Inazuma.co Risk Management Policy

Version: 1.0

Reviewed By: Risk & Compliance Committee

---

1. Objective

The objective of the Inazuma.co Risk Management Policy is to provide a structured, consistent, and continuous process for identifying, assessing, and managing risks across the organization. This policy ensures that Inazuma.co achieves its strategic objectives, protects its resources, and maintains resilience against operational, financial, reputational, legal, and technological risks.

---

2. Scope

This policy applies to all departments, functions, employees, and stakeholders of Inazuma.co. It covers:

- Strategic risks
- Operational risks
- Compliance risks
- Financial risks
- Technological risks
- Reputational and environmental risks

---

3. Risk Management Principles

Inazuma.co adheres to the following principles:

Principle	Description
Integrated Approach	Risk management is embedded into all business processes
Proactive Identification	Risks are identified early and managed before they escalate
Continuous Improvement	Processes are regularly reviewed for effectiveness
Accountability & Ownership	Risk owners are designated at every level of the organization
Communication & Awareness	Risk culture is promoted through open communication and training

---

4. Risk Governance Structure

The governance structure ensures clear roles, responsibilities, and escalation paths.

Role	Responsibilities
Board of Directors	Approve risk policy and oversee overall risk management framework
Risk & Compliance Committee	Monitor and report on risk exposures and effectiveness of mitigation strategies
Risk Officer	Coordinate risk identification, assessments, and mitigation
Department Heads	Implement risk controls within their functions
All Employees	Identify, report, and manage risks in daily operations

---

5. Risk Management Process

Inazuma.co follows a structured risk management cycle:

5.1 Risk Identification

- Conduct workshops, audits, and stakeholder interviews
- Identify internal and external sources of risk

5.2 Risk Assessment

Criteria	Definition
Likelihood	Probability of the risk occurring
Impact	Consequences on business operations or objectives
Risk Score	Combination of likelihood and impact

Risk Assessment Matrix

Likelihood ↓ \ Impact →	Low	Medium	High
High	Medium	High	Extreme
Medium	Low	Medium	High
Low	Low	Low	Medium

5.3 Risk Mitigation

- Develop action plans for unacceptable risks
- Assign ownership and allocate resources
- Implement controls and monitor progress

5.4 Risk Monitoring

- Use dashboards and tools to track risk indicators
- Review mitigation progress quarterly

5.5 Reporting and Review

- Escalate key risks to the Board and stakeholders
- Revise strategies based on incident feedback

---

6. Risk Categories and Examples

Category	Examples
Strategic	Market entry failure, competitive threats, regulatory changes
Operational	Supply chain disruption, system downtime, human errors
Financial	Budget shortfalls, investment losses, currency fluctuations
Technological	Cyber attacks, data breaches, IT infrastructure failure
Legal & Compliance	Contractual disputes, IP infringement, non-compliance with laws
Environmental	Natural disasters, carbon footprint, waste management issues

---

7. Risk Appetite and Tolerance

Inazuma.co defines its risk appetite as the amount and type of risk it is willing to take to achieve objectives. Risk tolerance levels are determined per department and reviewed annually.

Business Function	Risk Appetite	Tolerance Level
Product Development	Medium	Moderate
Finance	Low	Conservative
Marketing & Sales	Medium-High	Flexible
IT & Data Security	Very Low	Stringent

---

8. Risk Communication and Culture

Risk awareness is built into company culture through:

- Risk training programs
- Cross-functional risk meetings
- Regular updates from the Risk Officer
- Encouraging reporting without fear of reprisal

---

9. Business Continuity and Disaster Recovery

Inazuma.co maintains a business continuity plan (BCP) and disaster recovery plan (DRP) to ensure:

- Continuity of critical operations during crises
- Timely recovery of essential services
- Protection of critical data and infrastructure

9.1 DRP Testing Schedule

Component	Testing Frequency
Data Backup & Recovery	Monthly
Emergency Communication	Quarterly
IT Failover Tests	Bi-annually

---

10. Compliance and Legal Considerations

This policy is aligned with:

- ISO 31000 Risk Management Standards
- IT Act and Data Protection Guidelines
- Companies Act, 2013
- SEBI Governance Principles (if applicable)

---

11. Training and Awareness

All employees will undergo risk management awareness training annually. Specialized workshops will be conducted for leadership, IT, finance, and project teams.

Training Module	Frequency	Target Group
Introduction to Risk	Annual	All employees

Cybersecurity Threats	Semi-annual	IT and Data Teams
Risk Reporting and Response	Quarterly	Department Heads

---

12. Policy Review and Audit

This policy will be reviewed annually or in the event of:

- Major incident or breach
- Regulatory changes
- Strategic shifts in the business

Internal audits will assess the implementation of risk controls and policy compliance.

---

13. Contact Information

For queries, concerns, or reporting:

Risk & Compliance Committee
Email: risk@inazuma.co

Acknowledgment Form

I acknowledge that I have read and understood the Inazuma.co Risk Management Policy. I agree to comply with its principles and participate actively in risk-related activities.