Thomas Cook (India) Limited

Risk Management Policy

Issued By: Mr Aniruddha Chaudhuri (Head - BPIA)	***Recommended By: Risk Management Committee*** ***Approved By: Board of Directors***
Effective: August 2021	
Version: 1.0	

Table of contents:

1. Foreword

Thomas Cook (India) Limited (TCIL) is the leading integrated travel and travel related financial services company in the country offering a broad spectrum of services that include Foreign Exchange, Corporate Travel, MICE, Leisure Travel, Insurance, Visa & Passport services and E-Business.

Risk is an inherent part of the decision making process across the business and much of the success of the company is based upon seizing opportunities and managing the associated risks.

In order to effectively manage the risks, all areas of the company have a structured method for risk identification, measurement, evaluation, reporting, and risk mitigation.

The current dynamic and competitive business environment within which Thomas Cook (India) Limited operates makes it necessary for the company to establish an internally developed proactive and robust risk management framework. The framework will assist the Company in identifying and managing various internal, external and business risks such as credit, operational, market, financial, information technology including cyber security, BCP (business continuity planning), reputational, compliance, human resource and strategic risks, etc., in an effective manner with an aim to achieve its overall business objectives. For this purpose, Thomas Cook (India) Limited has implemented an organization-wide, multi-layered risk management framework aligned to its business needs.

Defining 'Risk'

In business terms, a risk is any threat that may prevent the achievement of business objectives. Whilst it primarily refers to risks with a negative impact such as the loss of assets or of business reputation it also includes risks related to those activities that aim to identify and exploit opportunities within our business.

Purpose and benefits of risk management

Risk management is the process of identifying and mitigating strategic, business, technical, financial and non-financial risks. Risks include events or occurrences that prevent the organization from achieving its business objectives in an effective manner.

The purpose of risk management is also to proactively identify potential risks/ events before they occur, so that risk management activities are planned and invoked as needed to manage adverse impacts on achievement of business objectives. An integrated and robust risk management framework can help support the maximization of business performance through:

- Clarity of roles and responsibilities
- Informed and risk-adjusted decision-making across the organization

- Improved communication of risks to the Risk Management Committee and Audit Committee wherever required.
- Integrated governance practices and
- Reduced earnings volatility and increased profitability

Scope and objective of enterprise wide risk management policy

The need for an enterprise wide risk management policy is to ensure that an effective risk management framework is established and implemented within Thomas Cook (India) Limited and to provide regular reports on the performance of that framework, including any exceptions, to the Risk Management Committee, and the Audit Committee. This risk management policy complements and does not replace other existing risk management policies such as the Credit Control or Information Security policies, or compliance programs, such as those relating to service, quality and regulatory compliance matters.

The key objectives of this risk management policy are to:

- Provide an overview of the principles of risk management at Thomas Cook (India) Limited
- Define the risk management structure for effective risk management, including roles and responsibilities of various participants in the risk management framework. Define the methods and thresholds for the evaluation of risks
- Explain the methodology for identifying, assessing and managing existing and new risks
- Specify guidelines for implementation of the risk management framework within the Company
- Define the process to be followed for review and monitoring of various business risks.

To achieve the risk management objectives, the Company aims to adhere to the following risk management principles:

- The identification and management of risk is integrated in the day to day management of the business
- Risks are identified, continuously monitored, assessed, and reported in the context of the Company's appetite for risk and their potential impact on the achievement of objectives and managed to an acceptable level
- The escalation of risk information is timely, accurate and gives complete information on the risks to support decision making at all management levels
- Risk is primarily managed by the individual business units transacting the activity wherein the risk arises, and the support functions such (e.g. airlines, credit control, IT, compliance,

shared services centre, business process improvement & audit, etc.) and reported to the Executive Risk Committee and The Risk Management Committee for oversight and mitigating action, if any.

- Employees actively engage in risk management within their own areas of responsibility and in a coordinated manner across the business units as mentioned above.
- Activities which may affect the Company's image, reputation or financial stability will be reported to the Executive Risk Committee and the Risk Management Committee.

Ownership

The Risk Management Committee of TCIL will have the overall responsibility for the risk management policy, framework and its effectiveness. An Executive Risk Committee [comprising the MD, the ED & CEO, the CFO, the Heads of Business Units (BUs), and the Head of the Business Process Improvement & Audit (BPIA) team] will be responsible for its implementation and day to day monitoring.

Applicability

This policy applies to all employees of Thomas Cook (India) Limited and every part of its business and functions.

Approval authority

This risk management policy and periodic updates to it will be reviewed and recommended by Risk Management Committee and subsequently approved by the Board of Directors of the Company.

