

Risk Management Policy

Contents

Change Order Form	2
Definitions	3
Introduction	4
Enterprise Risk Management (ERM) Defined	5
Applicability of Enterprise Risk Management (ERM)	6
Components of ERM	7
Definition of Risk at FIIB	9
Approval & Review of the Risk Management Policy	10
Distribution of the Risk Management Policy	10
Risk Management Charter	10



Change Order Form

Serial Number	Reference	Description
1	Name of the document	RISK MANAGEMENT POLICY
2	Purpose & scope	This policy and supporting guidance establishes a comprehensive approach to risk management at FIIB.
3	Date of First Approval	April 2021
4	Date of last approval/amendment	September 2022
5	Indicative Date of Next review	September 2023
6	Administering entity	Strategic Planning Committee (SPC)
7	Approving authority	FIIB Board of Governors (BoG)
8	Reference to related policies, procedures, guidelines & regulations	Strategic Plan – FIIB2025 Risk Management Charter

Definitions

“Board” shall mean the *Board of Governors (BoG) of Fortune Society for Development & Promotion of International Business*

“Academic & Business Advisory Council (ABAC)” shall mean the Academic & Business Advisory Council of Fortune Institute of International Business

“Institute” shall mean *Fortune Institute of International Business (FIIB)*

“Strategic Planning Committee (SPC)” means the committee constituted by the BoG to monitor and review the Risk Management Policy, Risk Management Charter and such other functions pertaining to risk management, by whatever name called.

“Risk Owner” means the persons appointed to monitor implementation of mitigation plans of risks identified, update risk registers and such other responsibilities as may be defined by SPC.

Introduction

In the dynamically changing education landscape, *Fortune Institute of International Business* (FIIB) is exposed to risks from Strategic, Operational, Technological, Regulatory, and Financial Perspectives. The *FIIB Board of Governors* (BoG) proactively establishes a comprehensive approach to risk management at FIIB through the *Enterprise Risk Management (ERM) Policy* which includes a framework for Identifying, Measuring, Mitigating, Monitoring, and Reporting of all risks facing the organization. A *Risk Charter* provides an overview of the risk management organization structure, procedures, roles and responsibilities associated with the ERM implementation. The ERM links to the strategic planning process through the associated monitoring and reporting mechanism.

Through the establishment of an ERM framework, the BoG aims to realize the following objectives:

- a) Develop a risk appetite appropriate to the FIIB context and mandate its commitment to the ERM.
- b) Embed ERM into organization's culture by improving the associated governance and accountability.
- c) Align ERM framework with strategic objectives laid down in Strategic Plan *FIIB2025*
- d) Facilitate informed, data driven, risk-based decision making
- e) Enhance credibility with wide range of stakeholders (e.g. Students, Employees, Regulators, Society, etc.)
- f) Protect and enhance stakeholder value by minimizing risks and exploiting opportunities.

Enterprise Risk Management (ERM) Defined

Enterprise risk management (ERM) is the process of identifying and addressing methodically the potential events that represent risks to the achievement of strategic objectives, or to opportunities to gain competitive advantage (Chartered Global Management Accountant)

Through this approach to risk management, FIIB aims to:

- Deal effectively with future events that create uncertainty, pose a significant risk or opportunity and respond in a manner that creates a net positive outcome.
- Enable decision making based on data, evidence, and appropriateness to our mission, values, and strategic plan
- Improve planning and prioritization through a structured understanding of opportunities and threats.
- Support effective use of resources such that we continue to develop, adapt and improve in a complex, competitive and changing higher education environment

Applicability of Enterprise Risk Management (ERM)

This ERM framework is applicable across the institute. FIIB follows a multi-level approach to risk management as enumerated below:



1. *Strategic Level* relating to the institute.
2. *Tactical Level* relating to the departments (e.g. Department of People Success, Department of Technology Support, Department of Institutional Growth etc)
3. *Operational Level* relating to the individual employee owning an action item from the strategic plan.

