Document generated on 08/04/2025 11:56 p.m.

Assurances et gestion des risques
Insurance and Risk Management

The Board of Directors In Risk Governance

James Greenhill

Volume 74, Number 2, 2006

URI: https://id.erudit.org/iderudit/1092511ar
DOI: https://doi.org/10.7202/1092511ar

See table of contents

Publisher(s)

Faculté des sciences de l'administration, Université Laval

ISSN

1705-7299 (print)
2371-4913 (digital)

Explore this journal

Cite this document

Greenhill, J. (2006). The Board of Directors In Risk Governance. *Assurances et gestion des risques / Insurance and Risk Management*, *74*(2), 187–199. https://doi.org/10.7202/1092511ar

Article abstract

While the Board of Directors is not expected to carry out risk management for the organization, the Board serves to prevent downfalls that could stop the organization from achieving its goals or even threaten its survival. The author shows the link between the strategic Board's role and Enterprise Risk Management.

Tous droits réservés © Faculté des sciences de l'administration, Université Laval, 2006

This document is protected by copyright law. Use of the services of Érudit (including reproduction) is subject to its terms and conditions, which can be viewed online.

https://apropos.erudit.org/en/users/policy-on-use/

This article is disseminated and preserved by Érudit.

Érudit is a non-profit inter-university consortium of the Université de Montréal, Université Laval, and the Université du Québec à Montréal. Its mission is to promote and disseminate research.

https://www.erudit.org/en/

The Board of Directors In Risk Governance
Greenhill, James
Assurances et Gestion des Risques; Jul 2006; 74, 2; ABI/INFORM Complete
pg. 187

ARTICLES PROFESSIONNELS
PROFESSIONAL ARTICLES

Assurances et gestion des risques, vol. 74(2), juillet 2006, 187-200
Insurance and Risk Management, vol. 74(2), July 2006, 187-200

The Board of Directors In Risk Governance

by James Greenhill

ABSTRACT

While the Board of Directors is not expected to carry out risk management for the organization, the Board serves to prevent downfalls that could stop the organization from achieving its goals or even threaten its survival. The author shows the link between the strategic Board's role and Enterprise Risk Management.

RÉSUMÉ

Bien que la gestion des risques ne soit pas l'apanage du conseil d'administration, il demeure que le conseil est en mesure de prévenir certaines défaillances pouvant empêcher l'entreprise de réaliser ses objectifs ou même de menacer son existence. L'auteur fait le lien entre le rôle stratégique du conseil d'administration et la gestion intégrée des risques.

The Board of Directors serves in a critical advisory role at a strategic level, not only seeking new opportunities to move the agenda of the organization forwards, but also preventing downfalls that could stop the organization from achieving its goals or even threaten its survival.

To support the board and senior management there has to be an effective Enterprise Risk Management (ERM) process that is able to assimilate, analyze and integrate data from a wide variety of sources and provide effective responses.

The author:

James Greenhill is president of Risk Horizon, Ottawa.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In the past various aspects of risk management were often carried out by different people dispersed throughout an organization and were not part of a formal integrated risk management process. For example one person would handle business continuity planning, another would focus on safety equipment, a third would be in charge of purchasing insurance, and risk management might be considered briefly at a high-level as a subset of the strategic planning process. These individuals would rarely, if ever, meet to exchange information resulting in replicated efforts that could waste resources, or worse, could lead to gaps where each person would assume that someone else was handling a critical risk issue. In larger organizations this situation might have been replicated several times over resulting in even greater inefficiencies.

Today risk management is a more comprehensive function. Information is still gathered from all levels of the organization, but is viewed and managed on an organization or enterprise wide level. Risk is also analyzed on a more proactive basis. Instead of reviewing an incident and asking the question «How do we stop this from happening again?», the organization seeks out information on potential risks and looks to prevent them from happening in the first place. As well risk management is seen not only as a way to mitigate or minimize losses, but also as a way to seek new opportunities–i.e. determining that the organization is robust enough to take on new and possibly riskier endeavors.