2. Risk Management Committee

2.1 Composition:

The Risk Management Committee (RMC) shall have minimum three members with majority of them being members of the board of directors, including at least one independent director.

The Chairperson shall be a member of the board of directors and senior executives of the listed entity may be invitees/ members of the committee.

The Managing Director, the Chief Executive Officer, the Chief Financial Officer and the Head - Business Process Improvement & Audit shall be permanent invitees. The Company Secretary shall act as the Secretary to the Committee, whereas the Head of Business Process Improvement & Audit will be the rapporteur.

2.2 Quorum

The quorum for a meeting of the RMC shall be either two members or one third of the members of the Committee, whichever is higher, including at least one member of the board of directors in attendance.

2.3 Frequency of meetings

The RMC shall meet on a half yearly basis, and not more than one hundred and eighty (180) days shall elapse between any two consecutive meetings.

3. Risk Management Framework

The key elements of the company's internal risk management framework include

- Risk management structure
- Risk profiling
- Risk mitigation
- Risk monitoring and review

Risk management structure

Risk management structure provides effective management of risks by establishing appropriate reporting relationships and authorization protocols. It facilitates identification, assessment, review and monitoring of risks and controls at appropriate levels within the Company and also includes roles and responsibility of key levels defined in the risk management structure.

Risk profiling

Risk profiling is the process of creating an organization-wide repository of risks impacting the business objectives. This phase begins with risk identification, followed by risk assessment and finally recording / updating of risks in the risk registers for risk monitoring and review.

Risk identification

Risk identification refers to the process of recognizing both internal and external potential risk factors/events affecting the achievement of business objectives and includes identification of their root causes and existing/ planned mitigation measures.

Risk register

The risk register is a central repository of organization-wide risks. The purpose of the risk register is to record identified risks and related information in a structured manner. The risk register is a key document used to communicate the current status of all known risks and is vital for management reporting.

Risk assessment

Risk assessment refers to the process of quantification of Company's exposure to the risk on the basis of their impact significance and likelihood of occurrence. This is to assist the company in quantifying the risk exposures and prioritizing risks for management oversight and review. Refer Annexure 2 for Risk Evaluation Questionnaire.

Risk mitigation

Mitigation of risks involves managing the Company's exposure of various risks and bringing them in line with the risk appetite of the Company through avoidance, reduction, transfer or acceptance of risk.

Risk monitoring and review

Risk review involves re-examination of risks recorded in the risk register on a periodic basis with an aim to determine current exposure to the Company and to review the progress of risk mitigating actions/controls (Refer Annexure 1 for top External & Internal Risks). The progress of risk mitigating actions/controls is measured by evaluating the Company's performance on the Key Risk Indicators ('KRI') defined for every risk.

KRI are variances between budgeted and actual performance of various business activities and helps to determine the effectiveness of the control.