One distinctive feature of this model is the “inverted pyramid” approach, which places employees at the top so that the plan is driven on the ground. The idea is to maximize collaboration, increase the speed of ideas, and to create a more responsive team that adds continuous value to the organization. The process aims to ensure that the organization is following the direction established during strategic planning and all stakeholders are best aligned and reinforce each other. Such a multi-tier approach engenders collaboration, engagement leading to crucial insights for course-correction.

Components of ERM

The ERM framework at FIIB consists of the following components:

- a) Risk identification
- b) Risk Measurement
- c) Risk Mitigation
- d) Risk Monitoring
- e) Risk Reporting

Risk identification:

Risk identification deals with finding, recognizing, & describing exposure to uncertainty, and implies environmental scanning in relation to the strategic objectives.

Risk measurement

Risk measurement for the purpose of this Policy means the quantification of the impact of risks to determine their potential severity and the likelihood of occurrence of the risk to determine frequency.

FIIB uses the following method to measure the risk:

- High Probability of occurrence and High Consequences
- Medium Probability of occurrence and Medium Consequences
- Low Probability of occurrence and Low Consequences

Based on this, risks shall be categorized into Extreme, High, and Significant Risks.

Risk Mitigation: FIIB uses the following framework to decide appropriate strategy for each risk:

- Accept the risk (Acknowledge the existence of a particular risk, and make a deliberate decision to accept it without engaging in special efforts to control it).
- Manage the risk (Adjust requirements or constraints to eliminate or reduce the risk).
- Transfer the risk (Reassign organizational accountability, responsibility, and authority to another stakeholder (third party) willing to accept the risk).

- Avoid the risk

Risk Monitoring

Risk monitoring is a periodic process for reviewing risks, updating status of the mitigation plans and reporting status to the BoG / Strategic Planning Committee. It also includes process to ensure that new risks are escalated appropriately, considering the change in the business environment. FIIB follows a multi-level approach to monitoring risks. Operational level risks are monitored at individual level, tactical risks are monitored at departmental level, and strategic risks are monitored at the senior management level.

Risk Reporting

The purpose of risk reporting is to create awareness of key risks, improve accountability for the management of risk and the timely completion of risk treatment plans. The strategic risk register is prepared by the Chief Risk Officer and reviewed by the Strategic Planning Committee on a monthly basis. The ABAC gets reports semi-annually and the BoG is reported on a quarterly basis.

Definition of Risk at FIIB

FIIB defines risk as any event that could impede the institute's ability to achieve objectives fulfilling its mission and vision through its business and strategic plan. While we have created the following categories of risks, there could be some overlap.

Risk Types	Examples
Strategic	• Reduction in business vitality (dip in enrolment numbers, changing learning preferences, changing technology, etc.) • Failure to attract & retain talent • Unplanned leadership changes • Negative impact to reputation/loss of trust
Operational	• Internal & External Fraud • Employment practices & workplace safety • Business disruption & system failure • Execution, delivery, and process management • Inefficient use of resources • Physical property/damage
Technological	• Data security breach • Hardware and software failure • Virus attacks • Misuse of IT resources • Power outage
Regulatory	• Changes in approval process • Fee capping • Changes in accreditation norms • Non-Eligibility for external funding
Financial	• Fee dependent revenue model • Dip in enrolments • High Costs • Unfavourable cash flow

Approval & Review of the Risk Management Policy

The Policy shall be approved (one time) by the BoG and reviewed by the Strategic Planning Committee (yearly). However, it may be reviewed earlier based on requirement and / or under special circumstances. In case of changes to existing policy, SPC shall recommend changes to the Risk Management policy, if any, and submit to the BoG for its approval.

Distribution of the Risk Management Policy

Distribution of policy shall be controlled centrally in the institute. The policy shall be classified as 'Confidential' as it sets out in detail the procedures and policies to be followed by the institute. The ABAC and all the Risk Owners who shall be given access to this policy shall be instructed to keep the copies in their safe custody.

Risk Management Charter

The Risk Management Charter describes Risk Management organization structure, procedures, roles and responsibilities. SPC shall review the charter annually or earlier if the need arises. The Risk Management Charter shall be approved by the BoG. Refer "Risk Management Charter" document for details.