatment is shown in the diagram below.

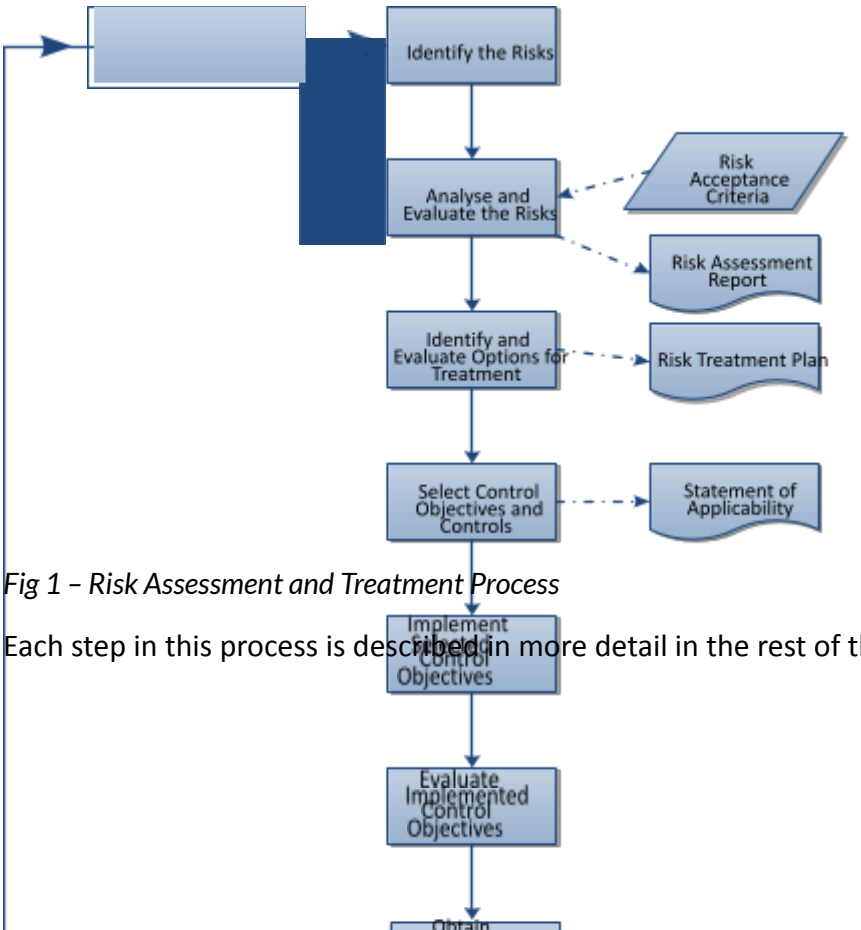

Fig 1 – Risk Assessment and Treatment Process

Each step in this process is described in more detail in the rest of this document.

2.3 Identification of Risks

Information security risks shall be identified in line with the requirements of ISO/IEC 27001 and shall relate to threats to the confidentiality, integrity, or availability of information within the defined ISMS scope.

2.3.1 Compile Asset Inventory

CBL shall maintain a complete and up-to-date inventory of information assets. An asset is defined as anything that has value to the organisation and therefore requires protection.

Assets may include, but are not limited to:

- Physical assets (e.g. servers, network equipment, operational machinery).
- Information assets (e.g. customer data, application databases, records).
- Supporting assets (e.g. software, services, facilities).

The authoritative asset register is maintained in **CBL ISMS0602 – Information Asset Inventory**.

2.3.2 Identify Potential Threats

For each identified asset, potential threats that could reasonably be expected to affect it shall be identified. Threats may arise from accidental, environmental, or malicious sources.

Examples include:

- Environmental threats (e.g. fire, flood, power failure).
- Accidental threats (e.g. human error, system failure).
- Malicious threats (e.g. malware, theft, unauthorised access, sabotage).

A baseline list of typical threats is provided in Appendix A to support consistency.

2.3.3 Assess Existing Vulnerabilities

Vulnerabilities that could be exploited by identified threats shall be assessed for each asset. Vulnerabilities are weaknesses or conditions that increase the likelihood of a threat being realised.

Examples include:

- Unpatched or unsupported systems.
- Inadequate physical protection.

- Poor access controls.
- Insecure storage of paper or electronic records.