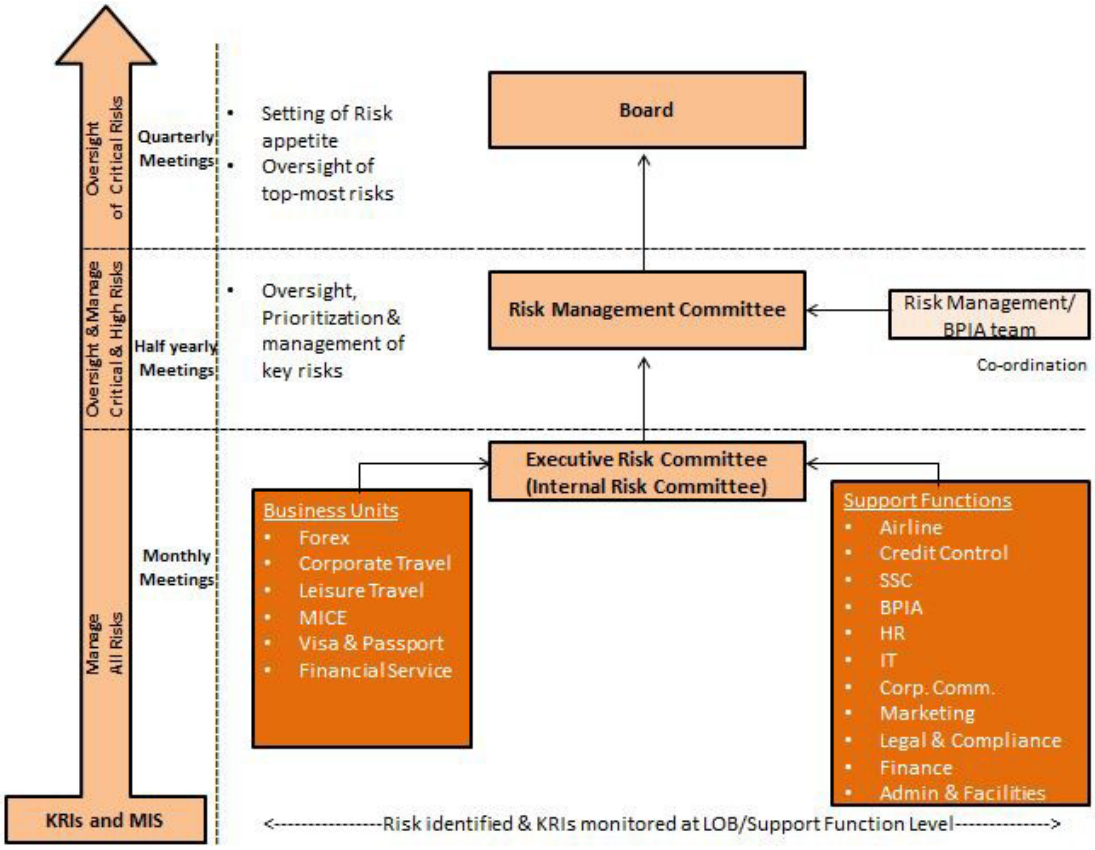
4. Risk management

4.1 Risk management structure

For the ongoing success of risk management, it is vital that the risk management framework is embedded into the Thomas Cook (India) Limited organization structure and aligned with its

corporate culture. Risk management must not be the task of one dedicated business unit or function, but rather is an explicit or implicit part of everyone's job description.

To facilitate the identification and communication of relevant risk information to the responsible decision-makers, the group has defined the following risk management structure, including roles and responsibilities at each level.



The Risk Management Committee, will co-ordinate with the Audit Committee (AC) and other committees, and will primarily be responsible for overseeing the risk management policies and framework. While the Risk Management Committee oversees the Company's risk management, the Executive Risk Committee, Business Unit / Support services Heads are responsible for day-to-day execution of the risk management framework. Head – Business Process Improvement & Audit will provide the necessary support to the aforementioned personnel in implementing the framework.

Roles and responsibilities

The risk management roles and responsibilities at various levels are as follows:

- Risk Management Committee
- Executive Risk Committee

- Head - BPIA
- Business Unit / Support Services Heads

Risk Management Committee

The Risk Management Committee provides overall guidance and oversight of the risk management framework and its governance within TCIL. It also reviews and approves the overall risk management framework and related policies.

Roles and responsibilities of the Risk Management Committee:

On an annual basis

- Review and approve the risk management framework, policy and structure (including changes thereto, if any, during annual reviews)
- Oversight on the effectiveness of the risk management framework
- Review of the reports of audits conducted - internal audits, concurrent audits, IFC audit, Secretarial Audit
- Review of the omnibus limits suggested by the management for transactions with related parties (RPTs)
- Approve risk management disclosures in annual filings/reports

On a half yearly basis

- Review critical risks and existing/proposed measures to manage these risks effectively
- Review the ratifications of the Sub-Committee on credit limits, and on RPTs, if any
- Provide inputs on any emerging critical risks

Power:

The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

Duties:

The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.

Executive Risk Committee

The Executive Risk Committee comprises of the MD, the ED & CEO, the CFO and Heads of Business & Support services. The MD is the Chairperson of the Executive Risk Committee.

The Executive Risk Committee is responsible for developing, implementing and maintaining an effective risk management framework within Thomas Cook (India) Limited.

Roles and responsibilities of the Executive Risk Committee

- Promote and foster a proactive risk management culture within the Company
- Responsible for managing current and potential risks within the Company and ensuring that risk exposures are within the acceptable risk thresholds of the Company.
- Review and monitor risks and measures to manage them effectively
- Evaluate and provide inputs on emerging risks emanating out of changes in business and economic environment. These risks need to be documented in the risk register and reported as per the reporting framework.
- Responsible for reviewing all projects/ decisions/ initiatives reported to the Executive Risk Committee for decision making as per the risk threshold.
- Review the cumulative exposure of the company and status of any new projects/ decisions/ initiatives.
- Ensure communication and implementation of risk management policies throughout the Company.
- Developing and providing recommendations to the Risk Management Committee on the following:
    - Risk management framework (including risk policy, risk threshold, risk management structure and roles and responsibilities)
- Define Key Result Areas ('KRAs') for the Support services and business unit heads, their direct reportees and line managers to ensure identification and mitigation of risks and strengthening of controls.
- Escalate critical risks and mitigation measures to the Risk Management Committee on a periodic basis (half-yearly) and also based on urgency of the risk materialization
- Advise BU/ Support service heads on risk initiatives and risk management strategy
- Develop and review the risk management disclosures which need to be made to stakeholders

The Executive Risk Committee shall submit a summary of the key

- Operational
- Financial
- Process
- Information technology including cyber security, and
- Compliance risks

assessed on a monthly basis along with the mitigation measures taken, to the Risk Management Committee for its review.

