Risk & Compliance

Enterprise Risk Management Policy (ERM)

Purpose

The purpose of this policy is to establish a comprehensive, integrated, and proactive approach to managing risk across B&S Investments. As a Saudi-rooted, globally operating holding group spanning exhibitions, manufacturing, tourism, creative content, hospitality, and digital ventures, the ability to identify, assess, respond to, and monitor risk is essential to protect value, ensure regulatory compliance, and enable sustainable growth. This policy provides the foundation for embedding risk awareness into decision-making at all levels.

Scope

This policy applies to the Board of Directors, executive leadership, functional heads, business unit managers, and relevant staff across B&S Investments and its subsidiaries. It governs risk management activities across all geographies and sectors, including financial, operational, strategic, legal, reputational, technological, and environmental risks. It also applies to joint ventures, strategic partnerships, and outsourcing arrangements where B&S Investments has governance or fiduciary responsibility.

Policy Statement

B&S Investments is committed to a structured, transparent, and forward-looking Enterprise Risk Management framework. The ERM policy ensures that risk is not viewed merely as a compliance obligation but as a strategic discipline that enables informed decisions, protects stakeholder value, and supports resilience in a dynamic global

environment.

All employees are responsible for managing risk within their areas of influence. Management must integrate risk management into planning, budgeting, execution, and reporting cycles. The Board retains ultimate accountability for oversight of the ERM framework and risk appetite.

- Key principles of this policy include:
- Risk is inherent to all business activity and must be proactively managed
- Risk ownership is embedded in business functions, with escalation channels for material exposure
- Risk appetite and tolerance levels are defined, approved by the Board, and reviewed annually
- Risks are prioritized by likelihood and potential impact across financial, operational, legal, reputational, and ESG dimensions
- Risk response strategies must align with corporate objectives and regulatory obligations

Roles & Responsibilities

Role	Responsibility
Board of Directors	Approves the ERM framework, risk appetite, and reviews strategic risk reports quarterly
Audit & Risk Committee	Oversees implementation, evaluates risk reports, approves mitigation plans, and monitors emerging risk trends
Group CEO	Ensures enterprise-wide application of ERM; leads integration of risk management into strategic decision-making
Chief Risk Officer (CRO)	Develops the ERM framework, leads risk assessments, maintains the corporate risk register, facilitates risk workshops, and provides independent oversight
Executive Committee	Identifies cross-functional risks, approves mitigation strategies, and ensures alignment with performance objectives
Business Unit Heads	Responsible for identifying and managing operational and sector-specific risks within their units and ensuring compliance with Group-wide controls

Role	Responsibility
Functional Heads (Finance, Legal, HR, IT, ESG, Procurement)	Own and manage function-specific risks; report material issues to the CRO
All Employees	Expected to identify risks in their day-to-day roles, report concerns, and support implementation of controls and mitigation actions

Procedures & Implementation

1. **Risk Identification**
    - Risks are identified through a variety of methods including strategic planning sessions, operational reviews, incident reporting, audits, compliance assessments, and employee feedback
    - Emerging risks are identified through industry benchmarking, regulatory monitoring, and macroeconomic scanning
2. **Risk Assessment**
    - All identified risks are assessed based on:
        - Likelihood of occurrence (on a -5point scale)
        - Potential impact (financial, reputational, operational, legal)
        - Velocity (speed of onset)
    - Risk scoring results in classification as: Low, Medium, High, or Critical
3. **Risk Appetite & Tolerance**
    - Risk appetite is defined by the Board annually and guides decision-making at all levels
    - Tolerance thresholds are developed per category (e.g., revenue deviation, compliance incidents, reputational exposure)
    - Any proposed activity exceeding tolerance must be escalated for executive or Board review
4. **Risk Response**
    - Risk response strategies include:
        - Avoidance (ceasing high-risk activity)
        - Reduction (implementing controls or process changes)

- Transfer (insurance or third-party outsourcing)
- Acceptance (with monitoring, where within tolerance)

- Response owners are assigned and tracked via the Group Risk Dashboard

5. Risk Monitoring & Reporting

- All critical and high-level risks are included in the Corporate Risk Register, which is updated quarterly
- Business Units and Functions must maintain operational risk registers and escalate any changes to the CRO
- The CRO issues quarterly risk reports to the Executive Committee and Audit & Risk Committee, highlighting trends, incidents, and control effectiveness
- Ad hoc risk reviews may be triggered following incidents, internal audits, or external investigations

6. Training & Culture

- ERM training is mandatory for all senior managers and risk owner
- Risk awareness campaigns and scenario-based workshops are held annually to strengthen the risk culture
- Sector-specific risk simulations (e.g., cyberattacks, supplier disruption, reputational crisis) are conducted semi-annually

7. Technology & Tools

- Risk assessment tools, dashboards, and templates are hosted on the enterprise governance platform
- Incident reporting and key risk indicators (KRIs) are digitally integrated to support real-time monitoring

Monitoring & Review

The ERM Policy will be reviewed every 18 months by the Chief Risk Officer in collaboration with the Internal Audit and Legal teams. The review evaluates:

- Alignment with changing business strategy and operating models
- Feedback from risk owners and Board committees
- Performance of controls and effectiveness of response strategies
- Trends in key risk indicators, incidents, and near-misses

Revised policies, frameworks, and risk registers will be communicated to all stakeholders and embedded in training and business planning processes..

Associated Documents

- Risk Management Framework & Methodology
- Corporate Risk Register
- Risk Appetite & Tolerance Statement
- Delegation of Authority Policy
- Business Continuity & Crisis Management Plan
- Internal Audit Charter
- Compliance & Regulatory Risk Map
- ESG Risk Integration Guidelines
- Whistleblower Protection Policy
- Incident Reporting Protocol