Risk Management

Manage your risks

bsi.

…making excellence a habit.™

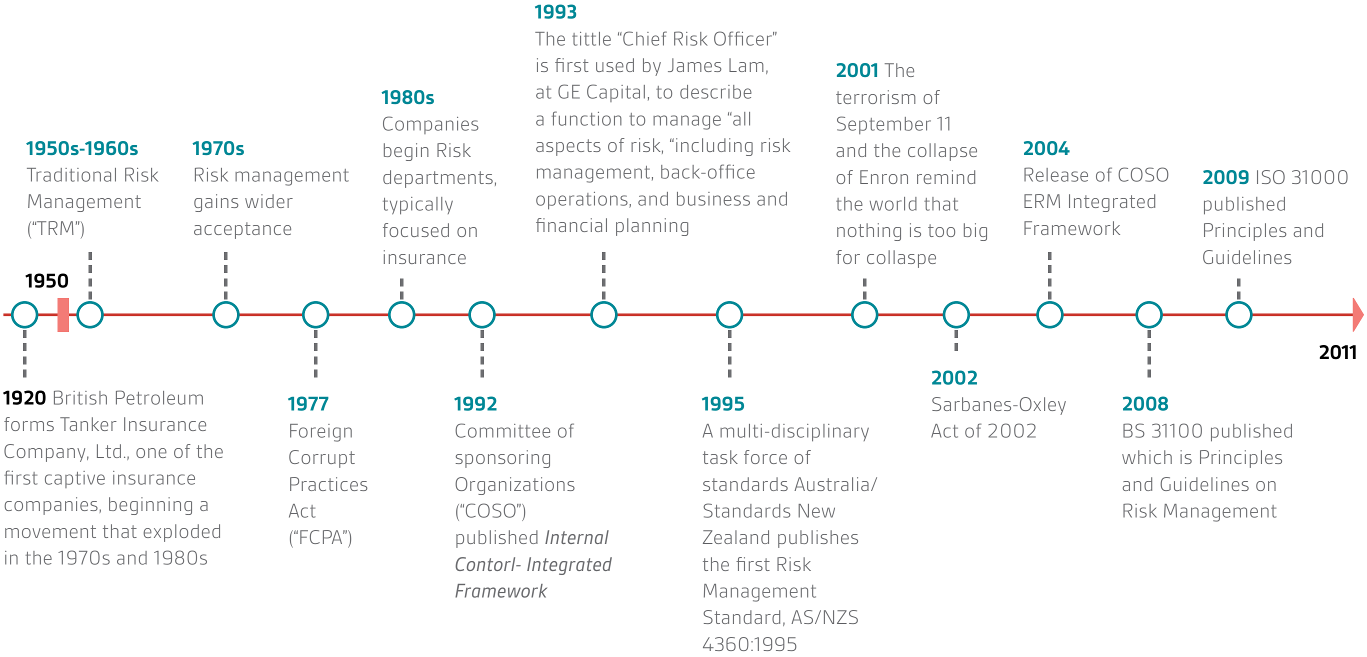
Risks

Risk concerns the deviation of one or more results of one or more future events from their expected value.

Technically, the value of those results may be positive or negative. There are different definitions of risk for each of several applications. The widely inconsistent and ambiguous use of the word is one of several current criticisms of the methods to manage risk.

There could be several kinds of risks such as: Insurance and Health risk, Information technology risk, Information security risk, financial risk, Economic Risk, Credit Risk, Political risk and so on and so forth.

