

Title: Risk Management Analysis in SmarTech

Table of Contents

Title: Risk Management Analysis in SmarTech	1
Policy Purpose and Objectives	3
Scope	3
Policy Principles	4
Roles and Responsibilities	7
Risk Management Framework	10
Business Risks	11
Risk Management and Compliance Structure	11
The Risk Management Framework	13
Risk Management Process	13
Risk Assessment-Likelihood Scale	14
Recording the Risk Management Process	16
Stakeholder Analysis	16
Communications Plan	17
Industry Analysis	18
Risk Assessment Template	18
Risk Treatment and Action Plan	19
References	22

Policy Purpose and Objectives

The Telecommunications sector has some specific characteristics, like vast infrastructure requirements, robust competition, and very short turnaround times for threats identifications, including their subsequent assessments, and mitigations of associated risks in order to minimise network downtime. However, organisations in the telecom sector are constantly looking for methods and solutions to streamline their processes as a means of reducing organisational risk. Therefore, towards this end organisations, like SmarTech, want to face challenges, by reducing silos, and ensuring consistent information across channels and training agents to handle queries.

Scope

Great troubles, in terms of economic recession, have been implied for a lot of companies during market globalisation and the ongoing world economic crisis. Further, more complexities have been faced while combining the global development with the needs of the local context adaptation due to difficulties in international partnerships and credit crunch. Since the change in critical success factors and enlargement of firm relations are essential elements of the global competition, therefore risk management becomes more important for assuring long-term effectiveness. The analysis of risk management is closely related to the safeguard of the stakeholders' interests, sustainable development, and integration among social, economic, competitive, and environmental success (Brondoni, 2010, pp.12). In SmarTech, the policy is consistent with the international standard AS/NZS ISO 31000:2009 and to ensure a good management plan, the risk managers set up priorities and assists in providing comprehensive management efforts. In this process SmarTech reframe their journey into four stages of maturity, which are depicted below-

(0) Initial
Transparency
Stage

(1) Systematic
Risk Reduction

(2) Risk-return
Management

(3) Risk as Competitive
Advantage

Drivers

<ul style="list-style-type: none">• Compliance with basic standards/regulations• Reduction of regular surprises	<ul style="list-style-type: none">• Avoiding unexpected large loss events• Stability to enable growth plan• Professionalised Management	<ul style="list-style-type: none">• ROE¹ improvement requirements• Competitive pressure• Navigating trade-offs	<ul style="list-style-type: none">• Top management focus on risk-adjusted performance• Finding niche in mature marketplace
--	---	---	---

Key Tools

<ul style="list-style-type: none">• Opportunistic approaches	<ul style="list-style-type: none">• Risk heat map based on consensus assessments	<ul style="list-style-type: none">• At-risk measures (e.g. VAR², CFAR³)• Systematic scenario analysis of profit and loss	<ul style="list-style-type: none">• Strong risk culture• Unbounding risks through contracting and markets
--	--	---	--

- 1- Return on Equity
- 2- Value at risk
- 3- Cash flow at risk

Through these approaches the prudent managers at SmarTech want to minimise their exposure to potential risks and at the same time maximise savings and opportunities. The telecommunication sector, mainly deals with minimising, controlling, and preventing the potential costs while implementing Risk Management policy (Brondoni, 2010, pp.19).

Policy Principles

SmarTech is committed to provide adequate and reliable essential telecommunications to all aspects of contemporary community life, from supporting the State's economy to creating and maintaining connected and cohesive social networks. The basic objective of this business organisation is to apply telecommunications and related technologies to general business operations to satisfy business needs. In order to play the role

of a global competitive player, the risk managers of SmarTech are obliged to create a plan that will help the organisation in attaining its objectives, but prevent the risk associated with it in terms of policies, laws of other countries, or the consumer needs of the product and service.