While there has been a very positive evolution, there is still room for improvement. One recent global survey of executives and management of public and privately held companies showed that only 18% of their Board of Directors had a complete understanding of their organization's risks. [1]

While the Board of Directors is not expected to carry out risk management for the organization, there are a number of factors encouraging good risk governance. Shareholders and owners want to ensure the preservation of their investment. For publicly traded companies there are a number of laws and governing bodies which have a risk management aspect. Finally there is the board members' sense of duty from being associated with and wanting to help their organizations.

Failure to manage key risks can produce dramatic negative effects that reach far beyond the incident itself. For example, at the global telecommunications firm Ericsson all the chips used in their telephone handsets were produced at a single plant in the United States. In May of 2000 there was a minor fire that lasted less than half an hour. However the smoke and fire fighting efforts contaminated

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

the clean room environment of the production facility, resulting in a loss of most of the inventory. The result was an inability to deliver cell phones to customers in a timely manner. The division posted a major financial loss and Ericsson announced in January of 2001 that it was exiting the telephone handset market. Within a few hours of the news there was a 14% drop in stock value.

As well there can be adverse effects for directors on a personal basis. In some recent shareholder lawsuit settlements directors paid for a substantial portion using their own funds. This has shown that Director and Officers (D&O) insurance which had in the past paid for defense costs and settlements may not help if directors are shown to be ineffective at managing risks.

Assessing the effectiveness of an organization's Enterprise Risk Management program requires an understanding of the general risk management process, the language or lexicon used by practitioners, and the types of responses available for managing risks.

A number of definitions of Enterprise Risk Management have been developed. The one by the Committee of Sponsoring Organizations (COSO) that is listed below captures three key ideas of what is required in such a program:

- It is a dynamic function that follows changes in the organization in order to remain effective.
- It is led at a high level balanced with that ability to accept input from any level.
- It helps manage risks so that the organization can achieve its goals.

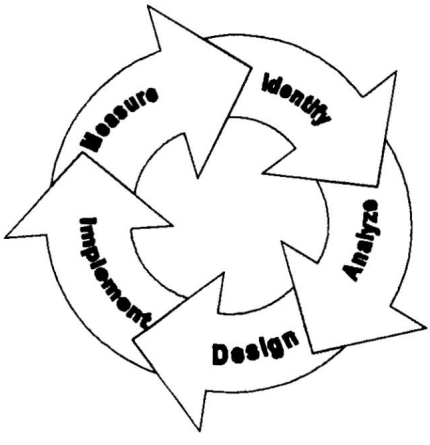
> *"Enterprise Risk Management is a process effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives."*
> Source: COSO.

Ultimately risk management is a form of general management; it is both an art and a science for making better decisions. To help this, a number of frameworks have been produced by such groups as the Institute of Risk Management, the Canadian Institute of Chartered Accountants, and the Treasury Board Secretariat of Canada. While they all have some variation in their structure, they generally follow the flow of the process in the figure below. Thus what is covered here can be applied to the other frameworks.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

At the end of the discussion of each step in this risk management process are a number of questions that a board member should ask in making an assessment.

FIGURE 1
RISK MANAGEMENT PROCESS



IDENTIFICATION

The first step is to identify risks that could affect the organization. To ensure that all aspects of the organization are reviewed different categories are developed. Below is a sample set and some of the risk that might occur within them, though each organization will develop categories that best suit its culture and structure.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

SAMPLE RISK CATAGORIES

STRATEGIC RISKS

Business Model Business model does not work in current market conditions with little organization ability to change it.

Industry Adverse changes in the industry landscape or reduction in market needs.

Leadership Lack of ability to develop effective vision and to implement it.

Product / Service Failure Poor or adverse product/service performance leads to excessive costs, loss of customer, product recalls and/or law suits.

OPERATIONAL RISKS

Capacity Insufficient capacity to meet customer demands, or excess capacity reduces profitability.

Support Structures Infrastructure (IT, communications channels, knowledge sharing) cannot support the organizations needs.