Historically Speaking



1920 British Petroleum forms Tanker Insurance Company, Ltd., one of the first captive insurance companies, beginning a movement that exploded in the 1970s and 1980s

1950

1950s-1960s Traditional Risk Management ("TRM")

1970s Risk management gains wider acceptance

1977 Foreign Corrupt Practices Act ("FCPA")

1980s Companies begin Risk departments, typically focused on insurance

1992 Committee of sponsoring Organizations ("COSO") published *Internal Contorl- Integrated Framework*

1993 The tittle "Chief Risk Officer" is first used by James Lam, at GE Capital, to describe a function to manage "all aspects of risk, "including risk management, back-office operations, and business and financial planning

1995 A multi-disciplinary task force of standards Australia/ Standards New Zealand publishes the first Risk Management Standard, AS/NZS 4360:1995

2001 The terrorism of September 11 and the collapse of Enron remind the world that nothing is too big for collaspe

2002 Sarbanes-Oxley Act of 2002

2004 Release of COSO ERM Integrated Framework

2008 BS 31100 published which is Principles and Guidelines on Risk Management

2009 ISO 31000 published Principles and Guidelines

2011

The simple fact is that risk is always a probability issue.

Risk Management

Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Risks can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attacks from an adversary etc.

The strategies to manage risk include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk (better known as 4 T's : - Treat, Tolerate, Transfer, Terminate)

Managing Risk

Risk management is a central part of any organization's strategic management. It is the process whereby organizations methodically address the risks attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. Risk management should be a continuous and developing process which runs throughout the organisation's strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, future.

Risk Management Techniques

Risk is the ultimate four-letter word of business, investment and government. Entrepreneurs and political leaders understand as well as anyone that if nothing is ventured, nothing can be gained, and that therefore risk can never be entirely eliminated. Nonetheless, the effort to minimize, or at least manage risk, has become a major focus of most corporate entities, and it's standard practice for public companies to disclose their operating risks each quarter in their public filings. There are as many actual risk management techniques as there are types of businesses, but once a risk has been identified and assessed, most efforts at mitigating the risk fall into four basic categories regardless of the context. The first, avoidance, can be as simple as not engaging in activity that produces the risk, but this not only eliminates risk but potential benefits as well. Risk reduction through concrete steps is far more common, and the specifics will be related to the type of business and risk involved. Risk transference is also highly beneficial as when an available option; it involves outsourcing the problem to another entity such as through the purchase of insurance. Finally, risk retention is inevitable in some cases where the risks are either unlikely, or the costs of mitigating or transferring the risk are prohibitive.

Standards approach to Risk Management

There are a number of national 'standards' for risk management. The first was developed by Standards Australia/New Zealand in 1995 (AS/NZS 4360), followed by Canada (CAN/CSA-Q850) in 1997 and the United Kingdom (BS-6079-3) in 2000. COSO document was delivered in late 2004 as the 'Enterprise Risk Management – Integrated Framework'.

BS 31100, BSI's new code of practice for risk management, began life in 2006. BS 31100 aims to widen this discipline by focusing on how it can be employed to help drive profits through responsible risk-taking. The committee that drafted BS 31100 approached risk management from two angles. First, it dealt with practical solutions: the principles, framework and processes required for an effective and scalable code of practice

ISO 31000:2009 addresses the entire management system that supports the design, implementation, maintenance and improvement of risk management processes.

The golden rule is that there are no golden rules.

(G.B. Shaw 1856-1950, Irish critic and poet)