The planning policy of this organisation is aimed at balancing the need for effective telecommunication services with the efficient roll-out of networks, together with protecting the community interest in local areas (ISO/IEC: Information technology, 2008). The policy and underlying principles will be reviewed annually by the Board to ensure its continued application and relevance-

- In order to accomplish business objectives, risks must be considered and managed enterprise-wide
- Risk management is integral to the strategic planning process, business decision making, and day-to-day operations
- Risks are identified, analysed, responded to, monitored, and reported on in accordance with SmarTech's policies and procedures
- Risk responses must be tailored to each particular business circumstance
- Management must regularly assess the status of risks and risk responses
- Compliance with the Enterprise Risk Management Framework must be monitored and reported

The objective of risk management plan is to provide a formal process to assist SmarTech in-

- Penetrating into the Australian smartwatch market by identifying and managing risks associated with SmarTech's future strategic plans (Oppliger, 2011, pp.22)

- In order to ensure the identification of potential risks, assessment against accepted criteria, and establishment of necessary control measures, the relevant procedures should be developed and implemented
- Competitive advantage can be availed by providing vital input for the feasibility study in terms of project viability, resource allocation, and understanding opportunities which helps in shedding light to the changes and threats that SmarTech will face
- The critical risks can be appropriately managed only by providing assurance to the Executive Team, Board Members, and all other stakeholders (ISO/IEC: Information technology, 2008)

Like any other organisation, SmarTech also has risk management plans, in which a risk strategy includes. However, the project may choose from four potential risk strategies, with numerous variations-

- i) Avoid risk- Change plans to circumvent the problem
- ii) Control/Mitigate Risk- Reduces impact or likelihood (or both) through intermediate steps
- iii) Accept Risk- Take the chance of negative impact and then eventually budget the cost, through a contingency budget line
- iv) Transfer Risk- Outsource risk/Share a portion of the risk to a third party or parties that can manage the outcome.

In these circumstances, the project organisation has adopted the **ORCA Approach** to ensure consistent application of risk management by all staff towards-

- execution of the strategy
- accomplishment of business objectives
- day-to-day operations

ORCA represents-

- O Objectives** (Goals and results that SmarTech aims to achieve)
- R Risks** (Any potential event which could prevent the achievement of an objective)
- C Control** (Management's response to risks) (ISO/IEC: Information Technology, 2008)
- A Alignment** (Alignment of SmarTech's objectives, risks, and control across the enterprise which is determined by its viewpoint and tolerance for risks)

Roles and Responsibilities

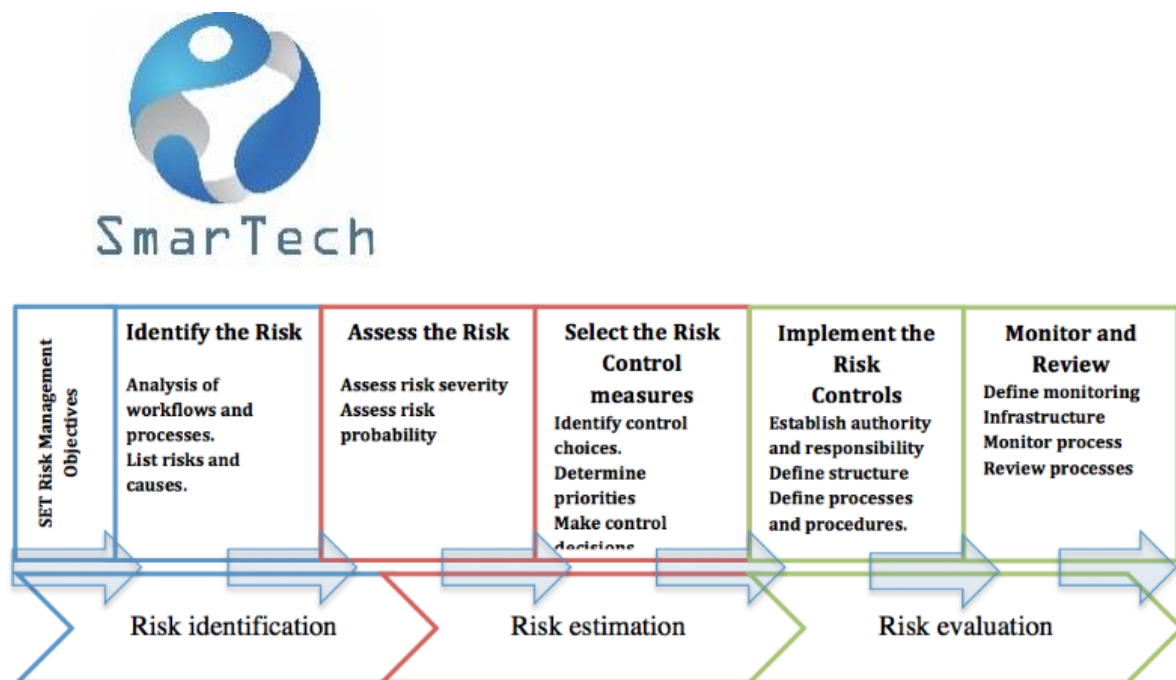


Fig 1: Risk Management Process

<https://www.linkedin.com/pulse/6-steps-risk-management-process-sheraz-ali>

The Risk Management Process in this organisation consists of the following processes-

