ENTERPRISE RISK MANAGEMENT

Author:	CHIEF RISK OFFICER
Date:	22-Mar-23

Table of Contents

1. Abbreviations

CFO – Chief Finance Officer

CRO – Chief Risk Officer

EBIT - Earnings before interest and taxes

ERC – Enterprise Risk Committee

ERM – Enterprise Risk Management

FRC – Financial Risk Committee

ICG - ISMS Core Group

IRC – Internal Risk Committee

ORC - Operational Risk Committee

SPOC – Single Point of Contact

2. Objective

The core business area in which Expleo operates is dynamic and given the nature of the market, service expectations, regions being serviced etc., elements of risk are inherent. **Enterprise Risk Management (ERM)** hence is required to proactively manage what the Organisation Leadership identify as the critical goals and the most critical risks to the achievement of the organisation's mission and objectives.

The **Core Business Objectives** of Expleo Solutions shall be as below:

- **Strategic**
  - Addressing Customer needs
    - Deliver built in quality
    - Addressing client needs in Digital business / Software
    - Driving Innovation & Agility
  - Customer Satisfaction & Retention
- **Financial**
  - Achievement of target revenue, EBIT & Cash Adequacy
- **Reporting & Compliance**
  - Timely & Accurate Financial Reports
  - Timely & Accurate Reporting on efficiency, Sales and other objectives.
  - Manage Risk & Controls in a complex digital world
  - Adherence to all internal processes, statutory, Regulatory, certification and customer specific requirements

  - Compliance to Information and Data security which leads to confidentiality, integrity and availability.
- **People Centric**
  - Employee Retention, benefits, satisfaction & attract potential recruits.
  - Employee Health and safety, working model.
  - Employee skill development

The yearly objectives and targets for these areas shall be defined and published as part of the Budget exercise and Annual Planning exercise.

The purpose of ERM policy is to:

- Facilitate proactive risk management
- Enhance understanding of all risks faced by the business across all levels of the organization, considering the internal and external context. The categories of risks identified are strategic, Financial, Operational and Compliance risks.
- Facilitate the prioritization of risks.
- Enhance the effectiveness of risk management measures and its results.

3. Scope

The Enterprise Risk Policy of Expleo is formulated in compliance with Regulations of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("the Listing Regulations") and provisions of the Companies Act, 2013 ("the Act"), which requires the Company to lay down procedures about risk assessment and risk minimization.

The scope of the ERM Policy covers risks across all levels of the organization, considering the internal and external context The key categories of risks identified are:

- **Strategic** - Any risk that impacts the company's strategy and makes it less/ineffective; could be technology changes, new competitor, change in customer demand etc.,
- **Financial** – Risks relating specifically to the money flowing in and out of business, and the possibility of a sudden financial loss
- **Operational** – Risks that could facilitate or hinder the efficiency and effectiveness of core operations within the organization.
- **Compliance** - Risks relating to non - adherence of any applicable legal requirements, statutory adherence, security threats, certification requirements, customer requirements etc.,
- **ISMS** – Risk relating to IT Security, Cyber Risks, Information security incidents, Data Protection & BCP

Risk identification and assessment includes the risks provided below. However, the list is illustrative and not conclusive. Any other risks that may be determined by the Committee shall be included and covered as part of the Enterprise Risk Register.

Category	**Risks**
Strategic	Economic environment and market conditions – Economic slowdowns or factors affecting the business of our clients and the industry impacting our revenue growth
Strategic	Strategic risks – Risks associated with strategic development, alliances, business mix, business planning, performance targets, failure of alignment of functional strategies and objectives with enterprise-wide strategies,
Strategic	Political environment - Change due to political environment in the country impacting the growth strategies
Strategic	Marketing / Business Development - Risks associated with customer sources, competition, brand management & brand licensing.
Strategic	Any risk having a potential impact on the reputation of the company including risk related to adverse comments from clients, internal or external stakeholders, data security violations, cyber-attacks, poor workplace operations and conduct, bad financial statements, employee misconduct or disputes, regulatory violations, branding, lawsuits, penalties, etc.
Financial	Finance related risks- Relationship management with lenders, management of cash, billing and claims processing, customer credit risks, receivables management, inadequacy of controls and lack of adequate monitoring leading to higher risks of fraud. Also, include uncertainty concerning changes in the economic-financial situation of sectors (sectoral risks)
Financial	Foreign exchange risks
Operational	Technical, quality or performance risk: Meeting performance standards and time schedule
Operational	Human resource management risks: Risks associated with culture, organizational structure, communication, recruitment, workplace, health and safety, performance management, remuneration, learning & development, retention and attrition
Operational	Information Security, Cyber Security and Technology Risks – Inadequate capacity planning, systems are inadequately managed, data integrity, reliability, cyber security related risks, including security related risk related to employees working from home
Operational	Supply chain - Risk associated with sourcing and vendor management
Operational	Business Continuity related - Global disruptions like pandemic, natural disasters, IT outages, cyber security, terror attacks and unrest, power disruptions. includes COVID outbreak
Compliance	Legal and Compliance – Risk relating to non-compliance with legislations, including direct & indirect tax law provisions, adequacy of financial reporting & disclosures, regulations, internal policies and procedures. Also includes data privacy related regulations and violation of intellectual property.