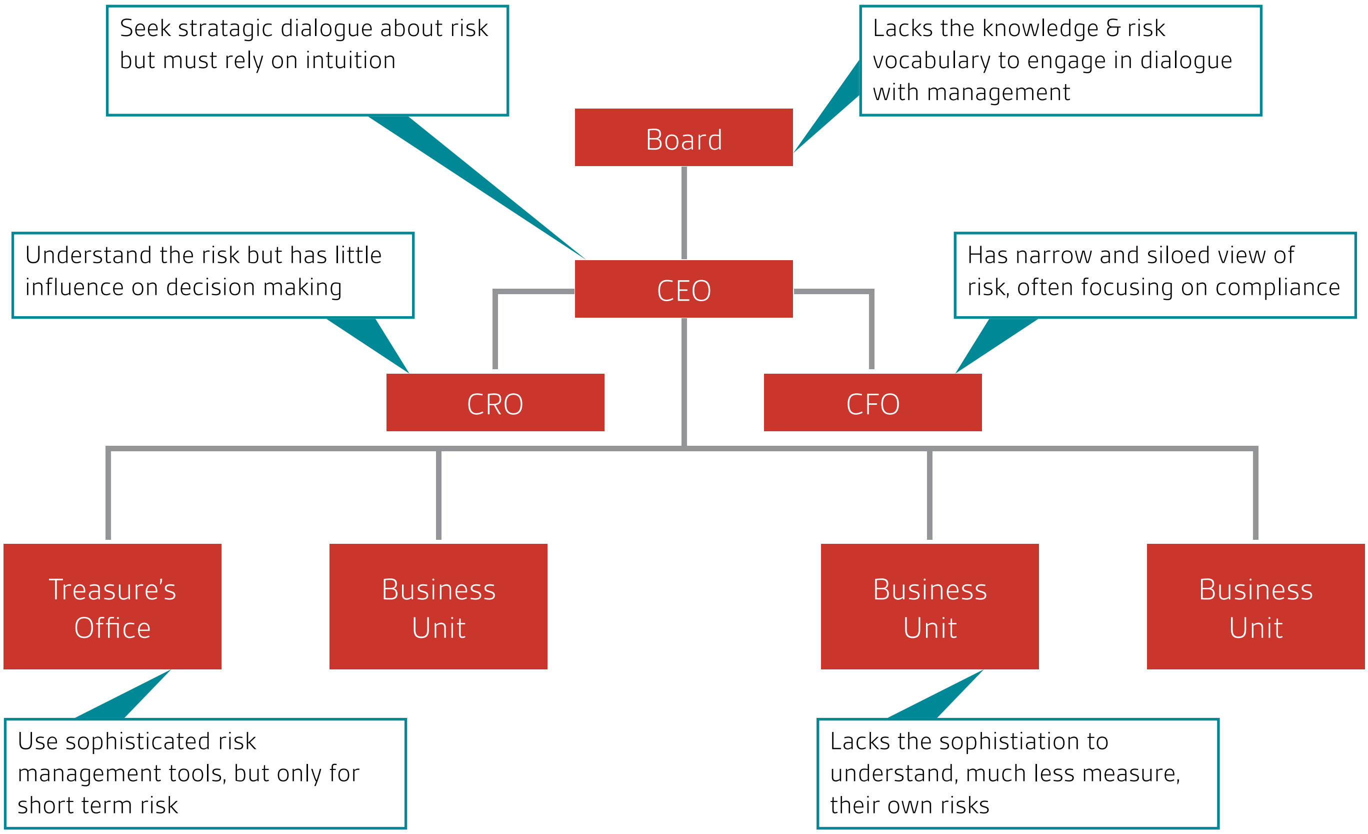
Risk Management : Why reinvent the wheel?

It is no longer acceptable to drive businesses exclusively through financial controls. Although profit is fundamental to business success, other factors must be considered to ensure that business remains successful in the medium term. Customers, employees, legislation, litigation, local and wider community opinion can all have a significant impact on the health and prosperity of any organisation.

Indian corporate houses are increasing their focus on Corporate Governance and Internal Controls. The result will be increased requirements for organisations to demonstrate that they have structured management systems in place to review and prioritise the needs of all their stakeholders, as well as manage the business risks they face.
Essentially the first step along the risk management process, after all the necessary business information is available, is to perform a risk assessment. Risk assessment may seem to be more of an operational issue but in fact requires an organisation wide approach. Risk can be inherent in an opportunity to acquire another organisation as much as it can be the potential for loss should an incident occur.