- i) **Identify** key risks
- ii) **Analyse** the potential impact and likelihood of risks

- iii) **Respond** to risks by considering existing controls as well as selecting, prioritising, and implementing appropriate actions
- iv) **Monitor** the internal and external environment for potential changes to risks and ensure that risk responses continue to operate effectively
- v) **Report** on risks and the status of risk responses adopted

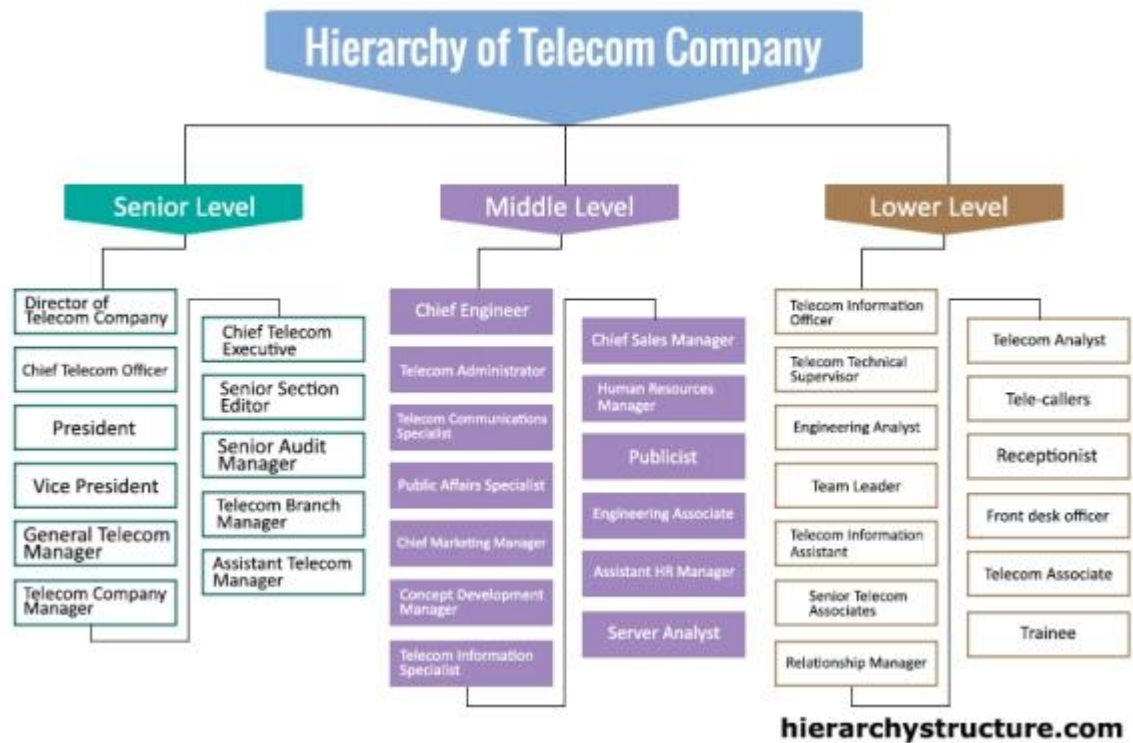


Fig 2: Hierarchy of Telecom Company

<http://www.hierarchystructure.com/hierarchy-of-telecom-company/>

With the advent of newer technologies, telecom companies have undergone through immense structural changes and in this respect huge popularity of mobile phones and mobile internet services also have considerable roles. In the global market of today, telecom companies are measured as one of the well accredited and busy firms (Chakraborty & Nandi, 2003, pp. 36). In the modern context, where mobile is an urgent need, telecom services are a type of CSP/Communications Service Provider, which provide ardent telecommunication

services, like data communication and telephony access, to its users. Since the telecom companies are operating in a broad field, therefore the hierarchy of telecom companies are quite critical. In a simplified way, like below, the telecom company has been categorised into three core levels with the further incorporation of some sub levels. Further, the Board of Directors acknowledges the relationship of the organisation with its stakeholders as a core capital to create additional value in the competitive market.