2.3.4 Assess the Impact

For each risk scenario, the potential impact of a loss of confidentiality, integrity, or availability shall be assessed.

Impact assessment shall consider effects on:

- Customers.
- Financial position.
- Health and safety.
- Reputation.
- Internal operations and dependencies.
- Legal, regulatory, contractual, or organisational obligations.

2.4 Risk Analysis and Evaluation

CBL shall analyse and evaluate identified information security risks to determine their significance and the appropriate risk treatment actions.

2.4.1 Numerical Classification

Risk analysis shall consider:

- Identified threats.
- Existing vulnerabilities.
- Likelihood of occurrence.
- Potential impact if the risk materialises.

CBL applies a 3-point numerical scale for both likelihood and impact:

Likelihood
1 = Low | 2 = Medium | 3 = High

Impact
1 = Low | 2 = Medium | 3 = High

Risk scores are calculated as:

Risk Score = Likelihood × Impact

This produces a minimum score of 1 and a maximum score of 9, as illustrated in the risk matrix below.

		IMPACT		
		1	**2**	**3**
LIKELIHOOD	**3**	Medium	High	High
	2	Low	Medium	High
	1	Low	Low	Medium

Table 1 – Risk Matrix Chart

Risk Classification

- High: 6–9
- Medium: 3–5
- Low: 1–2

For each risk, the rationale for the assigned likelihood and impact ratings shall be documented to support consistency, repeatability, and future reassessment.

2.4.2 Risk Acceptance Criteria

Risk classifications are interpreted as follows:

- **Low (Green):** Acceptable risk level. No immediate action required beyond routine monitoring.
- **Medium (Amber):** Risk shall be managed and reduced where reasonably practicable.
- **High (Red):** Unacceptable risk level. Treatment actions shall be prioritised and implemented.

The objective of risk treatment is to reduce risks to an acceptable level, for example:

- High ⟶ Medium
- Medium ⟶ Low

Where a risk remains classified as High after treatment, CBL may formally accept the residual risk, provided:

- The decision is justified.
- Management approval is obtained.

- Compensating controls are in place where applicable.

Risk treatment actions and priorities shall be reflected in the **CBL IMS1003 – Continual Improvement Log**, with priority determined by the highest-rated risk addressed by each action.

2.5 Risk Treatment

Risks assessed as exceeding CBL's acceptance threshold shall be treated to reduce them to an acceptable level.

2.5.1 Risk Treatment Options

CBL shall apply one or more of the following treatment options:

1. **Risk Reduction:** Implement controls to reduce the likelihood and/or impact.
2. **Risk Avoidance:** Discontinue or change the activity giving rise to the risk.
3. **Risk Transfer:** Transfer the risk to a third party (e.g. insurance or contractual arrangements).

Treatment decisions shall consider business objectives, regulatory and legal obligations, technical feasibility, and commercial or contractual constraints. The ISMS Manager shall ensure relevant stakeholders are consulted.

2.5.2 Selection of Controls

ISO/IEC 27001:2022 Annexe A shall be used as the primary reference for selecting risk treatment controls. Where Annexe A controls are insufficient, additional controls may be defined and implemented as required.

2.5.3 Implementation and Evaluation of Controls

Selected controls shall be prioritised, implemented, and evaluated based on risk level and cost-benefit considerations. Risk owners and line managers, supported by the ISMS implementation team and ISO Champion, shall ensure that appropriate technical, administrative, and physical controls are applied to effectively mitigate identified risks.

2.6 Risk Assessment and Treatment Plan

The outputs of the risk assessment and risk treatment activities shall be documented in the Risk Assessment and Treatment Plan. This plan provides a consolidated view of identified risks and how they are managed, including the following information:

- Asset(s) (where an asset-based risk assessment is applied).
- Associated threats (asset-based only).
- Identified vulnerabilities (asset-based only).
- Existing controls.
- Likelihood rating, including rationale.
- Impact rating.
- Risk value.
- Risk classification (High / Medium / Low).
- Assigned Risk Owner.
- Risk acceptance decision (accepted or requires treatment).
- Selected risk treatment option.
- Required control(s).
- Assigned Mitigation Owner.

The Risk Assessment and Treatment Plan shall be maintained as a controlled ISMS document and reviewed whenever significant changes occur.