Changing role of CRO/CFO

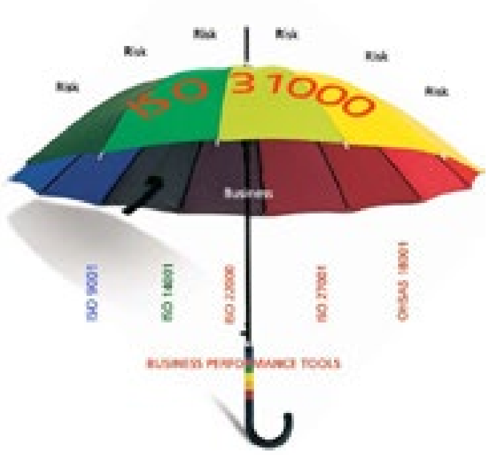
As a key member of the senior management team, the CRO is a peer and advisor to the rest of senior management who can translate risk management into the terms that matter to their key stakeholders (i.e., stockholders, employees, customers), such as the effect of risks and risk management on capital, growth, return and consistency. The top skills required for CROs include the ability to understand business issues, the ability to measure and compare and the ability to communicate.
The most important benefit of appointing a single CRO for the enterprise: expanded risk management that encompasses a wider range of enterprise risks release of ISO 31000, we have an Internationally recognised standard available to help organisations take account of the needs and expectations of all their stakeholders. The results from internal and external audits to these standards can be used to drive organisational risk management. The whole system needs to have a continual improvement focus, in line with strategic objectives, thereby safeguarding the future prosperity of the organisation.


Seek stratagic dialogue about risk but must rely on intuition
Lacks the knowledge & risk vocabulary to engage in dialogue with management
Board
CEO
Understand the risk but has little influence on decision making
Has narrow and siloed view of risk, often focusing on compliance
CRO
CFO
Treasure's Office
Business Unit
Business Unit
Business Unit
Use sophisticated risk management tools, but only for short term risk
Lacks the sophistiation to understand, much less measure, their own risks

The Umbrella Concept

The umbrella term ‘risk assessment’ includes the activity of ‘risk identification’ in BS ISO 31000. ISO 31000 can be integrated with other management systems such as ISO 14001 Environmental Management; Z1000 Occupational Health and Safety Management; the OHSAS 18001 Occupational Health and Safety Management System Requirements; and Z1002 Occupational Health and Safety – Hazards and Risks – Identification, assessment, elimination and control (currently under development).

It can also be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.



ISO 31000 is

Principles and practical guidance to the risk management process

- Applicable for all types of organizations
- Applicable to a wide range of activities
- Harmonization of risk management coverage in existing and future standards viz ISO 9001, ISO 14001, ISO 27001, ISO 22000 etc

ISO 31000 is not intended

- To promote uniformity in risk management across organizations
- For the purpose of certificationFor the purpose of certification