Fig 3: Stakeholder Relations

https://www.bluelabeltelecoms.co.za/online_reports/ar2015/gov-relations.php

Risk Management Framework

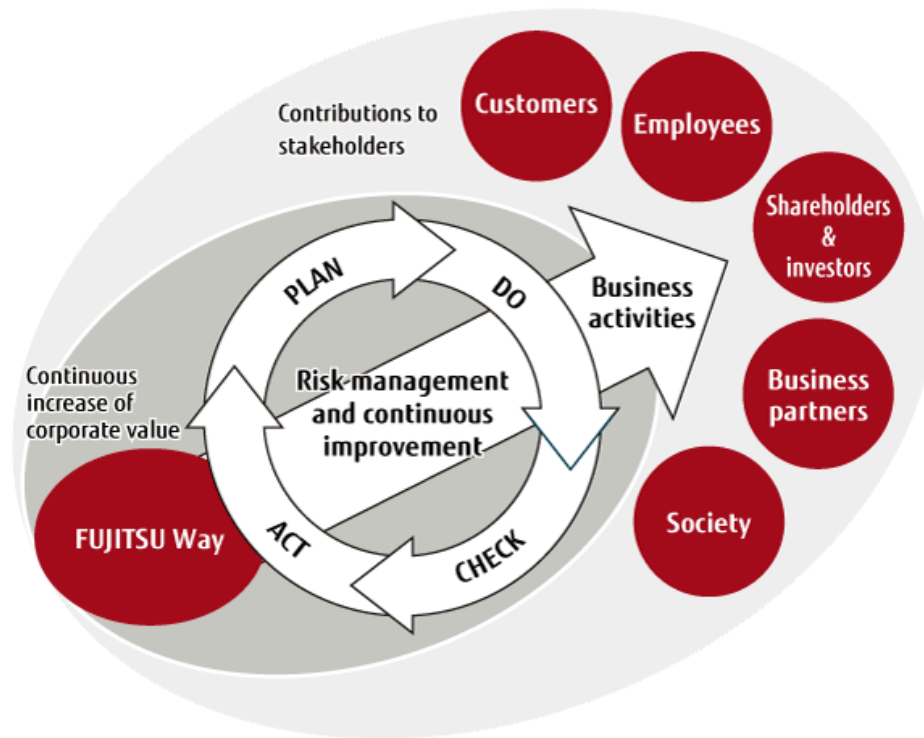


Fig 4: Risk Management Framework

<http://www.fujitsu.com/global/about/csr/management/riskmanagement/>

Through its wide activities in the ICT industry, SmarTech continuously seeks to increase its corporate value, and to contribute to its customers, local communities and indeed all stakeholders. Properly assessing and dealing with the risks that threaten the achievement of the objectives, while taking steps to prevent the occurrence of these risk events, and establishing measures to minimise the impact of such events if they do occur and to prevent their reoccurrence are assigned as a high priority by management. Moreover, they have built a risk management and compliance system for the organisation and are committed to its continuous implementation and improvement (Chakraborty & Nandi, 2003, pp. 41).