Critical Facility Loss or restricted access to important facilities.

Key Supplier Loss of supplier or its product impairs organization's ability to operate as no suitable alternative is readily available.

FINANCIAL RISKS

Budget Process Unavailable or unreliable budget and planning information may cause inappropriate financial conclusions and decisions.

Capital Availability Insufficient access to capital threatens the organization's capacity to operate and grow.

Pension Funds Assets of pension funds insufficient to meet obligations in timely manner.

EMPLOYEE RISKS

Change Readiness Employees unable or unwilling to implement new processes, products or systems.

Psychological biases can also impede the identification of risks. It used to be assumed that humans made logical, rational and objective decisions in risk management. Further study proved that this was not the case, and that they make use of a number of cognitive heuristics or mental shortcuts. These were developed during our evolution as survival tools that allowed for the rapid assessment and response to threats in a primitive environment i.e. detecting and evading predators. In modern situations, like in ERM programming, they are of little use, or worse, a liability. Such heuristics can lead to a false sense of security, or can cause the organization to focus on the wrong risks. Below are listed three biases that often occur. A more extensive listing can be found in the article *Psychological Factors in Risk Management* (Assurance, vol. 72 (4), Jan. 2005).

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Groupthink bias is where the group develops a consensus that does not allow for any meaningful dissension by individual members and ignores any contrary information. And often cited example is when the space shuttle Challenger was allowed to launch despite concerns of engineers and the evidence they brought about possible risks with the 'O-ring' seals in the booster rockets. Senior management overrode these concerns and launched the shuttle with disastrous results.

What often happens is a strong leader influences the rest of the team. Since business leaders are often strong individuals, they may cause certain risks to be ignored, despite contrary evidence. To help in identification of risks it might be helpful to remove possible influencers during discussions, such as department heads or senior management, so that others may be more comfortable in raising issues.

Optimism bias, or over-optimism, leads people to underestimate potential risks. This often occurs in assessing the possibility of being subject to a natural disaster. In New Orleans little preparations had been made for a hurricane with the intensity of Katrina since few people thought it could occur. This was exacerbated by an 'institutional optimism' of elected officials involved with possible management of this risk. Given that their terms were four to five years in duration, and that a storm with the intensity of Katrina occurred roughly once every 70 years, officials were optimistic that there was little chance they would have to manage this situation. Thus this risk was left as a legacy for incoming administrations. Conducting scenario planning and preparing for a worst case situation is one way to counter this over-optimism.

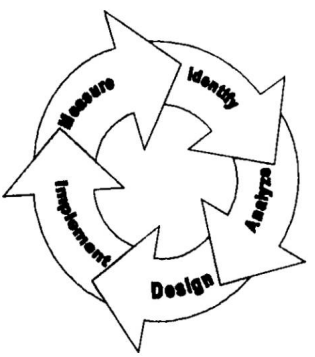
Perspective bias can also influence identification; recent or intense events attracting attention away from possibly greater issues. On December 29, 1972 the cockpit crew of an Eastern Airlines Lockheed L1011 was conducting a night time approach, and became focused on a single light that indicated that the landing gear may not have extended properly. While investigating the problem, they were not aware that the autopilot had become disengaged and the aircraft flew into the ground, killing over 100 people. In identifying risks an objective prospective of what key risks are must be kept despite the distracting influence of recent or intense events.

Beyond the psychological biases, there has to be a common understanding of risks by development of specific definitions. Otherwise there can be a situation where the same risk has different definitions for different groups. This can result in uncoordinated and wasteful efforts and lead to possible gaps in the risk management process.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

As well as the regular assessment process there has to be a way to report a new serious risk that appears outside of the regular risk management cycle in order to develop a timely response and disclosure. For example the Association of Certified Fraud Examiners cited in its 2004 Report to the Nation that fraud was detected 40% of the time outside of the regular audit process via a tip from an employee, customer or vendor. One solution is to have an individual within the organization designated as a "risk ombudsman" to whom people can bring issues.

