EMBASSY DEVELOPMENTS LIMITED

(formerly Equinox India Developments Limited)

(CIN: L45101HR2006PLC095409)

Enterprise Risk Management Policy

Document control

Field	Detail
Policy title	Enterprise Risk Management Policy
Entity	Embassy Developments Limited (EDL / Company)
Version	V1.0
Policy Owner	Company Secretary and Group Chief Compliance Officer (Nominated as Risk Officer)
Reviewers	AVP – Finance and Accounting, CFO, Relevant senior management
Recommending Authority	Risk Management Committee (RMC)
Approving Authority	Board of Directors
Effective date	November 03, 2026
Review cycle	At least once every two years, or earlier upon a material change

Board approval

Version	Recommending Authority	Approving Authority	Approval date	Effective date
1.0	Risk Management Committee	Board of Directors	November 03, 2026	November 03, 2026

Version history

Version	Date	Owner	Summary
1.0	November 03, 2026	Risk Officer	Initial policy for approval

Contents

1. Purpose and policy statement 4
2. Scope and application 4
3. ERM principles 4
4. ERM governance structure 4
5. Roles and responsibilities 5
5.1 Board of Directors 5
5.2 Risk Management Committee 5
5.3 Audit Committee 5
5.4 Senior management .....
5.5 Risk Officer 6
5.6 Risk owners 6
5.7 Employees and third parties 6
6. ERM process 6
6.1 Establish scope, context and criteria 6
6.2 Identify risk 6
6.3 Analyse risk 7
6.4 Evaluate, prioritise and consolidate 7
6.5 Treat risk 7
6.6 Monitor, review, record and report 7
7. Risk taxonomy 7
8. Risk assessment methodology 7
8.1 Assessment principles 7
8.2 Likelihood criteria 7
8.3 Impact criteria 8
8.4 Resilience assessment 8
8.5 Risk rating and heatmap 9
9. Risk treatment 9
10. Monitoring, reporting and escalation 11
10.1 Minimum reporting cadence 11
10.2 Escalation triggers 11
11. Specialist risk frameworks 11
12. Risk culture and capability 11
13. Assurance and continual improvement 11
14. Related documents and records 11
15. Policy administration 12
16. Definitions 12

1. Purpose and policy statement

Embassy Developments Limited ("EDL" or the "Company") recognizes that uncertainty can affect the achievement of its objectives and can create both threats and opportunities. Enterprise Risk Management ("ERM") is the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value (COSO 2017 ERM Framework).

Risk is the:

- Is the effect of **uncertainty** on objectives (ISO 31000)
- Is the possibility that events will occur and affect the achievement of strategy and business objectives (COSO 2017 ERM Framework)

This Policy establishes the minimum governance and process requirements for ERM. It is intended to support compliance with the Companies Act, 2013 and the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended ("SEBI LODR"), and is informed by ISO 31000:2018 and COSO Enterprise Risk Management, Integrating with Strategy and Performance (2017).

2. Scope and application

This Policy applies to EDL and to the extent legally permissible and proportionate to EDL's ownership, control and influence, its subsidiaries and Special Purpose Vehicles (SPV). It applies to directors, senior management, risk owners and employees.

The ERM programme covers all material internal and external risks, including strategic, operational, project, financial, legal, regulatory, compliance, technology, cyber security, data privacy, people, health and safety, sustainability, ESG, business continuity, crisis and emerging risks. Specialist policies and frameworks (E.g., cyber security, data privacy, BCP) where available shall remain applicable and shall operate consistently with this Policy.

3. ERM principles

- Creates and protects value and supports sustainable achievement of objectives.
- Is integrated into governance, strategy, planning, capital allocation, projects, transactions and performance management.
- Is structured, comprehensive and proportionate to the Company's context and risk profile.
- Is customised and proportionate to EDL's real estate development business, project lifecycle and risk profile.
- Is inclusive, transparent and based on timely consultation with relevant stakeholders.
- Is dynamic and responsive to change, emerging risks, interconnected risks and risk velocity.
- Uses the best available information while acknowledging uncertainty, assumptions and data limitations.
- Considers human behaviour, incentives, culture and decision-making biases.
- Promotes accountability, constructive challenge, timely escalation and continual improvement.

4. ERM governance structure

The Board has ultimate oversight of risk management. The RMC is the principal Board committee overseeing ERM and recommends this Policy to the Board. Senior management and risk owners own and manage risks. The designated Risk Officer coordinates the framework and consolidates reporting. Internal Audit provides independent assurance and shall not assume ownership of management risks or controls.

