Risk Assessment – Where to Next?

21 April 2009

Alf Esteban
Head of Consulting & Client Services
Governance, Risk & Compliance

Email: alf.esteban@saiglobal.com
Web: www.saiglobal.com
SAI Global (ASX: SAI) is an applied information services company that helps organizations manage risk, achieve compliance and drive business improvement.

Access to Standards & technical information
SAI Global is your source for global technical content such as Standards and legislation.

Comply with Standards, technical & legislative requirements
Sarbanes-Oxley, Basel II, Anti-money laundering, CLERP 9… compliance can be a burden.

Empowering people through training
SAI Global trains business professionals around the world every day.

Recognize assurance achievements
SAI Global provides independent assessment, certification and registration services, offering you one of the most widely recognizable symbols of excellence and assurance, the “five ticks” StandardsMark™.

Our journey
Sustainable business performance delivered by good people, working together as a great team in the interests of customers, shareholders and the community. At SAI Global your business performance is our journey.

Our people
SAI Global’s people know your business. Our people come from diverse backgrounds and offer a wide range of skills. Business professionals, innovators, technologists, scientists, engineers, designers and many more. There is an SAI Global expert near you ready to start thinking about your business
Increasingly complex business environments, dynamic regulatory landscapes, the increasing expectations of stakeholders and the public’s awareness of ethical breaches are driving a convergence in ethics, governance, risk and compliance initiatives at organizations worldwide. Critical to this convergence is the need to improve performance and build and maintain a workplace where an ethical culture permeates all aspects of the workplace.

At SAI Global we break down this complexity and help organizations manage risk, achieve compliance and promote an ethical culture.

We provide legal, compliance and risk management professionals with a broad range of technology enabled programs and consulting services that facilitate good governance and awareness of compliance, ethics and policy issues.

With more than twenty years experience, offices in 25 countries, well over a thousand clients, and millions of satisfied users, we’re ready to work with you to integrate a flexible suite of solutions and services specifically tailored for your business and industry.
“The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future is more than a whim of the gods and that men and women are not passive before nature. … [the] discoveries about the nature of risk, and the art and science of choice, lie at the core of our modern economy… The ability to define what may happen in the future and to choose among alternatives lies at the heart of contemporary societies.”

“The word “risk” derives from the early Italian risicare, which means “to dare”. Risk is a choice rather than a fate. The actions we dare to take, which depend on how free we are to make choices, are what the story of risk is all about.”

– Peter Bernstein, Against the Gods: The Remarkable Story of Risk, 1996
Risk Management – What is it?

“The chance of something happening that will have an impact on objectives”
– AS 4360: Risk Management

“Risk is the possibility that an event will occur and adversely affect the achievement of objectives”
– Committee of Sponsoring Organisations of the Treadway Commission (COSO)

“All activities of an organisation involve risks that must be managed. The risk management process aids decision making by taking into account uncertainty and the possibility of future events or circumstances (intended or otherwise) and their effects on agreed objectives”
– ISO 31000 Risk Management (Draft)
AS 4360 Risk Management Principles

- Communicate and consult
- Establish the context
- Identify risks
- Analyse risks
- Evaluate risks
- Treat risks
- Monitor and review
Communicate & Consult, Establish the Context

- Consult with relevant internal and external stakeholders in each stage of the risk management process
- Communicate the risk management process to relevant internal and external stakeholders
- Understand and document the context in which risk management is to operate, including the amount of risk the organisation is willing to take (the “risk appetite”)

ICH Harmonised Tripartite Guideline
- Identify the risks
  - The ‘where, when, why, and how’ events
  - Results in a risk register

- Analyse the risks
  - Determine the consequences and likelihood of a risk event
  - Results in a determination of the inherent risk

- Evaluate the risks
  - Determine whether the organisation is willing to accept the inherent risk or whether the risk requires treatment
Risk Assessment – Identify the Risks

- Identify the risks
  - The ‘where, when, why, and how’ events
  - Results in a risk register

- Analyse the risks
  - Determine the consequences and likelihood of a risk event
  - Results in a determination of the inherent risk

- Evaluate the risks
  - Determine whether the organisation is willing to accept the inherent risk or whether the risk requires treatment

- What information is available?
  - Process maps
  - Incident reports
  - Insurance claims
  - Results of audits / inspections
  - Checklists
  - Focus groups

- People, processes and systems
  - Swim lane diagrams
  - Source of the risk
  - Effect on objectives
Risk Assessment – Analysis and Evaluation

- Identify the risks
  - The ‘where, when, why, and how’ events
  - Results in a risk register

- Analyse the risks
  - Determine the consequences and likelihood of a risk event
  - Results in a determination of the inherent risk

- Evaluate the risks
  - Determine whether the organisation is willing to accept the inherent risk or whether the risk requires treatment
# Example Risk Matrix (Mining Sector)

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Rare</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Unlikely</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>Possible</td>
<td>0</td>
<td>8</td>
<td>16</td>
<td>32</td>
<td>64</td>
</tr>
<tr>
<td>Likely</td>
<td>0</td>
<td>16</td>
<td>32</td>
<td>64</td>
<td>128</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONSEQUENCES</th>
<th>Safety</th>
<th>Environment</th>
<th>Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero Harm</td>
<td>No Effect</td>
<td>No Damage</td>
<td>0</td>
</tr>
<tr>
<td>Minor Injury</td>
<td>Slight Harm</td>
<td>Slight Damage</td>
<td>1</td>
</tr>
<tr>
<td>Major Injury</td>
<td>Minor Harm</td>
<td>Major Damage</td>
<td>2</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>Localised Harm</td>
<td>Localised Damage</td>
<td>3</td>
</tr>
<tr>
<td>Facility Loss</td>
<td>Major Harm</td>
<td>Major Damage</td>
<td>4</td>
</tr>
<tr>
<td>Multiple Facilities</td>
<td>Massive Effect</td>
<td>Extensive Damage</td>
<td>5</td>
</tr>
</tbody>
</table>

- **Low Risk**: Manage
- **Medium Risk**: Incorporate Risk Reduction Measures
- **High Risk**: Fail to Meet Screening Criteria
- Change the consequences and/or likelihood of a risk event through specific cost-effective strategies and action plans to increase potential benefits or reduce potential losses
  - Avoid the risk
  - Reduce the likelihood
  - Reduce the consequences
  - Transfer the risk
  - Retain the risk
- Resultant risk after risk treatment is the “residual risk”
Monitor and Review

- Analyse and learn lessons from events, changes and trends
- Detect changes in external and internal context including changes to the risk itself
- Ensure risk control and treatment measures are effective and meaningful in both design and operation
Questions?
Thank You

Alf Esteban  
Head of Consulting and Client Services - Asia Pacific  

SAI Global  
Solutions for Governance, Risk and Compliance  

286 Sussex Street  
Sydney NSW 2000  

Phone: +61 2 8206 6672  
Fax: +61 2 8206 6019  
Mob: +61 411 838 723  
www.saiglobal.com  
alf.esteban@saiglobal.com