Questions the Board should ask about IDENTIFICATION of risks



- Are the categories useful for prompting people to think about different types of risks and cover all aspects of the organization?
- Is there a common understanding or definition of each risk?
- Are there indications of psychological biases that could affect the identification process?
- Can new major risks be rapidly identified to management outside of the regular reporting cycle?

ANALYSIS

Once risks are identified the next step is to determine which ones have the greatest potential for harming the organization, usually measured as probability or frequency of occurrence, and potential severity of each risk.

Techniques for measuring the risk are either quantitative, for example Value-At-Risk calculations, mathematical modeling or statistical analysis, or qualitative, for example, workshops, interviews or surveys. A survey of Fortune 1000 companies noted that 59 percent of the respondents used incident reporting and loss measurement for identifying and prioritizing risks, making it the most common system or process. Others were risk assessment workshops with management and/or the Board of Directors (39 percent), risk modeling (32 percent), and risk mapping (28 percent).[2]

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

As with the identification phase, psychological biases can impede the impartial assessment of a risk. An anchoring bias is where an irrelevant piece of information provides a base or 'anchor' for value estimation. For example, given the question, "Last year was our worst year with total losses of $20 million. What is the greatest single loss the company could suffer and still survive?", respondents' answers will probably be close to the previous year's loss, even if the organization could survive a loss of several times greater. Ways to counter an anchoring bias are asking neutral open questions, not leading questions when gathering information, or when giving information, recognizing anchoring statements and dismissing them as irrelevant.

The way risks are presented or framed can influence how they are evaluated. The landmark study by Kahneman & Tversky (1984) exemplified the framing bias in its most frequent form of "gain vs. loss". The two researchers asked physicians to select between two medical treatments for an infected population of 600 people. The possible outcomes were: "If program A is adopted, 200 people will be saved. If program B is adopted, there is a one-third probability that 600 people will be saved and a two thirds probability that no people will be saved." In this case, 72 % of the participants chose program A. With another group the same outcomes were framed in the following negative manner. "If program C is adopted, 400 people will die. If program D is adopted, there is a one-third probability that nobody will die and a two-thirds probability that 600 people will die." In this case, 78 % of the physicians chose program D, the 'all or nothing' alternative.

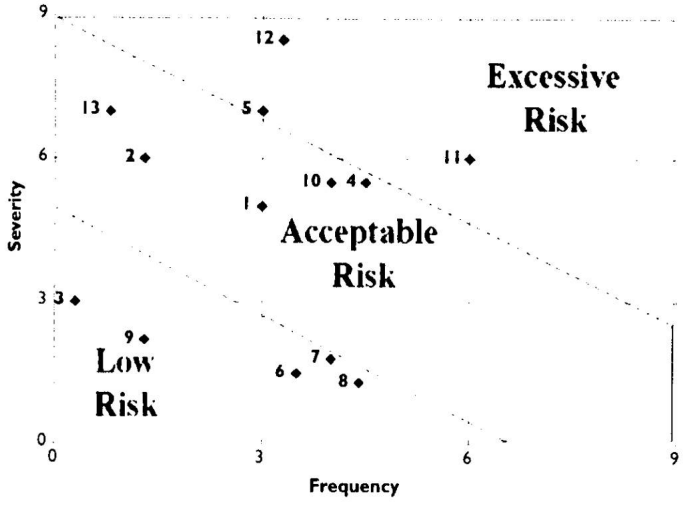
It is apparent that Plan A is equivalent to Plan C, and Plan B to Plan D, yet the different presentations led to dramatically different responses. The choices reflect the fact that people are risk averse when faced with definite gains however small, but risk tolerant when the alternative appears to be a greater loss.

Since it would be inefficient to try to control all risks, management should determine the 'threshold of pain' of loss below which risks would be considered inconsequential. Those that exceeded the threshold would be investigated in more depth and be prioritized.