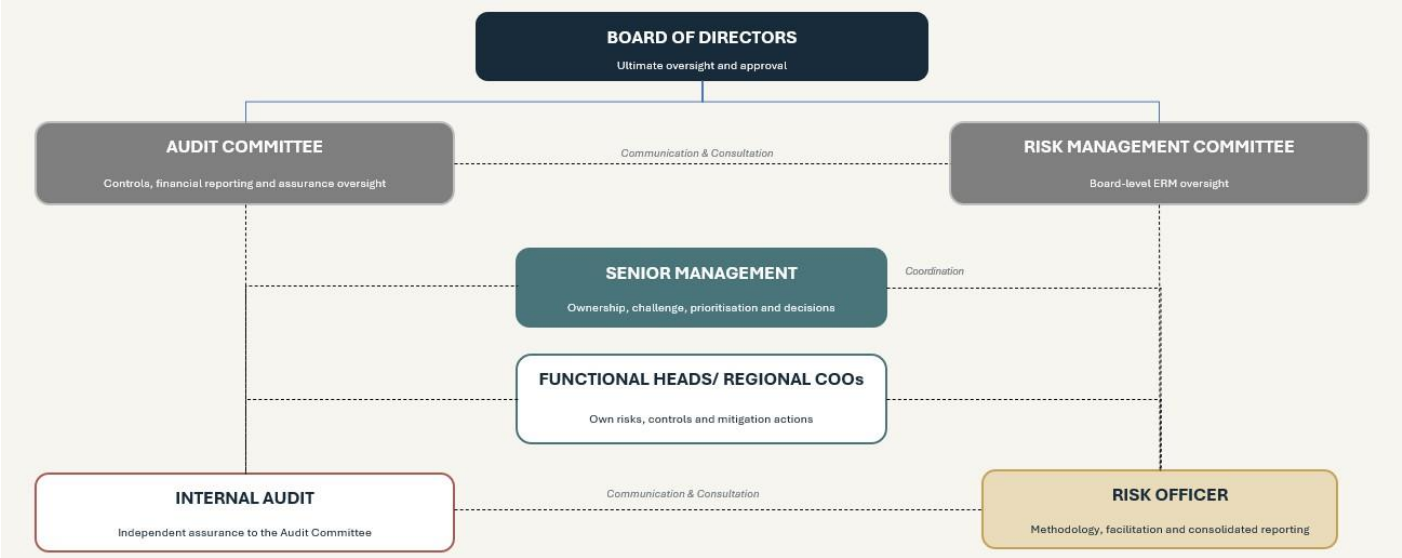


Figure 1: ERM governance structure

5. Roles and responsibilities

5.1 Board of Directors

- Approve this Policy and any material amendments on the recommendation of the Risk Management Committee.
- Retain ultimate oversight of the risk management plan and satisfy itself that appropriate procedures inform the Board about risk management program.
- Review the enterprise risk profile at least annually and consider material or escalated risks, significant incidents and emerging risks and matters that may threaten the Company's existence or going concern.

5.2 Risk Management Committee

- Review and recommend ERM Policy and any material amendments to the Board; review the Policy at least once every two years, considering changing industry dynamics and evolving complexity.
- To formulate a detailed risk management policy which shall include:
  - A framework for identification of internal and external risks including strategic, financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee
  - Measures for risk mitigation including systems & processes for internal control of identified risks
  - Business continuity plan
- Ensure that appropriate methodology, processes and systems are in place to identify, assess, evaluate, treat, monitor and report risk.
- Oversee identification of internal and external risks, measures for mitigation and applicable internal controls
- Monitor implementation of this Policy and evaluate the adequacy of risk management systems.
- Review the enterprise risk profile, material/ emerging risks, mitigation plans, resilience, overdue actions and significant changes in exposure.
- Keep the Board informed about the nature and content of its discussions, recommendations and required actions.
- Review appointment, removal and terms of remuneration of the Chief Risk Officer, if any.
- Coordinate with the Audit Committee and other Board committees where responsibilities overlap.
- Review the appointment, removal and terms of remuneration of the Chief Risk Officer, if any.

5.3 Audit Committee

- Evaluate internal financial controls and risk management systems.
- Oversee financial reporting risk, internal financial controls, internal audit, fraud and material control deficiencies.
- Coordinate with the RMC on matters involving controls, compliance, fraud, assurance or overlapping committee mandates.