Risk Index = Impact of Risk x Probability of Occurrence

ISO 31000 Risk Framework

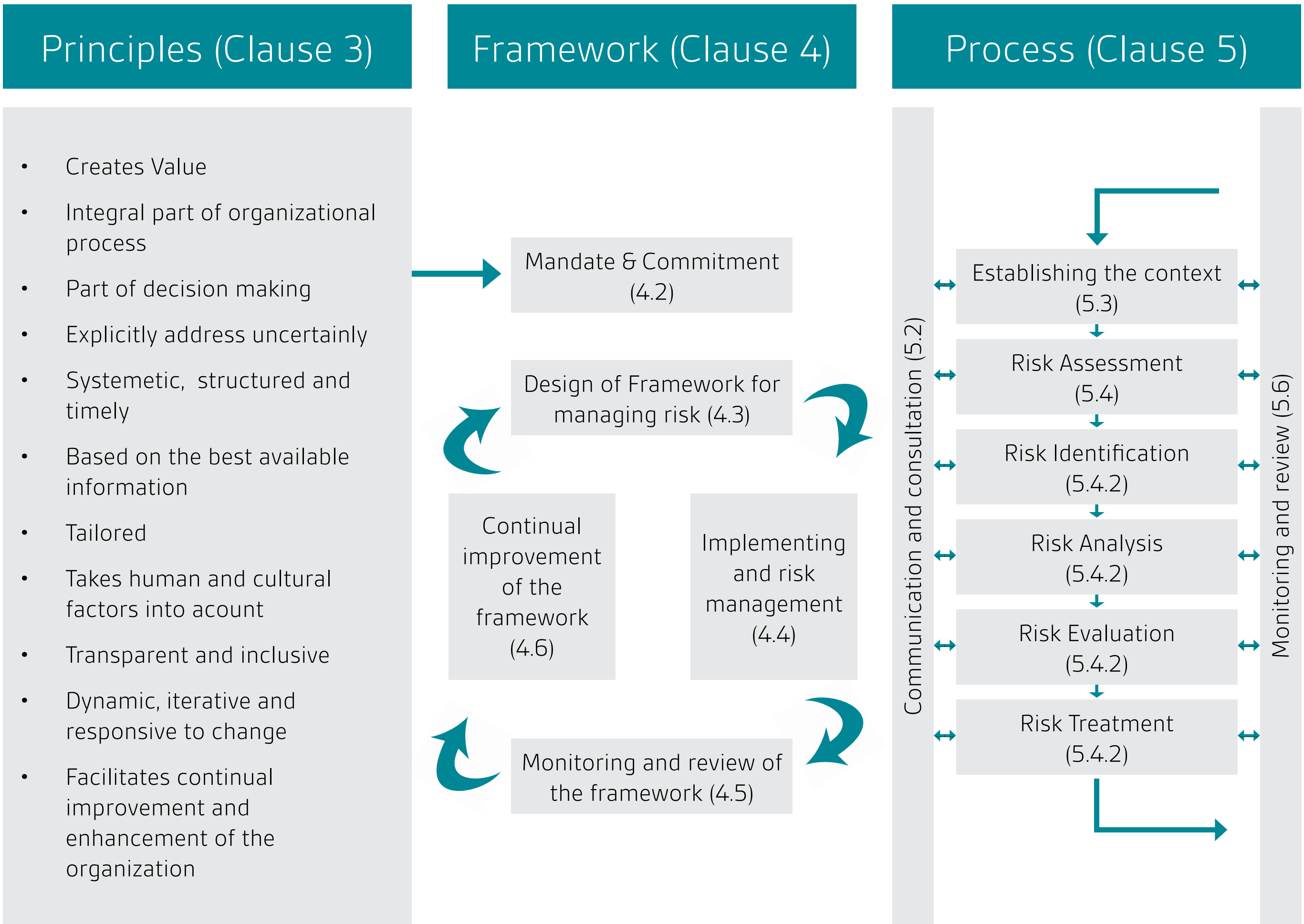
4.1	General
4.2	Mandate and commitment
4.3	Design of framework for managing risk
4.3.1	Understanding of the organization and its context
4.3.2	Establishing risk management policy
4.3.3	Accountability
4.3.4	Integration into organizational processes
4.3.5	Resources
4.3.6	Establishing internal communication and reporting mechanisms
4.3.7	Establishing external communication and reporting mechanisms
5.4	Implementing risk management
4.4.1	Implementing the framework for managing risk
4.4.2	Implementing the risk management process
4.5	Monitoring and review of the framework
4.6	Continual improvement of the framework
5.1	General
5.2	Communication and consultation
5.3	Establishing the context
5.3.1	General
5.3.2	Establishing the external context
5.3.3	Establishing the internal context
5.3.4	Establishing the context of the risk management process
5.3.5	Defining risk criteria
5.4	Risk assessment
5.4.1	General
5.4.2	Risk identification
5.4.3	Risk analysis
5.4.4	Risk evaluation
5.5	Risk treatment
5.5.1	General
5.5.2	Selection of risk treatment options
5.5.3	Preparing and implementing risk treatment plans
5.6	Monitoring and review
5.7	Recording the risk management process

