Risk Assessment and Management Policy

IronHub Inc

August 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1

Table 2: Document history

Date	Comment
Jun 1 2022	Initial document
Sep 11 2023	Updated approach

1 Purpose and Scope

The purpose of this policy is to define the methodology for assessing and treating risks related to information security and business continuity at IronHub. This policy establishes a structured approach to identifying, analyzing, mitigating, and monitoring risks that may impact the confidentiality, integrity, and availability of IronHub's data and systems.

This policy applies to:

a. All employees, contractors, and stakeholders involved in risk assessment and risk treatment.

b. All company assets, including electronic documents, databases, IT infrastructure, applications, and outsourced services.

c. Risks associated with operations, security, regulatory compliance, business continuity, and third-party relationships.

2 References

a. Risk Assessment Report Template

3 Risk Management Approach

IronHub follows a systematic approach to risk management that consists of the following key steps:

1. **Risk Identification** – Identify company assets and the associated threats and vulnerabilities.
2. **Risk Assessment** – Evaluate the likelihood and impact of risks.
3. **Risk Treatment** – Determine and implement appropriate mitigation measures.
4. **Risk Monitoring & Reporting** – Continuously assess and report risks to leadership.

4 Risk Appetite

IronHub's risk appetite reflects the level of risk the organization is willing to accept in pursuit of its objectives. The following thresholds apply:

- **Acceptable (Score 0–2):** Risks at this level may be accepted with monitoring. No immediate treatment is required, but risks must be documented in the Risk Register.

- **Requires Treatment (Score 3–4):** Risks at this level must be actively mitigated. Acceptance of a score 3–4 risk requires documented approval from the CEO or Leadership Team, along with a documented rationale and compensating controls.

IronHub has a **low risk appetite** for risks affecting the confidentiality or availability of client data, regulatory compliance obligations, and reputational harm. IronHub has a **moderate risk appetite** for operational risks where compensating controls are in place.

5 Risk Identification

Risk identification focuses on **people, processes, and technology** that could impact IronHub's operations or information security.

Key risk categories include:

i. Compliance risks related to regulatory obligations and contractual commitments.

ii. Information security risks such as data breaches, unauthorized access, and insider threats.

iii. Business continuity risks affecting system availability and operational resilience.

iv. Vendor and third-party risks associated with external service providers.

v. **Fraud risks**, including misappropriation of assets, unauthorized system access, financial fraud, and manipulation of financial reporting. Fraud risk must be explicitly assessed as part of the annual risk assessment.

Each identified risk is assigned a **Risk Owner** responsible for managing and mitigating the risk.

6 Risk Scoring and Assessment

Once risks are identified, they are assessed based on their **Likelihood and Impact** scores. The total risk score is calculated as follows:

i. **Risk Score = Likelihood Score + Impact Score**

6.1 Likelihood Levels

Likelihood Level	Likelihood Score	Description
Low	0	Either existing security controls are strong and have so far provided an adequate level of protection, or the probability of the risk being realized is extremely low. No new incidents are expected in the future.
Moderate	1	Either existing security controls have most provided an adequate level of protection or the probability of the risk being realized is moderate. Some minor incidents may have occurred. New incidents are possible, but not highly likely.
High	2	Either existing security controls are not in place or ineffective; there is a high probability of the risk being realized. Incidents have a high likelihood of occurring in the future.

6.2 Impact Levels

Impact Level	Impact Score	Description
Low	0	Loss of confidentiality, integrity, or availability will not affect the organization's cash flow, legal, or contractual obligations, or reputation.
Moderate	1	Loss of confidentiality, integrity, or availability may incur financial cost and has low or moderate impact on the organization's legal or contractual obligations and/or reputation.
High	2	Loss of confidentiality, integrity, or availability will have immediate and/or considerable impact on the organization's cash flow, operations, legal and contractual obligations,and/ or reputation.

6.3 Risk Acceptance Criteria

- **Risk Score (0-2)**: Acceptable risks.
- **Risk Score (3-4)**: Requires treatment and mitigation.

7 Risk Treatment and Mitigation

For risks that require treatment (score of 3 or 4), the following mitigation strategies may be applied:

1. **Implement security controls**: Strengthening security measures such as encryption, access controls, and monitoring systems.
2. **Transfer risk**: Through insurance or third-party agreements.
3. **Avoid the risk**: By discontinuing high-risk activities.
4. **Accept the risk**: Only if mitigation costs exceed the impact of the risk. This must be documented and approved by the CEO or Leadership Team.

Residual risks after mitigation must be documented in the Risk Register.

8 Risk Monitoring and Reporting

- **Annual risk assessments** must be conducted at a minimum.

- The **Risk Register** is updated whenever new risks are identified.
- Any **significant organizational, technological, or regulatory changes** trigger an immediate risk review.
- **Leadership Reporting:** Risk treatment plans and risk assessment results must be reported to the Leadership Team **quarterly**. The summary must include new risks identified, changes to existing risk scores, treatment status, and any accepted risks.
- **Board Reporting:** A consolidated risk assessment report must be presented to the Board of Directors (or equivalent governing body) at least **annually**. The report must include the organization's risk profile, material risks, treatment progress, and any unacceptable residual risks.
- A **Risk Assessment Report** is maintained as part of SOC 2 audit compliance.
- **Fraud Risk Assessment:** An explicit fraud risk assessment must be conducted as part of the annual risk assessment, covering at minimum: misappropriation of assets, unauthorized system access, financial fraud, and integrity of financial reporting. Findings must be documented in the Risk Register.

9 Continuous Improvement

The risk assessment process is continuously improved through:

- Regular internal audits and testing.
- Incident analysis and lessons learned.
- Enhancing controls based on emerging threats and business needs.

This policy ensures IronHub's commitment to strong risk management practices, supporting compliance with relevant industry and regulatory standards.