Date	Name	Role	Change	Version
Mon Jul 07 2025	Tim Murnaghan	CTO	Approved	V1.0

Risk Assessment and Treatment Policy

1. General

1.1 The Risk Assessment process is a critical component of Integrum ESG's ("the Company") internal control system.

2. Purpose and Scope

2.1 The Company's Risk Assessment and Treatment Policy and Procedure ("the Policy") aims to identify, assess, and manage risks that affect the Company's ability to achieve its objectives.

2.2 The risk assessment and treatment process involves identifying, assessing, and minimising risks through ongoing monitoring.

2.3 Risk assessment and treatment procedures are built into the usual business activities including regular management and supervisory authorities.

2.4 This Policy applies to all Company employees.

3. Responsibilities

3.1 Responsibility to follow this Policy applies to all Company employees.

3.2 The CISO is responsible for developing, maintaining, and implementing this Policy.

3.3 The roles and responsibilities of the respective employees at the Company are set out in the Roles and Responsibility Policy.

4. Document Ownership

4.1 The CISO is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the Company's review requirements. A current version of this document is available to all members of staff in the company's shared platform (Sharepoint).

Risk Assessment and Treatment Procedure

5. Method

5.1 Align security efforts with business objectives.

5.2 Minimise and prevent risks related to the confidentiality, integrity, and availability of the Company and its customers' information, assets, and business processes.

5.3 Consider the security requirements of interested parties.

5.4 Review the processes and controls regularly to improve the Company's security posture.

6. Risk Assessment

6.1 The Company must schedule an annual risk assessment workshop to identify and handle risks relevant to the Company and its operations. The outcome of the risk assessment workshop is documented and a risk assessment process is created from this outcome.

6.2 The risk assessment process is implemented through a risk assessment table (see Annexure A).

6.3 The risk assessment roles and responsibilities include the following:

6.3.1 The CISO must coordinate the overall risk assessment process and define the scope of the assessment by identifying areas where sensitive information is received, processed, or transmitted.
6.3.2 The asset owner identifies the assets and determines the threats and vulnerabilities associated with each asset.
6.3.3 The risk owners must assess the impact and likelihood of identified risks and ensure appropriate risk treatment measures are implemented.

6.4 Asset Identification

6.4.1 Assets include the people, processes, and technologies involved in processing, storing, transmitting, and protecting information.

6.4.2 Assets must be classified based on their importance and criticality to the organisation, ensuring appropriate safeguards are in place.

6.4.3 Each asset must be assigned an owner responsible for its protection.

6.5 Risk Identification

6.5.1 Identification of any risk that may affect the confidentiality, integrity, and availability of Company assets.

6.5.2 If and when a new risk is identified a risk assessment is conducted, and the new risk is added to the risk treatment and mitigation plan.

6.6 Vulnerability Identification

6.6.1 A vulnerability is a weakness that can be exploited by a threat and may originate from technology, the organisation, the environment, or a business process.

6.6.2 Identify all vulnerabilities associated with each asset.

6.6.3 In a risk assessment, all vulnerabilities should be considered. Every asset may be associated with several threats, and every threat may be associated with several vulnerabilities.

6.7 Determining the Risk Owners

6.7.1 Each risk must be assigned a risk owner, who is responsible for managing and mitigating that risk. The risk owner may be an individual or an organisational unit. This person may or may not be the same as the asset owner.

6.8 Control Analysis

6.8.1 Document and assess the effectiveness of security controls that have been or will be implemented by the Company to reduce the likelihood of a threat exploiting a system vulnerability.

6.9 Impact and Likelihood

6.9.1 Once risk owners have been identified, it is necessary to assess impacts for each combination of threats and vulnerabilities for an individual asset if such a risk materialises:

6.9.1.1 **Low impact (1-2)**: Loss of confidentiality, availability, or integrity does not affect the organisation's cash flow, legal or contractual obligations, or reputation.

6.9.1.2 **Medium Impact (3)**: Loss of confidentiality, availability, or integrity incurs costs and has a low or moderate impact on legal or contractual obligations of the organisation's reputation.

6.9.1.3 **High-Critical Impact (4-5)**: Loss of confidentiality, availability, or integrity has a considerable and immediate impact on the organisation's cash flow, operations, legal or contractual obligations, or reputation.