5.4 Senior management

- Implement the ERM framework and provide adequate people, information, systems and resources.
- Integrate risk considerations into strategy, budgets, investments, land and project diligence, project governance, business planning and material transactions.
- Review the consolidated enterprise risk profile at least quarterly, or at another cadence approved by the RMC, and direct action on material exposures and overdue plans.
- Assign risk owners at an appropriate level and ensure accountability for controls and mitigation actions.
- Promote timely and factual escalation and ensure material decision papers identify key assumptions, risks, mitigations and residual exposure.

5.5 Risk Officer

- Coordinate maintenance and implementation of this Policy and the ERM methodology.
- Maintain the enterprise risk register, assessment criteria, heatmap, action tracker and ERM reporting calendar.
- Facilitate risk identification, assessments and management reviews; provide methodology, coordination and constructive challenge without assuming risk ownership.
- Consolidate enterprise risk information and prepare reporting for senior management, the RMC and the Board.
- Monitor changes in risk exposure, mitigation plans and overdue actions and facilitate escalation.
- Coordinate with Finance, Legal, Compliance, Information Security, Sustainability, Human Resources, Projects and other specialist functions.
- Facilitate ERM awareness and capability-building within the organization.

5.6 Risk owners

- Identify, articulate, assess, manage, monitor and report assigned risks.
- Ensure controls are designed and operating, evidence is maintained and deficiencies are addressed.
- Define & implement mitigation plans with action owners and target dates.
- Escalate material incidents, control failures, significant changes and emerging risks promptly.
- Provide updates at least quarterly or upon material change.

5.7 Employees and third parties

Employees shall understand risks relevant to their work, comply with controls and report incidents, near misses and concerns in good faith. Contract owners shall ensure that material third-party risks are assessed and addressed through proportionate due diligence, contractual requirements, monitoring and escalation.

6. ERM process

EDL shall operate a continuous and iterative ERM process. Communication and consultation, monitoring and review, and recording and reporting apply throughout.

1 CONTEXT	2 IDENTIFY	3 ANALYSE	4 EVALUATE	5 TREAT	6 MONITOR & REPORT
Objectives, scope, criteria	Risk Event → Consequence	Inherent, resilience, residual rating	Prioritise, and consolidate	Response, owner, due date	Track, escalate, improve

Figure 2: EDL ERM process

6.1 Establish scope, context and criteria

Define the objective or decision, affected entity / project / region, internal and external context, stakeholders, assumptions, dependencies, assessment horizon and criteria.

6.2 Identify risk

Risks may be identified through strategy and project reviews, management workshops, risk interviews, incidents, near misses, loss events, audit findings, legal and compliance updates, customer feedback, scenarios and horizon scanning.

Risk statement syntax:

[uncertain risk event], resulting in [consequence].

Risk context or contributory factors (internal & external) shall be captured in the risk register.

6.3 Analyse risk

Assess inherent impact and likelihood before considering existing controls. Evaluate resilience based on ownership, control o peration, action status and contingency. Then assess residual impact and likelihood after considering existing controls and mitigations .

6.4 Evaluate, prioritise and consolidate

Prioritisation shall consider residual rating first and then resilience, strategic significance, urgency, interdependencies, legal or regulatory significance and management judgement.

6.5 Treat risk

Select a proportionate treatment and document the risk owner, action owner, action, resources, target date. Cost, benefit, feasibility and dependencies shall be considered by Senior Management.

6.6 Monitor, review, record and report

Risk owners shall monitor exposure and action status. Enterprise risks shall be reviewed at least quarterly by senior management and reported to the RMC in line with its meeting calendar. Material changes and incidents shall be escalated promptly.

7. Risk taxonomy

Risk category	Coverage
1. Strategy	Strategy execution, growth, portfolio mix, acquisitions, divestments, joint ventures, investment decisions and market positioning.
2. Development & Operations	Land, approvals, design, execution, quality, cost, schedule, handover, customer delivery, facilities, business continuity and operational resilience.
3. Financial	Liquidity, cash flow, collections, treasury, funding, refinancing, covenants, interest rates, taxation, financial reporting, insurance and capital management.
4. Legal, Regulatory & Compliance	Litigation, title, contracts, approvals, RERA, statutory compliance, governance, ethics, fraud, misconduct and investigations.
5. Technology & Information Security	Technology strategy, digital transformation, AI governance, cyber security, data privacy, information management, resilience, third parties and disaster recovery.
6. People, Culture & Safety	Leadership succession, talent, skills, culture, conduct, occupational health and safety, contractor safety and labour relations.
7. Sustainability & ESG	Climate, environment, emissions, water, resources, social impact, responsible development, stakeholder matters and sustainability reporting.