Comparisons between AS/NZS 4360 and ISO 31000

Elements	AS/NZS 4360:2004	ISO 31000:2009
Application	Universal application across all organizatoins - Australia and New Zealand	Universal application across all organizatoins - International
Context for risk management	Organization's objectives	Organization's objectives
Process for managing risk ("what you do")	Core of AS/NZS 4360	Part of ISO 31000
Framework for managing risk ("how you do it")	Revised substantially in 2004	Expanded on AS/NZS 4360
Principles for managing risk	Implicit - to some extent	Now clear and explicit
Attributes of enhanced risk management	No covered	Annex in ISO 31000 as informative (optional)
Guide to establishing and implementing effective risk management process	Covered in handbook (HB 436:2004)	Annex in ISO 31000 as informative (optional)

Components of Risk Management Process

ISO 31000 Model



Principles (Clause 3)

- Creates Value
- Integral part of organizational process
- Part of decision making
- Explicitly address uncertainly
- Systemetic, structured and timely
- Based on the best available information
- Tailored
- Takes human and cultural factors into acount
- Transparent and inclusive
- Dynamic, iterative and responsive to change
- Facilitates continual improvement and enhancement of the organization

Framework (Clause 4)

Mandate & Commitment (4.2)

Design of Framework for managing risk (4.3)

Implementing and risk management (4.4)

Monitoring and review of the framework (4.5)

Continual improvement of the framework (4.6)

Process (Clause 5)

Communication and consultation (5.2)

Establishing the context (5.3)

Risk Assessment (5.4)

Risk Identification (5.4.2)

Risk Analysis (5.4.2)

Risk Evaluation (5.4.2)

Risk Treatment (5.4.2)

Monitoring and review (5.6)

Our Service Portfolio

- GAP analysis
- Third party Audits
- Training
- Coaching and mentoring
- Business Risk Assessment

BSI India will offer the above suite of services. These services have a unique proposition namely

1. Affordability
2. Uses a Common sense approach
3. Standards based approach
4. Relevant to any Industry
5. Get your Heat map of your current Risk
6. Find your Risk appetite and Risk Profile "just in a day"

About BSI Group

By Royal Charter

BSI, a Royal Charter founded in 1901, focuses on standards creation, certification, supplier verification and training activities to help manage risk, reduce costs and ensure sustainability.

As the world's most experienced Standards Body and founding member of ISO, BSI leads the way in originating the majority of the world's most recognized standards, including ISO 9001, ISO 14001, BS OHSAS 18001, Business Continuity Management, Information Security, Cloud Computing, Energy Water Management, Anti-bribery as well as the originator of other supplier qualification standards covering Supplier Pre-Qualification, CSR, GMP, Security, Chain of Custody and other topics.

Certification

- 25,038 business locations certified by BSI in Asia
- Ranked 1st in North America and UK
- 7,424 CE marking certificates
- Our assessors score on average 9.3 / 10 in our Global Client Satisfaction Survey

Product certification

92% of the world's top 25 global medical device manufactures trust BSI as their notified body for CE marking certification to access global markets.

BSI's India Presence

Mumbai
+91 (0) 22 4257 8600/04/26

Bangalore
+91 (0) 8040472300

Chandigarh
+91 (0) 172 5026070/71/72

Chennai
+91 (0) 44 28361305/06/07/08

Kerala
+91 (484) 4036861

Kolkata
+91 (0) 33 22658803

Hyderabad
+91 (0) 40 40201004/05

Pune
+91 (020) 60709990

India Office:
BSI Group India
The Mira Corporate Suites,
A-2, Plot 1&2, Ishwar Nagar,
Mathura Road, New Delhi-110065, India
Call: **+91 11 2692 9000**
Email: **info.in@bsigroup.com**

bsi.
bsigroup.co.in

10,000
Industry experts dedicated to your success

80,000
Customers worldwide

120,000
Business locations worldwide

Training

Last year we provided training to over 112,000 delegates

Standards

Quality management systems Standard ISO 9001 – which started life at BSI in 1979 as BS 5750 – is the world's most successful standard, having been adopted by more than one million organizations in 178 countries