Meeting frequency

Head – Business Process Improvement & Audit (BPIA) meets the Executive Risk Committee on a monthly basis to review the top risks, and discuss the effectiveness of the risk management process.

The Chairperson of the Executive Risk Committee (i.e. The MD) seeks inputs from other Executive Risk Committee members on business risks, exposures and mitigation measures. The final decision making authority is with the Chairperson of Executive Risk Committee.

Minutes of Executive Risk Committee meetings (including agenda, decisions taken and attendance of Executive Risk Committee members) are maintained for each meeting by the Head – BPIA.

In every meeting, minutes of the last meeting along with an update on the status/ impact of the decisions taken earlier are presented.

Reporting relationship

On a half yearly basis, the Executive Risk Committee reports on the performance of the risk management activity and status of critical and high risks to the Risk Management Committee.

Head - BPIA

The primary role of the Head - BPIA in the risk management activity is to assist the Business Heads in establishing effective risk management in their respective areas of responsibility and

to monitor and report on the progress of the risk management activity to the Executive Risk Committee.

Roles and responsibilities of the Head - BPIA

- Developing risk management policies, including defining risk management structure, risk threshold, KRI and evaluating mitigating controls
- Assisting the Executive Risk Committee and BUs/ Support Service in implementing risk management policy across the entire Company
- Assisting the BUs/ Support services in conducting risk assessment for their respective units/ locations and help risk owners align risk responses with the Company's risk appetite
- Establishing a common risk management language across Thomas Cook (India) Limited that includes common measures around likelihood and impact, and common risk categories
- Reviewing quality of risk profiles including performance against KRIs, root cause and suggested action plans from across BU/ / Support services and provide quarterly performance report to the Executive Risk Committee
- Reviewing the risk thresholds/ levels which various business segments would have considered for existing/ new risks
- Ensuring necessary training for risk management, incident capture and self-assessment is arranged for all risk / control owners
- Ensuring that appropriate information regarding risks and controls is provided to the Audit Committee, in conjunction with the Executive Risk Committee
- Maintaining awareness of trends and developments in risk management that are significant to Thomas Cook (India) Limited
- Reviewing the internal audit, concurrent audit, and IFC audit findings and link the same to the various risks noted as part of the risk management exercise to understand the impact of the same.
- The Head of BPIA shall also act as Risk Coordinator and shall have the following additional responsibilities:

    - The management, update, and development of this Risk Management Charter/Policy.

    - Reporting on a periodic basis, a Risk Management Report to Risk Management Committee, which includes:

- The consolidation of Segment wise Key Risks.
- Reporting on the implementation of the Risk Management Processes.
- Reporting on high risk issues and changes in risk.

- The continuous improvement of the Risk Management Process and
- Act as a rapporteur for the Executive Risk Committee and the Risk Management Committee

Meeting frequency

- Monthly - presentation of organization wide key risks and related matrices such as credit, market, financial, operational, Information technology including cyber security, compliance, etc to the Executive Risk Committee
- Half yearly – Risk management presentation to the Risk Management Committee, and through it, to the Board
- Event based – Review risk registers and KRI information along with the BU / Shared Services Units heads and responsible individuals within the team in case of sudden escalation / new risk identification / escalation.

Deliverables

- Collate the risk / KRI information from across BUs/ Support services (through the respective risk officers within the BPIA team) and report on the status of critical and high risks to the Executive Risk Committee on a quarterly basis
- Updates to the Executive Risk Committee on the action plans for critical and high risks identified
- Update to the Risk Management Committee on critical risks identified on a half yearly basis
- Through the internal, concurrent, and IFC audits, report and manage key risks identified with the guidance of the Executive Risk Committee and the Risk Management Committee.
- Suggest changes to the risk management policy, risk threshold, risk management structure and KRIs, basis any changes to the internal or external operating environment of Thomas Cook (India) Limited.

Reporting relationship

- Monthly reporting to the Executive Risk Committee
- Half yearly reporting to the Risk Management Committee and quarterly reporting to the Audit Committee
- Escalate any critical and significant incidents to the Executive Risk Committee.