The taxonomy supports completeness and aggregation. A risk may affect multiple categories, but one primary category shall be assigned for reporting.

8. Risk assessment methodology

8.1 Assessment principles

- Risk rating is determined using likelihood x impact matrix
- Assess inherent risk before considering existing controls and residual risk after considering existing controls and mitigations.
- Resilience supports prioritisation and escalation. It does not replace or mathematically multiply the residual rating.
- Where quantitative data is reliable, same shall be used. Otherwise management judgement will be applied using the qualitative anchors.

8.2 Likelihood criteria

Score	Rating	Probability guidance	Evidence / time horizon
5	Almost certain	>80%	Event is occurring, recurring or expected within 12 months.
4	Likely	60–80%	Strong indicators; more likely than not within 12–24 months.
3	Possible	40–60%	Credible scenario; occurred internally or in comparable projects or markets.
2	Unlikely	10–40%	Could occur, but controls and current indicators make it less likely.
1	Rare	<10%	Exceptional circumstances; no current trigger and strong preventive evidence.

8.3 Impact criteria

For each risk, assess every applicable dimension and adopt the highest score.

Score	Financial & project economics	Delivery, customer & reputation	Legal, regulatory & compliance	Health & safety	Technology & cyber	People	ESG & environment
5 Severe	Threatens EDL's liquidity or funding capacity, or makes a strategic project unviable	>12-month launch/OC/hand over delay; multiple strategic projects delay; sustained national trust impact	Critical license/approval loss; adverse title outcome; prosecution or material listed-company breach	Fatality or multiple life-changing injuries; prolonged stop-work across material sites	Material data breach; prolonged critical-system outage; enterprise recovery failure; reportable privacy breach	Attrition of multiple critical leaders; enterprise plan cannot be executed	Severe environmental damage; critical consent withdrawal; portfolio-level climate disruption
4 Significant	Major project margin erosion or prolonged capital lock-up requiring substantial funding or plan changes	6–12 month delay; flagship/high-GDV project impact; major claims or national adverse coverage	Stop-work/major regulatory action; significant litigation or repeated material non-compliance	Single life-changing injury or multiple serious injuries; major site shutdown	Major cyber incident or multi-project outage; significant privacy breach	Attrition of critical leader/team affecting launches or delivery	Material breach/notice; significant remediation; project disruption from water/ flood/ heat/ pollution
3 Moderate	Meaningful cash-flow or project-return impact requiring senior management intervention	3–6 month delay; one material project impact; significant regional concern	Formal notice/ investigation; reportable breach; material contract/ compliance dispute	Serious injury requiring hospitalization; repeated high-risk findings or temporary stop-work	Contained incident/outage causing material project or functional disruption	Critical vacancy/ capability gap causes material delay; elevated regretted attrition	Moderate breach or climate/ resource disruption requiring management programme
2 Minor	Limited cost or margin impact manageable through project or annual budget reallocation	1–3 month localised delay; contained complaints; normal recovery mechanisms	Limited breach/notice/ dispute without material operating restriction	Medical-treatment injury or multiple minor injuries; isolated high-risk observation	Short disruption or contained data/control incident; no material external consequence	Temporary capacity gap manageable through cover or hiring	Localised issue/reporting gap; limited remediation and no material project delay
1 Negligible	Minimal financial impact within approved project contingency and routine authority	<1 month; isolated, reversible; negligible customer/ reputation effect	Technical/isolated lapse with no formal action	First-aid case or near miss with no lost time	Minor service/control issue; no sensitive data impact	Isolated vacancy/ attrition with no delivery impact	Minor observation with no breach, disruption or stakeholder impact

8.4 Resilience assessment

Rating	Assessment anchors
Well managed	Clear owner; controls operating effectively; actions implemented or on track.
Partially managed	Controls exist but effectiveness is partial or inconsistent; actions are planned & yet to be implemented;
Not adequately managed	Ownership or control gaps; repeated exceptions; overdue actions; absence of adequate mitigations

Resilience supports prioritisation and escalation. It does not replace or mathematically multiply the residual rating.