Once risks have been evaluated, they have to be prioritized in order to determine where to focus resources. One common way for rapidly determining this is by multiplying a risk's probability by it severity, and those with the greater product become the higher priority. Another way is to plot the risks on a Risk Map, as shown in the figure below, and those in the 'Excessive Risk' zone are higher priority.

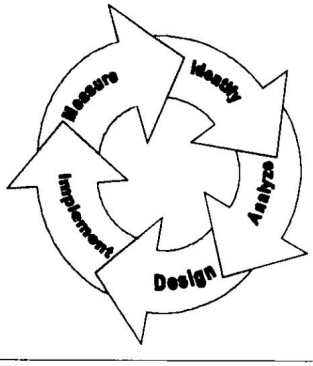
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

FIGURE 2
RISK MAP



1 Contracts
2 Political Risk
3 Product Failure / Liability
4 Key Personnel
5 Health and Safety
6 Trade Credit
7 Disruption of Operations
8 Environmental Occurences
9 Key Suppliers
10 Capital Availability
11 Weather
12 Price of Raw Materials
13 Reputation

Questions the Board should ask about the ANALYSIS of risks



- What techniques are used for evaluating the risk appropriate?
- Are there psychological biases that could impair the objective evaluation of the risk?
- What is the organization's threshold of pain?
- How are the risks prioritized?

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

DESIGN

After the risks have been prioritized the organization has to determine the optimal way to manage them. Often a combination of responses is used to produce a 'defense in depth'.

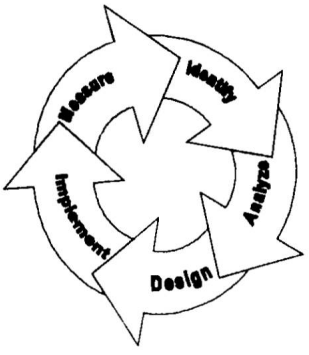
These responses fall into five general categories:

- Acceptance – The organization absorbs the risk as a part of doing business, for example, choosing to continue production of a profitable product that may soon become obsolete.
- Avoidance – The organization steps away from situations that could produce a risk exposure, for example, circumventing certain countries in order to avoid inherent political risks.
- Control – The organization looks to minimize the occurrence or effects of a risk, for example, developing succession plans to minimize the disruptions in case a key person is incapacitated or departs.
- Transfer – The organization moves the risk to a third party. This could be done contractually via such mechanisms as hold harmless agreements or limitations of liabilities.
- Finance – There are a number options including:
    - hedging agreements, including futures, forwards, swaps etc.;
    - insurance
    - hybrid or alternative risk financing programs which combine the characteristics of different financial disciplines – or example, a catastrophe bond which is a form of debt financing that embeds the trigger mechanism of an insurance policy that must be tripped in order for the organization to receive the funds.

For the responses to be considered effective the organization must also consider two factors. First is to ensure that the residual risk remaining after the implementation of responses is within the organization's tolerance for loss. The second factor is similar to the concept of 'do no harm' in medicine. The organization must be careful that its responses do not introduce a completely new set of risks. For example switching from paper to electronic records may reduce the risk of loss of information, but there may be new and bigger risks with Information Technology security.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Questions the Board should ask about the DESIGN of risk responses



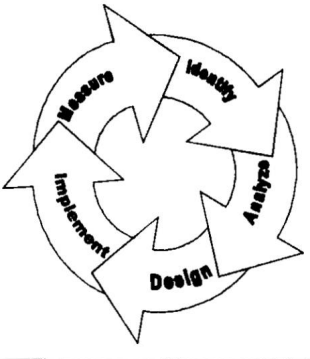
- What are the responses for the higher priority risks?
- Is the residual risk within the organization's tolerance level?
- Does the response introduce any new risks?

IMPLEMENT

From designing the responses, the organization moves to implementing them. From a governance point of view this means identifying someone with the mandate to implement and manage the response, in alignment with their responsibilities and skill set. For example a Chief Operating Officer would be more appropriate for managing supply chain risks and not the head of Human Resources. If a response is not in place, then a clear timeline should be set for its implementation.