Business Unit / Support Services Heads

BUs/ Support Services Heads are primarily responsible for reviewing and managing business, operational, financial, IT, and compliance risks within their respective BUs/ Support services. They are also responsible for implementing and ensuring effectiveness of action measures/ controls to mitigate risks as well as for reviewing all projects/ decisions/ initiatives reported to them for decision making as per the risk threshold. Typically, the BU/Support Services that would showcase the risks emanating out of their units would be:

- **Procurement**– risks related to
    - Airlines
        - Procurement
        - Deposits
        - Forfeitures
        - Accruals and
        - PLB receivables
    - Hotels
        - Procurement
        - Deposits
        - Forfeitures and
        - Receivables
    - Other vendors
        - Procurement
        - Deposits
        - Forfeitures and
        - PLB receivables
- **Credit Control**
    - Debtors and Creditors
    - Credit approvals, including monitoring and ratification
    - Non/delayed collection of receivables
    - Industry specific exposures and risks thereof
- **Shared Services Centre**
    - Reconciliations
    - SLAs
- **Compliance** -
    - Regulatory compliance
    - Timeliness of adherence
    - Transactions with Related parties - risks of not being in the ordinary course or at an arm's length or without prior approval, where required

- **BPIA**
  - Process risks
  - Fraud risk related matters
  - Business continuity planning
  - Risks identified during internal, concurrent, and IFC audits that may have operational, financial, and compliance aspects
- **IT risks**
  - Information security
  - Cyber security
  - System and Process risks
  - Network and Infrastructure issues
  - Applications

Others - any other operational risks not covered above, legal & reputational risks, financial stability, etc, in discussion with members of the Executive Risk Committee including the MD, CEO, CFO, etc.

Roles & responsibilities of BUs/ Support Service Heads

On a monthly basis

- Update the Executive Risk Committee on the:
  - Status of implementation measures and effectiveness of existing controls
  - Need to implement additional measures to reduce risk exposures to an acceptable level
  - Measure their risk management performance as per the defined key risk indicators and also update the status for key risk indicators
  - If any risks have materialized, reasons for the same and action plans to be implemented to strengthen the mitigation measures
  - Potential of any risk materializing in the near future which has a major impact for the Company
- Ensure adequate risk assessment is done for all key strategic initiatives in the respective BUs/ Support Services
- Capture and report all risk incident data such as breaches, near misses, etc at the executive risk management committees
- Provide KRI data to the Risk Committee (the composition of Executive Risk Committee shall be defined by the MD) for the review

On an annual basis (normally during annual business plan process)

- Ensure that a detailed risk assessment is conducted through Head - BPIA across their business unit to identify business, operational and compliance risks.

Event based

- Business Heads shall escalate critical and high risks immediately to the Executive Risk Committee and the Head - BPIA.

Meeting frequency

The BUs/ Support Service Heads to meet on a monthly basis with Head - BPIA to review the risk register and any additions / deletions to the risk register along with changes in residual exposure of risks.

Deliverables

- Updated risk register
- Assessment of risks
- Implementation status of agreed mitigating actions/ controls
- Any new risk identified or incident occurred during the period to be recorded and escalated or reported according to the significance of risk/ incident

Reporting relationship

- For all purposes of risk management, the BUs/ Support Service Heads shall report to the Chairperson of the Executive Risk Committee

4.2 Risk profiling

Thomas Cook (India) Limited performs an annual risk and control identification, assessment and prioritization exercise as part of the risk management framework. Activities involved in the annual risk identification, risk assessment exercise, and risk prioritization are described below.

Annual risk identification, risk assessment exercise, and risk prioritization

Risk identification

On annual basis, each BUs/ Support services Head will conduct a review of current state of operations to identify risks facing their BUs/ Support services. Risk identification will begin with an understanding of the business objectives that the BUs/ Support service Heads are

responsible for and also the strategies that have been adopted to achieve company's objectives. Each risk that threatens the achievement of a business objective will be entered in the risk register.

Risk identification is carried out using:

- Risk interviews and brainstorming sessions
- Risk questionnaire
- Analyzing the audit reports and other external reports, if any

Audit reports and external reports **–** Risks relating to the Company or BUs/ Support Services can also be identified through internal, concurrent and IFC audits as per the audit plan approved by the Audit Committee at the beginning of the financial year. These reports must be reviewed by the Head - BPIA on quarterly basis. Risks with significant impact identified in these reports are to be discussed with the respective BUs/ Support Service Head, and presented to the Executive Risk Committee, and the Risk Management Committee for their review.

Based on the risks captured in the risk registers and discussions with the BUs/ Support Services, the Head - BPIA will collate a list of key risks (considered high on residual impact) across the organization which will be rated in the risk assessment exercise.