Business Risks

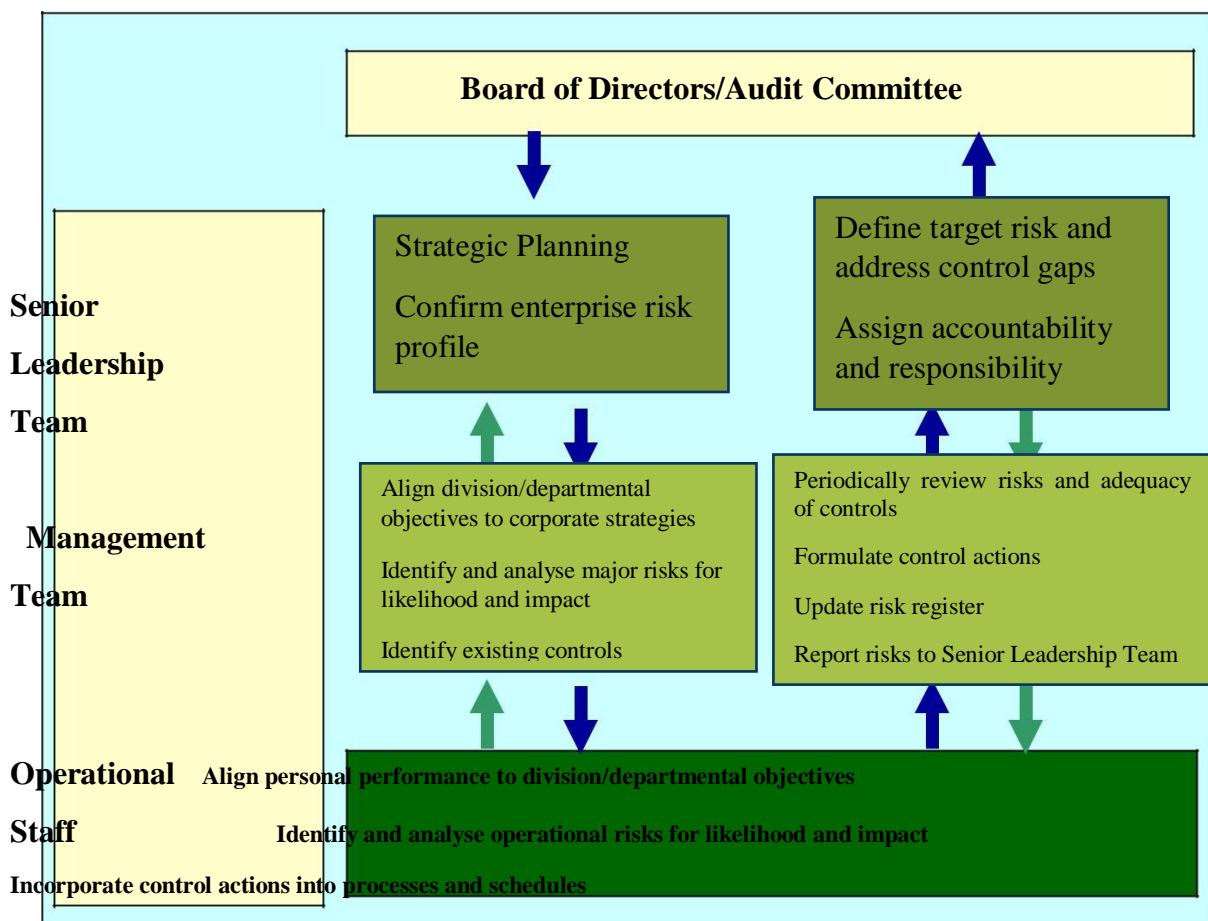
This organisation identifies, analyses, and evaluates the risks that accompany business activities and works on measures to avoid or reduce them, and to deal with them quickly in the unlikely event that they materialise. Major business risks are as follows-

- Competitor and industry risk
- Economic and financial market trend risk
- Customer risks
- Supplier and alliance risk
- Investment decision and business restructuring risk
- Financial risk
- Compliance risk
- Security risk
- Environmental risk
- Human resource risk
- Product and service deficiencies risk
- Natural disasters and unforeseen incidents risk
- Others

Risk Management and Compliance Structure

To respond aptly to materialise the risks and to prevent their recurrence, the organisation should grow up the ability to prevent potential risks of loss in business execution from materialisation. For that purpose this company has established a Risk Management and Compliance Committee under the Board of Directors (Chakraborty & Nandi, 2003, pp. 46). This committee acts as the highest-level decision-making body on matters involving risk management and compliance.

The Risk Management and Compliance Committee assigns Chief Risk and Compliance Officers to each of the organisational divisions. These divisions work collaboratively with each other, while building a risk management and compliance structure for the entire organisation to encourage them to guard against both potential risks and mitigate risks that have already been materialised.



The Risk Management Framework

The Risk Management & Compliance Committee is responsible for grasping the status of risk management and compliance, while establishing the appropriate policies and processes, including implementing and continuously improving them. Practically, the decision is taken on risk management regulations and guidelines, while applying them and continually reviewing and improving them.



