



# Critical Operational Risk Coverage

## The Ceylon Tobacco Experience

By Shirani Jayasekara FCA FCMA

**I**t is now recognised that poor management of risks, especially non-finance risks are decline drivers of profit and market capitalisation. Poor demand forecasting, poor management of supply chain and logistics, regulatory conflicts, poor IT integration are some of the more significant of non-financial risks.

Fundamental changes in Company law and governance requirements have brought in renewed attention to risk management which is gaining interest at Board level. Risk management is a senior management responsibility, which is often overlooked. The best risk information comes from those closest to the business. There must be a process in place to extract and capture this very pertinent risk information, which could at times be crucial to the success of a business operation. Management may not sometimes be equipped with the proper skills to clearly articulate or specify the risk implications. A broad framework or risk management methodology therefore is an important tool to make risk management a reality.

CTC encourages all staff, not just senior management to get involved in identifying and mitigating key business risks that may arise in

their respective business units. This is simply a self assessment technique that enables staff involved in a business area; or a team given responsibility for delivering on a project; to jointly identify the risks they face in achieving relevant objectives.

CTC has been influenced by the COSO (Committee of Sponsoring Organisations of the Treadway Commission) ERM framework which considers activities at all levels of the organisation, at Entity level, Division or Branch level, business unit level or at process or project level.

COSO defines its ERM framework as "...a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."<sup>1</sup>

Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. Both quantitative and/or qualitative aspects need to be considered. Any risk event which falls outside of the risk appetite line needs to have mitigation plans.



The COSO framework has been adopted by CTC with a spotlight on managing operational risk. The components are:

1. **Internal environment** - set by culture, internal policies, checklists and procedures
2. **Objective setting** - set by the top team after consultation with wider management
3. **Risk event identification** - identified by those closest to the business
4. **Risk assessment** - a quarterly agenda item at leadership meetings
5. **Risk response** - mitigation plans to risk items within risk appetite. Response options are; Accept, Avoid, Reduce or Share.
6. **Control activities** - carried out by the respective functions when implementing the mitigation plan
7. **Information and communication** - communication to stakeholders
8. **Monitoring** - review by the Board and independently by Audit

Some of the processes and practices adopted by CTC are highlighted below:

#### Internal environment

CTC embraces a solid internal environmental framework and has entrenched the values in all of its internal processes. The HR policies and employment principles cover areas such as induction of new recruits, non discrimination, promotion and pay, standards of business conduct, information security, social responsibility etc. These all form part of the culture, internal environment and acceptable ways of working.

#### Objective setting and Risk

Business Risk is defined as ‘any event, situation or circumstance which, if it occurred would adversely impact the achievement of objectives, including the failure to capitalise on opportunities’. Risk management is a process which seeks to reduce the likelihood of occurrence and the severity of loss, by proactive identification and application of mitigating controls to minimise the adverse impact on the business and its assets.

Effective risk management is possible where there is good business understanding at senior management level and all strategies are aligned to the overall mission or prime objective. Communication of a common and strong message is a key element to success in this.

#### OBJECTIVE SETTING AT CTC



### Event identification

This is all about identification of external and internal events that could impact on business objectives and therefore need to be managed.

External - Some of the generic external risks being managed are:

#### Natural disasters

The threat of natural disasters is considered to be mainly from fire, water and lightning. Fires have been infrequent in cigarette manufacturing plants. However, there is a potential for fires, primarily due to the combustibility of the materials used both within the contents of the cigarettes and the packaging materials.

Mitigation plans include automatic fire detection systems in storage areas, sprinkler protection throughout the cigarette manufacturing and storage areas, emergency response procedures and response teams set up to provide prompt fire response backed by nearby public fire brigades. Flood water pumping systems are triggered when waters in flood risk areas reach a certain level.

The residual risk is covered by insurance.

#### Regulatory conflicts

CTC supports the new law enacted to regulate the Tobacco Industry. Whilst abiding by the regulations stipulated under the National Authority on Tobacco & Alcohol Act No. 27 of 2006, The public was informed through several press notices, that the company supported the compliance of the provisions of the Act. Regulatory conflicts arise due to misrepresentation of the law and these need to be managed on a timely basis.