6.9.2 After the assessment of impacts, it is necessary to assess the likelihood of a risk occurring:

6.9.2.1 **Low likelihood (1-2)**: Existing security controls are strong and have provided adequate protection. No new incidents are expected in the future.

6.9.2.2 **Medium likelihood (3)**: Existing security controls are moderate and have mostly provided an adequate level of protection. New incidents are possible, but not highly likely.

6.9.2.3 **High - Critical likelihood (4-5)**: Existing security controls are low or ineffective. Such incidents have a high likelihood of occurring in the future.

By entering the impact and likelihood values into a Risk Assessment Table, the level of risk is calculated automatically by multiplying the impact and the likelihood (see Annexure A).

6.10 Risk re-evaluation

6.10.1 The Company will reassess risks whenever a major incident occurs such as;

6.10.1.1 Security breaches;

6.10.1.2 Company mergers and acquisitions;

6.10.1.3 Regulatory changes;

6.10.1.4 Introduction of new business procedures;

6.10.1.5 Major organisational changes; and

6.10.1.6 Feedback from internal and external audits.

7. Risk Mitigation

7.1 Risk mitigation involves prioritising, evaluating, and implementing the appropriate risk-reducing security controls recommended by the risk assessment process to ensure the confidentiality, integrity, and availability of business assets.

7.2 The Company must implement measures to reduce risks, including identifying and documenting potential threats and vulnerabilities that could impact systems processing business information.

7.3 The Company must maintain consistency in risk mitigation methods across departments.

7.4 Prioritise Action and Select Controls

7.4.1 Create a list of potential threats and vulnerabilities based on the level of risk, along with the actions needed to reduce those risks. Determine the appropriate security controls for reducing risks.

7.5 Assign Responsibility

7.5.1 Identify the individual or team with the necessary skills to implement each of the specific security controls and assign their responsibilities. Identify the equipment, training, and other resources needed for the implementation of the security controls.

7.6 Work Plan for Risk Treatment and Mitigation

7.6.1 Implement a selection of security controls.

7.6.2 Transferring the risks to a third party, for example by purchasing an insurance policy or signing a contract with suppliers or partners.

7.6.3 Avoiding the risk, for example by discontinuing a business activity that causes such risk.

7.6.4 Accepting the risk. This option is allowed only if the selection of other work plan options would cost more than the potential impact should such risk materialise. Risks can only be accepted if it has a risk rating or level of less than 10.

7.6.5 Mitigating the risk. This option must be selected only if the risk rating or level is 10 or more as the risk cannot be accepted and needs to be mitigated.

8. Risk Management

8.1 **Communication and consultation**: Communication with internal and external stakeholders should take place at each stage of the risk management process.

8.2 **Establishing the context**: Defining the parameters to be considered when managing risk and setting the scope and risk criteria for the process.

8.3 **Risk identification**: Generating a comprehensive list of risks.

8.4 **Risk Analysis**: Identify the risks' causes and sources, assess their potential positive and negative impacts, and determine how likely those impacts are to happen. Also, review existing risk controls and their effectiveness.

8.5 **Risk treatment**: Risk treatment options include:

8.5.1 avoiding risk;
8.5.2 removing the source of risk;
8.5.3 changing the likelihood of the risk's occurrence;
8.5.4 changing the consequences;
8.5.5 sharing the risk with another party; and
8.5.6 choosing to retain the risk.

8.6 **Monitoring and review**: Encompass all aspects of the risk management process to:

8.6.1 Analyse and learn lessons from the event, changes, and trends;
8.6.2 Detect changes in both the internal and external environment, including shifts in the risk itself;
8.6.3 Ensure that risk controls and treatment measures are well-designed and working effectively; and
8.6.4 Identify new and emerging risks.

Annexure A

Likelihood	**Impact**					
		Very Low (1)	Low (2)	Medium (3)	High (4)	Critical (5)
	Very Low (1)	1	2	3	4	5
	Low (2)	2	4	6	8	10
	Medium (3)	3	6	9	12	15
	High (4)	4	8	12	16	20
	Critical (5)	5	10	15	20	25