Risk Management Process

On the basis of the risk management framework in AS/NZS ISO 31000:2009, risks will be managed and the Risk Management & Compliance Committee, which maintains regular communications with Chief Risk Compliance Officers, identifies, analyses and evaluates the risks of business activities, and sets out and reviews the responsive measures (Kaspersky Labs, 2011). It also identifies, analyses, and evaluates important risks regularly and report the same to the Board of Directors.

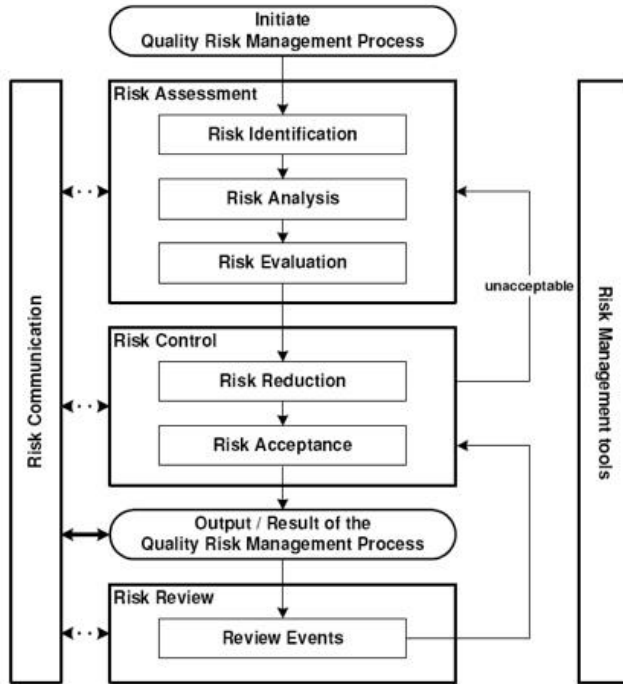


Fig 5: Overview of a typical risk management process

<http://eurogtps.com/PROJECTOUTCOMES/EuroGTPHOTTOPICS/4RISKMANAGEMENT/44Relevantdefinitionsintheriskmanagementpr/tabid/246/Default.aspx>

Risk Assessment-Likelihood Scale

Once the risks have been identified, the likelihood of the risk occurring and the potential impact if the risk does occur are assessed using the risk rating table below-

5	4	3	2	1
Almost certain	High probability	Possible	Low probability	Unlikely

Risk Impact Rating				
5	4	3	2	1
Financial – direct loss or opportunity costs of:				
>110m	>55m – 110m	>28m – 55m	>12mil-28mil	1mil - 12 mil
Operational - missed milestone by:				

>7 months	>4 -7 months	1-4 months	1-5 weeks	<1 week
Regulatory				
Large scale action, material breach of legislation with very significant financial or reputational consequences	Regulatory breach with material consequences but which cannot be readily rectified	Regulatory breach with material consequences but which can be readily rectified	Regulatory breach with minimal consequences but which cannot be readily rectified	Regulatory breach with minimal consequences and readily rectified
Strategic / Organisation -wide				
Failure to meet key strategic objective; organisational viability threatened; major financial overrun	Major impact on strategy; major reputational sensitivity	Moderate impact on strategy; moderate reputational sensitivity	Minor impact on strategy; minor reputational sensitivity	Minimal impact on strategy; minimal reputational sensitivity
Personnel - Loss of managerial staff in 1 year:				
>45	20-31	10-19	5-9	<4

These risks are depicted in a 5X5 Risk Map, which is represented in the above profile-

Risk Rating = Likelihood x Severity

S e v e r i t y	Catastrophic	5	5	10	15	20	25
	Significant	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Negligible	1	1	2	3	4	5
			1	2	3	4	5
			Improbable	Remote	Occasional	Probable	Frequent
			Likelihood				

Catastrophic	■	STOP
Unacceptable	■	URGENT ACTION
Undesirable	■	ACTION
Acceptable	■	MONITOR
Desirable	■	NO ACTION

Risk Level

Negligible	Low	Moderate	Serious	Catastrophic
Insignificant financial loss. Minimal time to recover. Brand image is protected.	Minor financial loss. Short time scale to recover both financially and politically.	Considerable financial loss and reputation. Reasonable time to recover.	Consequential financial loss. Major environmental implications and business interruption. Long time to recover.	Excessive long term injuries. Severe financial loss and damage in reputation. Significant business interruption.