#### Competition

CTC is still the only legal player in the tobacco market in Sri Lanka. However the Company is aware that there are many unauthorised players in the cigarette industry and must rely on the enforcement authorities to manage this situation. A Steering Committee comprising members of the top team has been set up to review competitor activity. The loss of revenue to government due to the illegal trade is significant as these players do not pay excise and relevant taxes.

Internal - Some of the internal risks that are being managed are:

#### Demand forecasting

The Company has a 12 month rolling forecast driven by consumer demand. This is broken down to sales and operations plans in the shorter term

with defined tolerances set for the 3 month horizon. Deviations from tolerances are reviewed by a team of senior managers by means of a colour coded dashboard, as they would have implications on working capital.

#### Operational risk

Industrial relations, within our operating environment, can be considered as the key driver to success in managing operational risk. This has created a conducive environment for people to get involved in productivity and quality improvement activities.

Any disruption to regular supply of material leads to considerable risk in a manufacturing organisation. Contingency supply plans are available for the all global and key local suppliers of wrapping materials.

Also, we have established an integrated management system covering both quality and environmental aspects and both systems are accredited as per ISO 9001: 2000 and ISO 14000: 1996 standards.

**Any disruption to regular supply of material leads to considerable risk in a manufacturing organisation.**

#### IT integration

IT systems development is handled centrally (regionally) through use of common platforms. These are rolled out to the operating companies on a phased out basis. IT related risks therefore are common and can be more easily controlled, than if the systems or their implementation were decentralised.

Global IT auditors periodically audit the systems and processes working on a risk based IT Audit plan.

IT Disaster Recovery plans and processes are in place and tested.

#### People development and succession planning

A robust and ongoing career development process manages the human resource risk. Each managerial position within the organisation has identified successors and plans are in place to develop individuals who would be taking up key roles. This would manage the risks of unplanned employee exits.



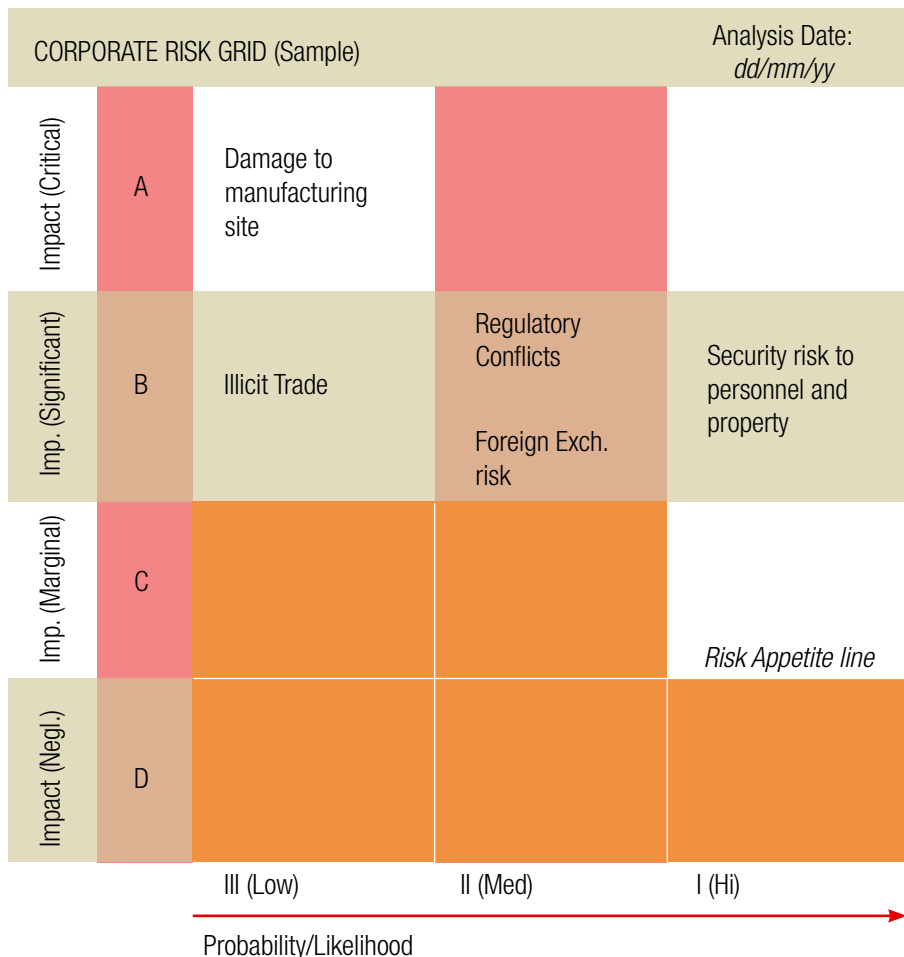
### Risk Assessment

Risks are analysed, considering likelihood and impact as a basis for determining how they should be managed.