8.5 Risk rating and heatmap

Residual risk is placed on the matrix using residual likelihood and residual impact after considering existing controls and mitigations.

Likelihood / Impact	1 Negligible	2 Minor	3 Moderate	4 Significant	5 Severe
5 Almost certain	Medium	High	Critical	Critical	Critical
4 Likely	Medium	High	High	Critical	Critical
3 Possible	Medium	Medium	High	High	Critical
2 Unlikely	Low	Low	Medium	High	Critical
1 Rare	Low	Low	Medium	Medium	High

9. Risk treatment

Treatment	Description
Avoid / terminate	Do not start, discontinue or exit the activity creating the exposure.
Reduce / treat	Implement or strengthen controls to reduce likelihood, impact or both.
Share / transfer	Allocate part of the exposure through insurance, contract, outsourcing or joint arrangements, recognising that accountability may remain with EDL.
Accept / retain	Retain the exposure within approved authority, with documented rationale, monitoring and review date.
Pursue / enhance opportunity	Take or increase exposure where expected value is consistent with strategy, authority and controls.

Treatment plans shall identify the risk owner, action owner, action and target date. Overdue or ineffective actions shall be escalated as required based on residual rating, resilience, ageing and consequence.

10. Monitoring, reporting and escalation

10.1 Minimum reporting cadence

Forum / activity	Minimum cadence
Business, function and project risk reviews	Quarterly and upon material change
Consolidated enterprise risk review by senior management	Quarterly, unless critical risks emerge during the quarter that requires senior management attention
Risk Management Committee	At each scheduled meeting to discuss critical & high risks and promptly for material matters
Audit Committee coordination	As required for internal audit, internal controls, financial reporting, compliance, fraud and assurance matters
Board of Directors	At least annually and promptly for material or escalated matters

10.2 Escalation triggers

Prompt escalation is required for:

- A Critical risk or a material increase in residual exposure.
- A significant incident, control failure, legal or regulatory breach, cyber or data event, serious health and safety event, environmental event or business interruption.
- A matter that may threaten liquidity, going concern, strategic execution, license to operate or require external disclosure.
- A material overdue or ineffective mitigation action.

Escalation under this Policy does not replace legal, regulatory, incident response or stock-exchange notification processes.

11. Specialist risk frameworks

ERM covers all types of risk. Specific areas including business continuity and crisis management, cyber security, information security, data privacy, sustainability, ESG, health and safety and third-party risk shall also be governed through the relevant specialist policies, standards and response plans. Material exposures, incidents and control gaps from those frameworks shall be reflected in ERM reporting where enterprise escalation is warranted.

12. Risk culture and capability

- Leaders shall promote transparent, timely and accountable risk behaviour.
- Employees shall be encouraged to raise concerns and near misses in good faith.
- Risk information shall be communicated to the right decision-makers in a timely manner.
- Role-appropriate ERM awareness and guidance shall be provided to directors, management, risk owners and relevant employees.

13. Assurance and continual improvement

The ERM framework shall be periodically assessed using management review, independent assurance, incidents, regulatory change, stakeholder feedback and lessons learned. Internal Audit may use ERM information to inform risk-based audit planning but shall apply independent judgement and shall not treat management's assessment as a substitute for audit risk assessment.

14. Related documents and records

- Enterprise risk register
- RMC charter / terms of reference

15. Policy administration

The Policy Owner and Risk Officer shall be the Company Secretary and Group Chief Compliance Officer. The RMC shall recommend this Policy and material amendments to the Board. The Board is the approving authority.

This Policy shall be reviewed at least once every two years and earlier upon a material change in applicable law, listing obligations, strategy, business model, governance, risk profile or operating environment.

16. Definitions

Term	Definition
Board	Board of Directors of Embassy Developments Limited.
ERM	The coordinated culture, capabilities and practices used to manage risk across strategy, performance and operations.
Risk	The effect of uncertainty on objectives; the effect may be adverse, favourable or both.
Inherent risk	Exposure before considering existing controls and mitigations.
Residual risk	Exposure remaining after considering existing controls and mitigations.
Resilience	The ability to prevent, respond to and recover from a risk event, assessed through ownership, mitigations & controls.
Risk owner	The executive or manager accountable for managing and reporting an assigned risk.
Action owner	The person responsible for delivering a defined mitigation action by the agreed date.
Emerging risk	A new or changing risk whose nature, likelihood, impact or timing is not yet sufficiently understood.
RMC	The Board-level Risk Management Committee of EDL.