With the implementation of risk management there also should be a system for verifying that the responses are in place and are functioning. This could be done through a system of self reporting, but often is done as part of the duties of the audit team.

Questions the Board should ask about IMPLEMENTATION of risk responses



- Who is managing each of the responses?
- If a response is not in place, what is the timeline for implementation?
- What is the process for verifying that responses are in place?

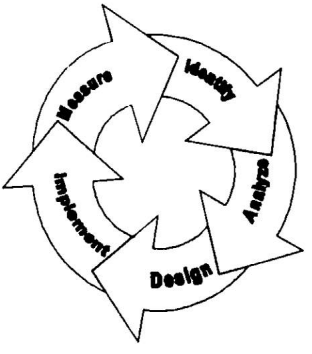
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

MEASUREMENT

As the risk management system operates, information on its performance should be measured. Some sample metrics include safe days of operations, total cost of risk, level of shareholder confidence or new opportunities pursued. However, receiving the data alone is not a useful exercise. To be of value the data must be:

- compiled into a usable format and analyzed;
- communicated to the appropriate groups – it is worth noting that while this information is often provided to audit personnel, they usually focus on compliance issues. Other bodies, for example those managing the risk responses, must be engaged in the process of using the information to enhance risk management;
- carried forward as feedback in the start of the next risk management cycle.

Questions the Board should ask about MEASUREMENT of risk responses



- What metrics are used to measure the effectiveness of the risk management program?
- How is the information used to improve the risk management process?

The board participates in Enterprise Risk Management by:

- providing oversight on the need for and level of sophistication of risk management required by the organization;
- concurring with or, if necessary, disputing the level of risk tolerance established by management;
- ensuring that risk management is carried out on a continuous basis.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

On occasion the board can be more directly involved in managing risk by serving as a source of advice to senior management during a crisis, or by managing cases that involve the loss or impairment of the CEO.

The audit committee of the board is often tasked with ensuring that risk management systems are in place and assessing their effectiveness. Sometimes audit processes will also include helping in the identification of risks and developing responses. If the audit committee is overloaded, or if risk management is of great concern, there may be a separate risk management committee.

Finally there is the role the individual board members. They should keep the right state of mind about risk management; not paranoia, but a healthy respect for risk issues. As well they can bring their experience and skill sets to help in making better decisions; just as a member would look at the profitability of each business opportunity, they should also think of the risk aspect. To help manage risks on an organization wide basis a board member does not need to know all the answers, just be able to ask the right questions.

References

[1] Felton, Robert & Fritz, Pamela. "McKinsey Quarterly 2005 Special Edition: Value and Performance". *The View From The Boardroom*. McKinsey Quarterly.

Gilovich, T., Griffin, D. & Kahneman, D. (2002) "Heuristics and Biases: The Psychology Of Intuitive Judgment". New York: Cambridge University Press.

Greenhill, James. *Psychological Factors in Risk Management*. Assurance, vol. 72 (4), Jan. 2005.

Greenhill, James. *Risk Management Processes: Cyclical vs. Linear Systems*. Assurance, vol. 72 (1), Apr. 2004.

HM Treasury (UK). Management of Risk–A Strategic Overview, January 2001.

Kahneman, D., & Tversky, A. (1984). *Choice, Values, and Frames*. American Psychologist, vol. 39, pp. 341-350.

Leech, Tim. *Communication by Consensus: Breaking the Risk Barriers*, Risk Management Magazine, April 2003.

Mason, Richard. *Lessons in Organizational Ethics from the Columbia Disaster: Can A Culture Be Lethal?*. Organizational Dynamics, Vol. 33 (2) 2004.

Nadler, David. "Building Better Boards – A Blueprint For Effective Governance". Jossey-Bass Publishing. 2006.

[2] Protiviti, "U.S. Risk Barometer – Survey of C-Level Executives with the Nation's Largest Companies". Feb. 2006.

Treasury Board of Canada. Review of Canadian Best Practices in Risk Management, 1999.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.