Risk radar screen - ongoing surveillance

Initial risk identification, debate and discussion takes place at Departmental level. On a quarterly basis senior management review same and pick up those significant risk events which are beyond the risk appetite line and therefore need more attention and necessitates central management. The Audit Committee reviews the corporate risk grid and

**Effective risk management is possible where there is good business understanding at senior management level and all strategies are aligned to the overall mission or prime objective.**



#### Impact

- A - Critical - 2 or more Co priorities/Obj impaired/ x% of PBT
- B - Signif - Affecting One Co priority/PBT Rs y to Rs x)
- C - Marginal - Co priorities threatened
- D- Negligible - No effect on Priorities at moment

#### Probability/Likelihood

- 1 - Hi already happening (high frequency)
- II - Happens. Some of the critical causes exist for event to occur
- III - Belief that event can take place

## Externally reporting takes place with communication through reporting to its stakeholder to give them an understanding of the risk management process.

discuss for inclusion any threats or vulnerabilities emerging in the external environment. This top down and bottom up practice, serves to integrate and embed risk management practices throughout the organisation, in addition to providing good company wide business awareness.

### Risk Response

Risks cannot always be eliminated. Depending on the severity of the risk, management may choose to Accept, Avoid, Reduce or Share the risk. Management needs to align the risk response with the entity's tolerance levels and risk appetite. Risks must be managed and controlled to an acceptable level, so that the residue risk after management lies within the risk tolerance level of the company.

### Control activities

#### a) Normal Business Operations

Control activities can take place in 3 areas. Embedded Controls in processes, Mitigation controls against the Risk Grid and managing risk logs on Programmes or Projects.

#### b) Crisis Management and Business Continuity Planning (BCP)

Any company can have at any time an unexpected incident, which needs to be managed before it becomes a crisis or worse, into a disaster, if not managed at crisis level. A crisis situation may be a temporary interruption in one small area, which if not managed (as in a electrical spark which started a fire and spread to other areas of the premises) affect many areas of the business, resulting in a significant loss. At times it may be just a loss of access to the manufacturing site, office environment, computer facilities or resources that are used in normal operations.

A Crisis Management Team was set up to develop plans of action at functional level, to enable that Function to resume their current business operation in the shortest possible time.

### Information and Communication

COSO suggested that relevant information should be identified captured and communicated in a form and time frame that enable people to carry out their responsibilities. Risk reporting and communication process incorporates an internal and external process. Internally the board of Directors is briefed about, approach taken to manage risk, top ten risks of the organisation, readiness of the organisation to manage a crisis, management of key projects etc.

Externally reporting takes place with communication through reporting to its stakeholder to give them an understanding of the risk management process on a regular basis to uphold the confidence levels placed on achieving business objectives. The good governance practices adopted demonstrate that a methodical approach exists, thus ensuring that members of the board effectively discharge their duties in building shareholder value and monitoring performance on an ongoing basis, in the interests of the shareholder.

### Monitoring, Oversight and Periodic Review

As demonstrated above there is a continuous and robust process of monitoring managing and reporting on risk at CTC. Active feedback is given to the Non Executive Directors at each Audit Committee meeting. Valuable input is received by the NEDS, with the knowledge skills and experience they bring in, from outside of the tobacco industry. There a periodic review of the process itself by Audit.

Audit can play a significant support role, by developing an audit plan which makes use of risk identification tools and processes.

The Audit plan should:

- balance risk related reviews, testing of financial controls, and operational effectiveness
- make use of the risk register and risk information by management
- be structured to respond and adapt to the emerging and changing risk environment.

It may therefore be said that as the risk vs. objectives is carefully considered collectively, by the power of three viz; management, audit, and the Board, there is a better chance of meeting corporate objectives.

<sup>1</sup>COSO Enterprise Risk Management – Integrated Framework 2004. COSO

*The writer is the Audit Manager of the Ceylon Tobacco Company Ltd.*