Recording the Risk Management Process

Stakeholder Analysis

	Board of Directors	Executive Team	Consumers	Creditor	Supplier
Role	Decision making	Overseeing and managing the project	Revenue generation	Bank loan liability	Providing essential materials for production
Internal/External	Internal	Internal	External	External	External
Interests	Financial	Financial Reputational	Value product	Financial	Financial
Contribution	Capital injection	Steering the project	None	Capital	Supplying raw materials

					and timely launching of the product
Level of Influence (Low, Medium, High)	High	High	Low	High	Medium
Level of Importance (Low, Medium, High)	Low	High	Low	Low	Low
Level of Interest (Low, Medium, High)	High	High	High	High	Low
Priority (1,2,3,4,5,.....n; 1 being the highest)	2	1	5	3	4
Method of Communication	Teleconference Videoconference Email Face-to-face	Email Face-to-face Progress Reports	Website Ads	Face-to-face Email	Face-to-face Email
Frequency	Before a key decision to be made that has a financial impact	Regular weekly updates	Regular marketing signals throughout the product lifecycle	Before the project and throughout the payment scheme when needed	Regularly throughout the Inbound Logistics, Supply Chain activities
Issues if not involved	Lack of resources essential to kick start the project	No management support, poor steering of the project-project failure	Poor financials and political damage	Insufficient capital	Lack of quality raw materials Impact on schedule

Communications Plan

	Director	Council Workers	Customers	Creditors	Supplier
Outcomes	Decision making at a high level, controlling individual employee groups within the company, seeking new capital	Internal communication, decision making, low-level involvement in the work of the company	Minimise the risk of loss of reputation	Minimise financial risk	Sourcing materials, new supply resource, organising supplies
Key Message	Risk management, resource allocation, decision making	Development of new strategic projects, organisation of internal company	Properties of the product, use of the product, the terms	Financials	Supply materials at the best prices
Channel	Email, phone, meeting	Email, face to face, phone, reports	Website	Email, phone	Email, phone

Responsible	Council workers, directors		Marketing and Public Relations	Director, council workers	Council workers
When	Before starting of the project	Every week	Regularly	Regularly	Regularly

Industry Analysis

Dimension	Details
Social	In Australia, over the last 20 years, 250k people are born at an average per year. This estimated number is calculated on the basis of and the amount of the remaining inhabitants of Australia and the arriving immigrants. The migration in the country has also been taken into account. The demand for new technologies of SmarTech increases with the ever-increasing population. Further, the Australian population is getting more educated and the lifestyle is changing as well. As a consequence of all these demands for technology increases every year (Chakraborty & Nandi, 2003, pp. 46).
Technological	SmarTech must use the latest available market technology in order to compete with other brands. The most important factor in determining strategy is whether at this time the product is manufactured by other companies or not.
Economic	With the still growing economy over 50 years, Australia is dealing with economic growth. As a result all these efforts directly transform into the prosperity of Australians. Just like SmarTech, bigger capacity portfolio means more money to spend on technology.
Legal and Political	The technologies of SmarTech must comply with applicable legal principles and should be prepared in such a way, so that if the rules change, then the organisation will be able to change the products also.
Policy (Government and Organisational)	There always exists the possibility that the government can change the rules and regulations. Further, the organisation can change the internal policy also. So, the strategy of the organisation will be flexible, so that they can change their product policy also. Company like SmarTech, should be always remain careful to assume such risks (Chakraborty & Nandi, 2003, pp. 47).

Risk Assessment Template

Risk ID	Risk	Risk Area	Likelihood	Impact	Consequence	Risk Ranking	Risk Level
1	Market	Financial	5	3	Lose market share	25	Major
2	Credit	Financial	3	3	Bad credit terms	15	Serious
3	Chemical Hazard	WHS	2	3	Injury	10	Minor
4	Biological Hazard	WHS	3	2	Injury	9	Minor
5	Monetary Changes	Commercial/Market	1	5	Inflation	9	Minor
6	Wars	Commercial/Market	1	3	Resource blocks	5	Minor

7	Employment Practices	Operational	5	5	Lawsuits	45	Catastrophic
8	Clients Practices	Operational	2	3	Lawsuits	10	Minor
9	Deficient Product	Technology	2	4	ACCC Investigation	14	Serious
10	Customer Issue	Technology	3	2	ACCC Investigation	9	Minor
11	Construction Work	Schedule	4	2	Injury	12	Serious
12	Testing	Schedule	3	2	Deficient Product	9	Minor
13	Earthquakes	Ext. Environment	5	1	Structure Damage	5	Minor
14	Volcano	Ext. Environment	3	4	Disaster	21	Major