Risk assessment

A risk assessment exercise is conducted annually to rate the key risks from each BUs/ Support Services, on their possible 'impact' and 'likelihood of occurrence'. Risk assessment is done by a group of senior management participants who represent different business/ functions within Thomas Cook (India) Limited

The key participants of the risk assessment exercise are -

- Managing Director
- ED & CEO
- Chief Financial Officer
- Heads of business units & Support Services
- Any senior management personnel as deemed necessary

The main objectives of this exercise are to;

- Improve risk transparency and promote common understanding of risks
- Assess the significance of each risk for achievement of business targets
- Rate and prioritize risks based on their impact and likelihood

- Identify and evaluate existing and planned risk handling measures and develop new measures
- Update the Executive Risk Committee and the Risk Management Committee on the above

Risk prioritization

Risks presented for rating in the risk assessment exercise are prioritized on the basis of the residual exposure. Higher the residual exposure, higher the risk priority. The objective of prioritizing risks is to map categorize risks identify organization-wide top critical risks which need to be escalated to the Risk Management Committee.

4.3 Risk mitigation

Options for risk mitigation at Thomas Cook (India) Limited:

- **Risk avoidance –** Exiting the activities giving rise to risk
- **Risk reduction –** Design controls to mitigate the risk in terms of its impact or reduce the likelihood of its occurrence (e.g. hedging, business continuity planning)
- **Risk transfer –** Design measures to transfer the risk on to a third party (e.g. insurance, sub-contracting)
- **Risk acceptance –** Accept risk in cases where either additional risk management measures are not cost effective or risks which are inherent to the business model and TCIL has a low degree of control to influence the risk

4.4 Risk monitoring and review

- An enterprise-wide integrated Risk Management reporting framework is implemented by the Company.
- Such information is needed at all levels of the organization to identify, assess and respond to future occurrences of risk events. Pertinent information from both internal and external sources is captured and shared in a form and timeframe that equips management to react quickly and efficiently.

Annexure 1 – Risk Register for Top Internal and External Risks

Sr. No.	Risk/Type (Internal/External)	Description
1	Natural/man-made Disaster (External)	Critical business processes may be impacted in the ***event of a natural*** (e.g. floods, earthquake) ***or man-made*** (e.g. fire, terrorist strike) disasters ***affecting delivery locations***. Web enabled centralized dynamic packaging system covers all travel related services on real time basis and hedging of foreign exchange exposure is also dependent on the real time updates of the foreign exchange rates. Any ***technical or internet connectivity failure may have adverse effect on business***
2	Credit (Internal)	Default or delay by clients on outstanding payments on account of ▪ Liquidity / bankruptcy / going concern issues at client-end (Business Travel / FFMC) ▪ Dissatisfaction with services rendered (all BUs) ▪ Delay in / inaccurate invoicing process
3	Attrition (Internal)	Attrition of ***key*** personnel or attrition of ***significant count*** of team members can disrupt normal business operations. A key vacancy open for long time can be a ***hurdle for business to achieve its objectives***. Absence of tracking mechanism for employee satisfaction or employee retention program can lead to high level of attrition over a period of time, while an entry of a competitor in an area where TCIL is a major player can bring sudden spike in attrition.
4	Fraud (Internal/External)	Frauds by employees / outsourced staff / channel partners can bring ***financial / reputational loss*** to the organization. Business units can be affected by mis-appropriation of cash / cash equivalents or misuse of customer credit card details / documents. Corporate travel is exposed to unauthorized / personal ticket bookings or misuse of corporate credit cards etc.
5	Financial resilience (Internal)	Financial resilience is essential to run day to day operations. Working capital challenges may arise due to unavailability of credit from banks, bad debts, high outstanding period, high cost short term lines of credit because of drop in credit rating or sudden capital expenses for organic growth or merger & acquisition activity.
6	Health & Safety (Internal/External)	Managing risks to health and safety is critical to ensuring a safe workplace and also to comply with ***statutory requirements***. Health & safety incidents can lead to loss of productivity / increase ***customer dissatisfaction and***

