Risk Management Policy

1. Introduction

1.1. General Considerations

Due to the nature of its business, the needs, and objectives of its interested parties, HRLocker has a low appetite for risk. Where it is necessary to accept risks, they are controlled and, where possible, insured against. Adequate resources and management energy will be committed to this critical endeavor. Where appropriate, HRLocker has drawn guidance from reputable sources, including ISO 22301 & ISO 31000, for Business Continuity and Risk Management, respectfully, to ensure that our policies, controls and methodologies meet the highest standards.

1.2. Management Commitment

This Policy, which is approved by the CEO, establishes the HRLocker commitment to effective risk and business continuity management. The overall objective of our business continuity strategy is to fully and reliably ensure the continued efficient operation of the business in a manner which maintains adequate standards toward the achievement of our business and customer objectives, and continual control of data confidentiality, integrity and availability. The resourcing requirements of HRLocker incident management plans are documented within the TMS Registers, and associated documentation.

2. Principles of Risk Management

The fundamental principle of the HRLocker approach to risk and business continuity management is to provide a framework which adds value and protection. Additional value is achieved by creating an environment where all personnel are aware of the risks, risk treatments and controls, etc., enabling them to be better prepared to carry out their work. The following principles are employed to support this framework.

2.1. Integrated

Risk management is an integral part of HRLocker operational and support processes.

2.2. Structured & Comprehensive

HRLocker has developed a formal approach to ensure that all aspects are considered relative to an established set of criteria.

2.3. Customized

Full consideration for internal and external contextual issues is factored into risk assessments, treatments, and controls.

2.4. Inclusive

The needs and expectations of all relevant interested parties are considered throughout the HRLocker TMS.

2.5. Dynamic

Risk assessments, treatments, and controls, including training, are regularly reviewed to ensure relevant changes to our operating environment are managed appropriately with regard to risk.

2.6. Best Available Data

HRLocker management ensures that all relevant organizational knowledge, expertise, relevant historical and current data, etc., are considered regularly to provide for the latest thinking and best practice.

2.7. Human & Cultural Factors

Appropriate consideration for human and cultural aspects is important to HRLocker given the nature of our global trading environment. Full consideration for these aspects are incorporated into the TMS.

2.8. Continual Improvement

The results of evaluation of risk management processes are considered through our quarterly management review meetings so that relevant learning and experience is factored into improvement objectives, where appropriate.

3. Total Management System (TMS)

To meet the organizational obligations toward certification to the subscribed ISO Standards and relevant applicable legislation, including GDPR, HRLocker has implemented its Total Management System (TMS). The management system has the full support of all interested parties. All operational and support processes are within the scope of the management system. All relevant personnel have been provided with access to a copy of this document, and it remains available in the HRLocker document system for further reference.

TMS Registers

The TMS Registers is a multi-spreadsheet document, developed to provide a single repository for organizational data to provide for evidence-based decision making. All registers referenced throughout this document are located therein. The HRLocker TMS Registers spreadsheet system documents organizational risks, whether strategic or process based, to ensure that all identified risks are categorized according to criticality, potential impact, and likelihood.

3.1. Contextual Issues

HRLocker has established its Contextual Issues register to provide for the effective management of external and internal issues that may have an impact on operations or be impacted by operations.

3.2. Interested Parties

The Interested Parties register provides for a full analysis of the needs and expectations of all relevant interested parties, both internal and external.

3.3. Process Risk Register

To support HRLocker's risk management objectives, the Process Risk register has been established to document all process activities so that they can be evaluated to consider identified risks dependent on our operational environments.

4. Risk Management Framework

4.1. Risk Identification

Organizational risks are identified through Process Audits, SWOT analysis and other means, including where appropriate, assessments conducted by external providers. All operational and support processes have been assessed to consider potential impacts on Operational, Information Security, Environmental and Occupational Health & Safety relevant to process activities. Where necessary, suitable controls have been implemented to mitigate the identified risks.

4.2. Risks relating to Contextual Issues

The Contextual Issues register provides the primary mechanism for the assessment of risks identified relating to achieving business and customer objectives. This register is developed using criteria provided by the subscribed ISO Standards. Where appropriate, potential vulnerabilities arising through our relationships with external and internal Interested Parties, including international trading partners, are considered therein. All issues are prioritized based on the significance of the potential impact.

4.3. Risks relating to Operational & Support Processes

Risk Management policies and controls across all operational and support processes. To ensure that all aspects are appropriately considered, the Process Risk register has been established to document all risk assessments, treatments, and business continuity considerations. This register provides for the analysis of all process activities, establishing responsibilities, accountabilities and authorities associated with carrying out specific tasks. Where process activities present vulnerabilities which require mitigation, risk treatments are documented with consideration for business continuity planning requirements.

The format of the Process Risk register is developed to include the criteria specified in the subscribed ISO Standards and applicable legislation, ensuring that we can meet our obligations accordingly. Categories for consideration include those listed in the table below.

4.4. Risks Management Criteria

Table 1 below sets out the criteria established to provide for risk management across the organization.