Risk Treatment and Action Plan

Risk Id	Risk	Risk Area	Risk Ranking	Root causes	Risk Treatment	Risk Control Measures Actions to be Taken	Monitoring Procedures	Responsible Person	Timeline
1	Market	Financial	25	Industry Insights	Accept Risk	Find differentiating quality from competition	Compare company results with competitor results	CEO	4 years
2	Credit	Financial	15	Finance Management	Mitigate Risk	Diversify use of capital and investments to protect against financial movements	Amount of Capital	Finance	2 years
3	Chemical Hazard	WHS	10	Lax OHS procedures	Accept risk	Ensure appropriate policies are in place	Employ lawyers and PR team	Lawyers & PR	4 years
4	Biological Hazard	WHS	9	Lax OHS procedures	Accept risk	Ensure appropriate policies are in place	Employ lawyers and PR team	Lawyers & PR	3 years
5	Monetary changes	Commercial/market	9	Customer satisfaction low	Avoid risk	Put utmost focus on customer satisfaction	Complaints/suggestions box and measure customer	Store managers	2 years

							loyalty by return rate		
6	Wars	Commercial/market	5	Ineffective management	Avoid risk	Ensure appropriate management incentives are available for leaders	Measure KPIs of managers and stores	Global leadership team	4 years
7	Employment Practice	Operational	45	OHS procedures	Avoid risk	Have appropriate OHS policy	Frequency of safety incidents	OHS	5 years
8	Clients Practices	Operational	10	Facilities management	Transfer risk	Lease equipment	Cost of maintenance	Facilities	7 years
9	Deficient Product	Technology	14	Poorly implemented systems	Mitigate risk	Improve systems	Efficiency	IS	2 years
10	Customer Issue	Technology	9	Cyber criminals	Mitigate risk	Ensure strong IS security and find alternative places to store confidential info	Frequency of security breaches	IS	5 years
11	Construction Work	Schedule	12	Completion risk	Avoid risk	Project manager to improve time management	Construction complete on time	Project manager	2 years
12	Testing	Schedule	9	Warehouse management	Transfer risk	Improve warehouse management	Quantity of bad products per batch	Warehouse manager	3.6 years
13	Earthquakes	Ext. Envi.	5	Environmental crisis	Accept risk	Ensure appropriate policies are in place	News	Crisis management team	1.2 years
14	Volcano	Ext. Envi.	21	World and business knowledge	Accept risk	Keep updated of business environment	Compare company results with industry and other businesses	Crisis management team	3.9 years

References

- Almici, A. (2012). Corporate Governance, Sustainable Development, and Value Creation – Some Evidences from Italian Listed Companies, *Chinese Business Review*, vol. 11, n. 3, pp. 322-333.
- Brondoni, S.M. (2010). Intangibles, Global Networks & Corporate Social Responsibility, *Symphonya. Emerging Issues in Management (symphonya.unimib.it)*, n. 2, pp. 6-24.
- Caldwell, T. (2011). Smart Security: Network Security. 2011 (4), 5-9 (2011).
- Chakraborty, C; & Nandi, B. (2003). Privatisation, Telecommunications and Growth in Selected Asian Countries: An Econometric Analysis, *Communications and Strategies*, vol. 52, n. 4, pp. 31-47.
- ISO/IEC: Information technology – Security techniques – Information security risk management. ISO/IEC 27005:2008, 1st Edition (2008).
- Kaspersky Labs: IT Threat Evolution: Q3 2011, http://www.securelist.com/en/analysis/204792201/IT_Threat_Evolution_Q3_2011.
- Mylonas, A. (2008). Smartphone spying tools. MSc Thesis, Royal Holloway, University of London (2008).
- Nachenberg, C. (2011). A Window into Mobile Device Security. Technical Report, Symantec Security Response (2011).
- Oppliger, R. (2011). Security and Privacy in an Online World. *Computer*, 44 (9), 21-22 (2011).

OWASP:

Top

10

Mobile

Risks,

http://www.owasp.org/index.php/WASP_Mobile_Security_Project.