		ultimately affect the bottom-line of business. The risk can arise for lack of defined health and safety policy or inadequate fire safety / physical security measures.
7	Data Confidentiality (Internal/External)	The organization holds ***customer's confidential data*** either in form of their demographic details, travel plans or physical documents submitted for visa processing. The data exchanges many hands involving employees and outsourced staff. ***Disclosure of sensitive data*** can result in financial / reputational loss / regulatory action due to identity theft, lawsuits, leakage of leads to competition etc. The risk can arise because of absence of appropriate information security policies / procedures, inadequate restrictions on access to confidential data by employees and absence of monitoring / detective mechanisms
8	IT Infrastructure & Cyber Security (Internal/External)	IT infrastructure like servers, networking systems or legacy applications may not keep pace with technological advancements. The ***effects of IT obsolescence*** may be aggravated by the declining manufacturer support and skill base required for modifying system components ***to meet evolving user requirements***. The obsolescence risk may arise because of unavailability of funds for replacement or because application development is not with latest / sustainable technology. There could be ***migration risk.***
9	Business Concentration (Internal)	Since some business units are dependent on few clients / industries for significant portion of their revenues, any ***loss of major client or economic*** / regulatory changes in particular industry may impact the revenues.
10	Insurance Coverage (Internal/External)	Risks are integral to opportunities and threats which may impact the expected outcome. Insurance is a mechanism through which firms can reduce negative financial consequences of an uncertain event or possible financial loss. However, ***adequate insurance policy*** and cover if not solicited may result in ***financial losses.*** The covenants of insurance policy if not adhered to may result in claim rejection
11	Product & Services Development (Internal)	For sustainability / growth in market share or revenue, it is important that the ***products & services constantly meet the customer requirements***. Absence of defined procedure involving marketing, sales, operations and commercial team, absence of competitor tracking mechanism, loss of early mover advantage, failure to leverage latest technology advancement ,Inability to deliver quality product/services or absence of capturing / review mechanism of customer complaints may ***lead to loss of market share or revenue***

12	Pending litigation (External)	Pending litigations may impact the ***profitability*** if they are ruled against the organization. The litigation can be filed either by the customer, regulator or government agencies or the organization as plaintiff. The absence of an adequate process for reporting new litigations or a process for timely response to / management of notices / litigations may ***lead to financial penalties against the organization***
13	Outsourcing partner/Vendor (External)	The recognized benefits of outsourcing include increased efficiency, controlled costs and an improved focus on core business activities. However, ***inappropriate selection of service provider*** can increase the risk and the cost for the organization. Outsourcing if not managed well, may lead to lengthy step of vendor selection, a longer (3-12 month) timeframe to complete work handover to the service provider, severance and costs related to layoffs of local employees who will not be relocated
14	Mergers & Acquisition (External)	A successful mergers & acquisition activity can provide immediate inorganic growth to the organization but ***a failed one can be a drain on resources***. An important factor of M&A is conducting due diligence which is often limited only to the verification of the financial reports of the acquired company. Some external factors threatening the ***success of an acquisition*** could be economic / political situation while internal factors may include different management styles, differences in system & processes or attrition of key employees of the acquired entity
15	Foreign Currency Exposure (External)	***Movement of foreign exchange*** and time lag between receipt and payments in different currencies, may positively or ***negatively impact*** the performance of several business units Hedging efficiency/ inefficiency may affect the business. (Travel Business)
16	Record Retention (Internal)	The organization may ***not be able to retrieve or retain the data required*** for statutory / regulatory / business purpose on account of absence of record retention policy highlighting the tenure for which records are to be retained, de centralized storage of customer / vendor contracts or absence of / inadequate back up for IT applications
17	Regulatory & Legal Compliances (External)	The company is required to ***comply with statutes***, laws, regulations of governing bodies in its working environment and RBI guidelines for its forex business. The company currently requires various approvals, licenses, registrations and permissions for operating its businesses. Any failure to obtain / renew / comply with requirements of these approvals/

		licenses ***may lead to license suspension or cancellation***. Similarly, non-adherence to contractual requirements with clients / suppliers may results in ***litigations / financial losses***
18	Outsourced Staffs/Channels (External)	Outsourcing gives organizations an opportunity to gain efficiencies, improve performance, ***lower costs and focus on core competencies***. If the organization fails to conduct appropriate due diligence or does not implement an on-going monitoring and reporting mechanism for outsourced staff / channels, can be ***exposed to service delivery failures, regulatory non-compliance or data protection / privacy breaches.***
19	Marketing (Internal)	Many players have entered the market both in the online and offline space. In order to protect existing market share or capture market share, TCIL may be required ***to judiciously and efficiently use its advertising and promotion expenditure***. Effective promotion and positioning of TCIL brand will depend largely on the success of marketing efforts.
20	TCIL/Third party IPR (Internal/External)	***Inadvertent misuse / violation*** of intellectual property rights (IPR) of third-parties by TCIL on account of inadequate awareness of IPR amongst employees. Similarly, ***TCIL's IP rights may be violated by third-parties*** if not identified, monitored and protected appropriately. ***Non registration of trademarks can allow any person to use a deceptively similar mark*** and market its product which could be similar to the products offered by TCIL.
21	External Representation/Investor Grievance (External)	External representations made to clients / investors / market by authorized / unauthorized persons ***may be inaccurate or misinterpreted leading to reputation damage or even litigation***.
22	Code of Conduct (Internal)	A defined code of conduct and its adherence is vital for any business. The code of conduct guides all managerial decisions, creating a common framework upon which all decisions are founded. The code of conduct should be applicable to all stakeholders including employees, vendors and outsourced staff. ***Any breach of the code can expose the organization to liabilities.***
23	Idle Funds (Internal)	Improper / ***inefficient investment of surplus funds*** as result of (a) absence of a defined investment policy / guidelines (b) improper selection of investment instruments or (c) operational challenges in investing surplus funds. Cash also has an "opportunity cost" and therefore the organization should review the options available for ***maximizing the***