Compliance	Environmental, sustainability, Social and Governance related risks - Environmental management practices and duty of care, working and safety conditions, respect for human rights, anti-bribery and corruption practices and compliance to relevant laws and regulations.
ISMS	Protection of information systems leading to data leakage, adequate controls to protect data from theft, viruses, sabotage or improper use. Data corruption / theft, misuse of assets, interruption of services / business disruption, disclosure of information, etc. Also, cyber risk exposure due to work from home.
ISMS	Protect the reliability and accuracy of the information provided by the information systems,

This ERM Policy is the umbrella framework for risk management in the organization. Detailed Risk Management Procedures detailing the methodology for performing risk assessment and templates are laid down.

The methodology for performing Risk assessment on Information Security would be covered as a separate process but however the outcome of such risk assessment impacting the business objectives would be included as part of the ERM process.

4. Approval

This Policy shall be approved by the Risk Management Committee consisting of Board of Directors. Chief Risk Officer shall be responsible for ensuring periodical review and updation of this policy. Functional heads shall be responsible for implementation of the policy and controls established through the risk assessment process across the organization.

5. Risk Committees

ERM framework of Expleo comprises of a series of processes, structures and guidelines which assist to identify, assess, monitor and manage its business risk, including any material changes to its risk profile. To achieve this, Expleo has clearly defined the responsibility and authority of Board of Directors, to oversee and manage the risk management program, while conferring responsibility and authority on senior management to develop and maintain the risk management program in light of the day-to-day needs of Expleo. Regular communication and review of risk management practice provides Expleo with important checks and balances to ensure the efficacy of its risk management program

The below table details the various committees involved in risk management program along with their roles and responsibilities.

Stakeholder	**Members**	**Responsibilities**	**Review Frequency**
Risk Management committee (RMC) - Board	Two Members of the Board and Managing Director	• Approve the Risk Management Policy • Provide guidance and direction on ERM and is responsible for implementing ERM policy • Delegate monitoring and review of risk management activities to risk committees • Apex body to approve the risks, its mitigation plan and the future course of action.	Half-Yearly
Enterprise Risk Committee (ERC)	MD/COO/CFO / Sales Head	• Monitoring and review of risk management activities as approved by Board • Review and recommend actions for mitigating risks • Review the effectiveness of mitigation plans for Enterprise risks	Half-yearly
Chief Risk Officer (CRO)	Manager- Process, Risk and Controls	• Liaise / coordinate with Risk Owners and Risk Champions on risk-related matters to obtain an enterprise-wide view of risks;	-

Internal Risk Committees:
• Strategic and Financial Risk Committee (SFRC) - All Financial Risks /All Strategic risks/ Share holder related/ legal risks, headed by the CFO.
• Operational Risk Committee – Managing all Operational risks), headed by
	Representatives from Department Heads/ Business Unit Heads	• Review the Enterprise level risk from each department
		• Ensure periodic review of KRIs and effectiveness of the mitigation plans against KRI
		• Organization level Risk dashboard review
		• Address action out of ERC and RMC meetings
			SFRC(Quarterly)
			ORC(Monthly) and ICG (Quarterly)

Head of Risk & Controls • ISMS Core Group (ICG)- All risks relating to Information Security & Customer specific compliances headed by Head of Risk & Controls			
Department Heads (Risk Owners)	Head of Department	• Identify, assess, monitor and report potential risks in their areas of responsibility; • Manage risk by implementing mitigation plans • Prepare / review risk registers • Report Enterprise level risks to Risk committees • Monitor and report changes to existing risks or risk profile to IRC, ERC and RMC	Periodic reviews
Department SPOC	Nominated Manager from Department	• Tracking and review of department risk in discussion with team and department head • Prepare and Update risk register whenever risks are identified • Share the risk register with risk officer	-

6. ERM Methodology

Enterprise Risk management shall cover the following:

- Risk Management framework which comprises of:
    - Identifying and assessing a broad array of internal and external risks that could adversely impact the achievement of organizational goals and objectives in a structured manner.
    - Ensuring appropriate ownership and accountability of risks

  - Developing and implementing appropriate risk mitigation and monitoring plans by risk owners including systems and processes for internal control of identified risks and business continuity plans
- Establishing a program structure that engages functional leaders across to identify and prioritize risks consistent with the Risk tolerances
- Providing senior leadership / Board with key timely information to make risk-informed decisions.
- Providing reasonable assurance with respect to organization's ability to achieve its strategic and business objectives.

The Key of a successful ERM program are structured processes and methodologies. The ERM methodology followed in Expleo consists of six key elements in line with the ISO 31000:2018

1. Communication and Consultation
2. Establishing scope, context, criteria
3. Risk assessment
4. Risk treatment
5. Monitoring and Review
6. Periodic Audit, Recording and Reporting.