2.7 Statement of Applicability

CBL ISMS0604 Statement of Applicability (SoA) shall document the applicability of controls from ISO/IEC 27001:2022 Annexe A, including:

- Controls selected for implementation and the justification for their selection.
- Controls implemented or planned.
- Controls explicitly excluded and the justification for exclusion.

The Statement of Applicability shall be reviewed and updated following changes to risk assessments, risk treatment decisions, or the ISMS scope.

2.8 Management Approval

Management shall be kept informed throughout the risk assessment and treatment process, including key decisions and identified residual risks. Formal management approval shall be obtained for the following:

- Risk Assessment and Treatment Plan.
- Statement of Applicability.

Approval and acceptance of residual risks shall be recorded in accordance with CBL's documented information control and approval procedures.

2.9 Risk Monitoring and Reporting

Key performance indicators (KPIs) shall be defined to measure the effectiveness of implemented controls in reducing or managing identified risks.

Risk performance metrics and trend information shall be reported at agreed intervals to enable management to identify exceptions, emerging risks, and control weaknesses, and to take timely corrective action.

2.10 Regular Review

Risk assessments shall be reviewed at least annually to ensure risks, assumptions, and controls remain valid and effective.

Additional reviews shall be conducted following significant changes to the business or operating environment, including but not limited to office relocations, mergers and acquisitions, or the introduction of new or materially changed IT services.

2.11 Roles and Responsibilities

Effective risk management requires clear assignment of responsibilities across the risk assessment and treatment lifecycle. The roles involved and their responsibilities are defined using the RACI model to ensure accountability and consistency.

2.11.1 RACI Chart

R = Responsible | A = Accountable | C = Consulted | I = Informed

Step	**Information Security Manager**	**Top Management**	**Team Lead / ISO Champion**
Identify assets	C	I	A/R
Identify risks	A	C	R
Define risk acceptance criteria	C	A/R	C
Analyse and evaluate risks	A	C	R
Identify and evaluate treatment options	A/R	C	C

Select control objectives and controls	A/R	C	C
Implement selected controls	C	A	R
Evaluate control effectiveness	R	I	A/C
Approve residual risks	A	R	C
Monitor and report risks	A	I	R
Perform regular review	A/R	C	C

Additional roles and responsibilities may be defined as the Risk Assessment and Treatment Process evolves within CBL.

3. Conclusion

The Risk Assessment and Treatment Process is fundamental to the effective implementation of CBL's ISMS and forms a key requirement of the ISO/IEC 27001 standard.

By following this process, CBL ensures that information security risks associated with day-to-day business operations are identified, evaluated, and managed in a consistent, auditable, and effective manner.

Effective application of this process supports informed decision-making, proactive risk mitigation, and continual improvement of security controls across the organisation.

4. Appendix A – Typical Threats

The following list provides a starting point for identifying threats relevant to the organisation's information assets. It should be adapted and expanded as appropriate for CBL's environment.

Threat Category	Threat	Example
Human	Malicious outsider	Denial-of-service attack on the payment platform
	Malicious insider	Employee or third party accesses information without authorisation.
	Loss of key personnel	Absence of staff with critical knowledge due to extended sickness

	Human error	Accidental deletion of customer database
	Accidental loss	Manager loses a memory stick containing sensitive bank data
Natural	Fire	Office destroyed due to electrical fault
	Flood	River overflows, flooding main office
	Severe weather	Staff unable to access the office due to extreme weather
	Earthquake	Earth tremor damages servers in main office
	Lightning	Data centre servers damaged by a lightning strike
Technical	Hardware failure	Key server processor fails
	Software failure	Financial system misprocesses invoices due to a bug.
	Virus / Malicious code	Malware spreads across network, preventing data access
Physical	Sabotage	Disgruntled ex-employee damages server room
	Theft	PCs or servers stolen from office
	Arson	Fire started intentionally against the organisation
Environmental	Hazardous waste	Lorry carrying hazardous waste has an accident outside office
	Power failure	Local substation fails, disrupting operations.
	Gas supply failure	Suspected leak shuts down office facilities
Operational	Process error	Data transfer procedure fails, causing data loss or misdelivery
	Crime scene	Office area sealed due to nearby criminal incident.