		value of surplus cash
24	Branding/Reputation (External)	To strengthen and manage the perceptions of the business a strong brand is needed. TCIL may face challenges an event which may cause material damage to the Trademarks and which has not been remedied within a period of 180 days
25	Social Media (External)	Rising importance of social media provides TCIL an opportunity to connect better with end-customers and improve market visibility, but also provides dissatisfied end- customers or persons with malicious intent to publicize their discontent, which may result in a ***negative impact on branding / reputation***.
26	Mis-selling (Internal)	Product mis-selling may lead ***to customer dissatisfaction*** and even legal cases involving compensation payout. Inadequate product information or stretched sales target may lead to mis-selling.
27	Disintermediation (External)	The increasing penetration of the internet coupled with online payment solutions, has given rise to the phenomenon of 'disintermediation', whereby service providers, i.e. airline companies / hotels, etc. ***enter into direct dealings with a prospective customer as opposed to dealing with travel service integrators***. Reduction / elimination in airlines commission may impact Corporate Travel unit. Introduction of biometrics by consulates may impact visa business
28	Suppliers & Vendors (External)	The business makes the company dependent on travel agents / hotels and airlines. The company normally enters into short term agreement with the suppliers for their services. The contracts with these suppliers/vendors when either not renewed or renewed at ***non favorable rates*** may adversely affect the business, operations and profitability. The suppliers / vendors may ***fail to provide the services as per the contract***. The company faces claims / liabilities / suits from customers should they perceive any deficiency in service or in the event of bodily harm / injury to them while on the tours organized by us through suppliers / vendors

Annexure 2 – Risk Evaluation Questionnaire

This questionnaire is intended to focus on the top current and emerging risks that could negatively and materially impact the business, despite the mitigation processes in place. It is the responsibility of MD, the ED & CEO, the CFO and Heads of Business & Support services to assess these risks on their probability of occurrence and their impact, on a scale of 1-4, with 1 being the lowest and 4 being the highest. Basis the inputs from management on these risks, the risks will be categorized from highest to lowest in terms of their ability to impact the company.

TCIL Risk Evaluation Questionnaire-FY21-

Abbreviations:

TCIL	Thomas Cook (India) Limited
AC	Audit Committee
RMC	Risk Management Committee
MD	Managing Director
ED & CEO	Executive Director and Chief Executive Officer
CFO	Chief Financial Officer
BU	Business Unit
IE	Inherent Exposure
RE	Residual Exposure
KRI	Key Risk Indicators

Glossary:

Business Continuity Plan (BCP): BCP is a set of protocols that how the company will continue and overcome a business disruption caused by an emergency. It outlines a range of disaster scenarios and the steps the company will take in any particular scenario to return to regular business/trade.

Credit Risk: Credit Risk is the risk of loss due to a customer's failure to make payments on any type of outstanding payments.

Compliance Risk: compliance risk is the risk posed to the company's financial, organizational, or reputational standing resulting from violations of laws, regulations, codes of conduct, or company policies.

Financial Risk: Financial risk is the risk which is associated with financing, including financial transactions that include company loans & advances in risk of default.

Information Technology (IT) & Cyber Security Risk: IT & Cyber Security Risk is the risk that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability. It includes:

(a) Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
(b) Unintentional errors and omissions
(c) IT disruptions due to natural or man-made disasters
(d) Failure to exercise due care and diligence in the implementation and operation of the IT system

Market Risk: Market risk is the risk of losses in positions arising from movements in market variables like prices and volatility.

Operational Risk: Operational Risk is the risk of loss resulting from inadequate or failed processes, people and systems risks. It includes legal risk but excludes strategic and reputational risk.

Reputational Risk: Reputational risk is the risk that some negative circumstance could negatively impact reputation and image of the company and its brands in the marketplace.

Residual Risk or Residual Exposure (RE): Inherent risk/exposure is the risk to an entity in the absence of any mitigating controls. The remaining likelihood and impact of a particular inherent risk/exposure after management has taken action plans by way of instituting controls to alter the risk's likelihood or impact is called as residual risk. Where the Company has implemented effective controls to mitigate risks, the residual risks refer to risks after controls or "net risks".

Strategic Risks: Strategic Risk is the risk associated with initial strategy selection, execution, or modification over time, resulting in a lack of achievement of overall objectives of the company.