6.1 Communication & Consultation

The ERM requires an inclusive communication and consultation approach with all relevant stakeholders, including but not limited to the Delivery, Sales and Business partner teams. This communication & consultation shall be done on a periodic basis to ensure information dissemination and periodic reviews. Risk Assessment process shall be communicated to the relevant stakeholders to understand the risk for taking decisions and in some cases, stakeholders shall be consulted to support decision making.

6.2 Establishing Scope, Context and Criteria

When establishing the context within its ERM process, Expleo takes into consideration the internal and external environments – as well as the purpose, goals, and objectives of the ERM Program. While establishing the context, it is critical to understand the existing condition, way the organization operates (including activities performed by each business function and its link/relationship in the organisation context), internal and external context impacting the realization of the defined organizational objectives.

The Department / Business Function specific objectives will also be derived from the Organizational objectives. This would be the base for identification of Risks.

6.3 Risk Assessment

Risk Assessment consists of 2 main steps:

- Risk Identification
- Risk Analysis & Evaluation

The risk assessment shall be conducted at least once a year. Any additional risk assessment process within the year shall be triggered by internal /external changes in the business environment. It is an iterative process and carried out diligently, to enable greater acceptance of risk while ensuring rigorous due diligence, treatment, monitoring and control.

Risk Identification:

The Risk Assessment process starts with a systematic identification of key risks. This involves analysing of all business processes/related activities along with the conditions and events that might result in a threat to the business objectives. Potential Risks across the ERM risk categories should be considered to ensure that all the relevant risks are identified.

Risks impacting the business function / Departmental objectives along with the Key Risk Indicators, will be recorded in the Departmental Specific Risk Register and Risks impacting the Organisational objectives in the Enterprise Risk Register.

Risk Analysis & Evaluation:

Risk Analysis allows Expleo to consider and identify the extent to which the potential risks might have an impact of the achievement of the organisational / Business functional / Departmental objectives. This requires an assessment of the likelihood of the risk and the potential impact (Consequences) of the same on the organisational objectives.

Classification of risk based on the risk analysis shall be done as High, Substantial, Moderate and Low. Risk criteria shall be evolved to identify risk control mechanisms for each of the above classifications for risk treatment. The Risk registers are updated accordingly.

6.4 Risk Treatment

Once risks are identified and analysed in accordance with the previous steps, the Enterprise Risk Register is further developed. Expleo will use an Enterprise Risk Register as the primary tool for articulating organisation’s risk profile.

In evaluating risks for prioritization to drive further action, Expleo will take into account the degree of control the organisation has over each risk, the cost impact, benefits and opportunities presented by the risks.

Risk treatment for Threats may be of four types: Terminate (seeking to eliminate activity that triggers such a risk), Transfer (passing ownership and/or liability to a third party), Mitigate (reducing the likelihood and/or impact of the risk below the threshold of acceptability), and Accept (tolerating the risk level).

Where risk exceeds acceptability (i.e. risk appetite), additional risk treatment strategies and mitigating actions may be applied to reduce the level of risk.

6.5 Risk Monitoring & Review

All risks are assigned a Risk Owner, the individual who is ultimately accountable for ensuring the risk is managed appropriately. Each treatment measure is assigned a Treatment Owner, the individual who is responsible for executing the risk treatment. The Risk Owner and Treatment Owner may or may not be the same individual. Ownership is assigned based on the principle of who is 'best suited' to take accountability for managing the risk, noting that many people may need to be involved. The primary ownership for the risk management would be Functional heads for their respective areas. Apart from this, the internal risk committees would ensure effectiveness of the overall risk framework, periodic review of KRIs and effectiveness of the mitigation plans.

Based on the risk categories, Risk monitoring and periodic review will be carried out by respective Risk Committees. The risk committees and the business owners would be assisted by the Internal Audit functions to review the effectiveness.

6.6 Recording & Reporting

Risk reporting ensures that relevant risk information is available across all levels of the organization in a timely manner to provide the necessary basis for risk-informed decision making. All the Risk Committees would be recording the information relating to the individual risk as well as have details wherever required.

All Risk Indicators are tracked on a pre-defined periodicity and would be reported to the Managing Director on either a monthly, quarterly, Half-yearly basis or need-basis for risks requiring immediate decisions/approval.

7. Related Documents

- Information Security Risk Management Policy and Procedure
- Defined Business Objectives / Department Objectives
- Enterprise Risk Register
- Department specific Risk Register
- Information Security Risk register

Policy Revision History

Version No	Date	Author	Reviewer	Approver	Change Description
1.0	1-Sep-22	Emerald Johnson	Roopa Rajesh / Desikan Narayanan	Risk Management Committee (Balaji Viswanathan/ Rajiv Kucchal / Jessie Paul)	The document is revised as part of QMS Convergence and new document number (EIN) provided
2.0	22-Mar-23	Emerald Johnson	Roopa Rajesh / Desikan Narayanan	Balaji Vishwanathan & Board of directors	Following changes done: 1. Objectives -Risk objectives revisited. 2. Scope - ISMS risk added as part of the Risk category. 3. Risk committees – Revisited based on One India committee and review frequency modified. 4. The applicability changed from Technology to One India