Table 1. Process & Risk Assessment Criteria

Identification of Organizational Risks & Opportunities	TMS Registers, including: *Contextual Issues Register* *Interested Parties Register* *Process Risk Register* *Objectives Register*
Process Analysis	Process Activity Description of Objective, documenting the expected outcomes (KPI) Process Responsibilities / Interdependencies Process Authorities Monitoring Priority Information Assets
Risk Assessment & Risk Treatment	Information Security Risk Category Risk Context Contextual Relevance Risk Description Impact Area Risk Classification / Prioritization Impact Assessment Likelihood Assessment Pre Treatment Risk Rating Risk Treatment Classification Risk Treatment Description
Risk Treatment Evaluation	Effectiveness of Risk Treatment Post Treatment Risk Rating Business Continuity Analysis Business Continuity Planning

4.5. Risk Treatment Planning

Operational process documentation specifies necessary information security controls required to mitigate identified risks. Where risk treatments are deemed to be significant, the management team plans for effective mitigation through management review meetings, where all aspects are considered. Where appropriate, the mitigation processes are documented to meet specific objectives using the HRLocker Process Risk Register.

4.6. Risk Owners Approval & Acceptance

To provide for the effective management of identified risks and opportunities, a nominated management representative is appointed with responsibilities for each issue documented on the relevant register.

All personnel involved in activities where there are identified risks are made aware of determined risk treatments through training and workplace talks. Risk owners are identified and made aware of their responsibilities toward monitoring and reporting.

4.7. Risks related to Information & Privacy Security

The Statement of Applicability (SoA)

All information security controls have been established using ISO 27002:2013 to develop the HRLocker Statement of Applicability. The SoA is regularly evaluated for continual suitability and effectiveness as a key internal audit objective.

4.8. Suitability of Risk Treatments

The HRLocker Internal Audit Programme (IAP) has been developed to ensure that all processes are audited at least once per calendar year, dependent on the complexity and criticality of the processes. In this regard, Incident Management and Business Continuity Planning requirements are treated as organizational processes, and are formally audited accordingly.

Each audit considers the suitability and effectiveness of risk treatments to ensure that operational and risk objectives are being achieved. Management ensures that risk treatments remain suitable and effective through ongoing monitoring and evaluation. Where objectives are not achieved, risk treatments are reassessed with appropriate corrective actions applied.

5. Incident Management & Business Continuity Planning

5.1. Determination & Selection

Where an identified risk may present a significant vulnerability to HRLocker operations, top management ensures that appropriate planning is carried out, with adequate levels of resourcing, to meet business and customer objectives.

All incident management planning is documented, where the responsibilities and authorities of personnel nominated to carry out related activities are established, with clearly defined objectives.

5.2. Incident Management Plans

Risks which can have a significant impact and can benefit from formal planning are documented using the HRLocker Contextual Issues Register, which ensures that all relevant criteria are considered and managed effectively.

5.2.1. Incident Response

Each incident management plan described the specific activities determined necessary to respond to a reported incident, including the roles and responsibilities of personnel nominated with responsibilities toward the plan. Where incident response requires a series of activities, it is treated as a process and documented accordingly on the Process Risk Register.

5.2.2. Business Continuity

All HRLocker incident management plans document any applicable business continuity considerations, including planning for specific activities, where applicable.

5.3. Exercising & Testing

Where appropriate, company incident management plans are tested periodically to ensure that they remain suitable and effective. Resulting data is recorded and stored for future reference, and may require the revision of the risk analysis documented in the relevant registers.

5.4. Distribution

All relevant interested parties, including HRLocker personnel have been provided with a copy of this document, and relevant incident management plans, which remain available in the shared document system for further reference.

6. Performance Evaluation

6.1. Monitoring & Measuring

Where applicable, all personnel involved in the implementation of the risk treatment and incident management plans are required to adhere to the requirements of the plans for monitoring and measuring. In particular, where there is an identified nonconformity to expected outcomes, personnel are to report observations accurately to ensure that the results of the risk treatment can be effectively assessed.

Responsibilities toward monitoring and measuring during the implementation of organizational plans are documented above as part of the planned processes, where relevant to each activity. Overall responsibilities and authorities for reporting on monitoring and measuring activities are described here.

Where applicable the HRLocker Audit Template is used to document the monitoring requirements of the risk treatment and incident management plans. The audit criteria is extracted from the risk treatment process documented, with provision for recording observations made throughout the implementation and execution processes. The effectiveness of the risk treatment and incident management activities are recorded therein, using an established fixed scoring mechanism. Identified nonconformities are documented on the HRLocker CAR Register for reference and follow up.

6.2. Analysis & Evaluation

During the implementation of the risk treatment and incident management plans, the nominated team leader is responsible for ensuring that monitoring and measuring activities are producing expected outcomes with regard to achieving the objectives of the respective risk treatment and incident management plan. Where appropriate, the team leader will seek input from the nominated top management representative, to ensure that all organizational objectives are effectively met.

6.3. Management Review

The team leader and the top management representative will jointly take responsibility for reporting on the outcomes of the implementation of the risk treatment and incident management plans. This report will be presented to the HRLocker quarterly management review meetings. Where applicable, specific reporting requirements are documented here.