Assurances et gestion des risques
Insurance and Risk Management

Best Practices and Structures in Organization / Enterprise Wide Risk Management Frameworks

James Greenhill

Volume 71, Number 2, 2003

URI: https://id.erudit.org/iderudit/1092868ar
DOI: https://doi.org/10.7202/1092868ar

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. (2003). Best Practices and Structures in Organization / Enterprise Wide Risk Management Frameworks. *Assurances et gestion des risques / Insurance and Risk Management*, *71*(2), 331–339. https://doi.org/10.7202/1092868ar

Technical Study

by James Greenhill

BEST PRACTICES AND STRUCTURES IN ORGANIZATION/ENTERPRISE WIDE RISK MANAGEMENT FRAMEWORKS

A number of organizations are taking active steps to build organization/enterprise wide risk management frameworks to identify, assess and mitigate risks on a continuous self-improving basis with the ultimate goal of helping the organization achieve its goals and objectives. The types of organizations that are looking to implement this are wide ranging, from corporations looking to build shareholder value to governments wanting to protect their citizens and infrastructure. This paper gives an overview on drivers behind implementation of these frameworks, best practices used in such systems and how the focus of risk management can vary depending on an organization's structure.

Drivers

Internal drivers behind implementing organisation/enterprise wide risk management structures include the desires to :

– **protection of the organisation.** This means actively reviewing its risk profile on a holistic basis and ensuring that risk management systems can respond appropriately. There is ample evidence indicating that this is not a wasteful endeavour. One study carried out by Mercer Consulting on Fortune 1000 companies found 100 cases where a company's stock price declined more than 25 % in a single

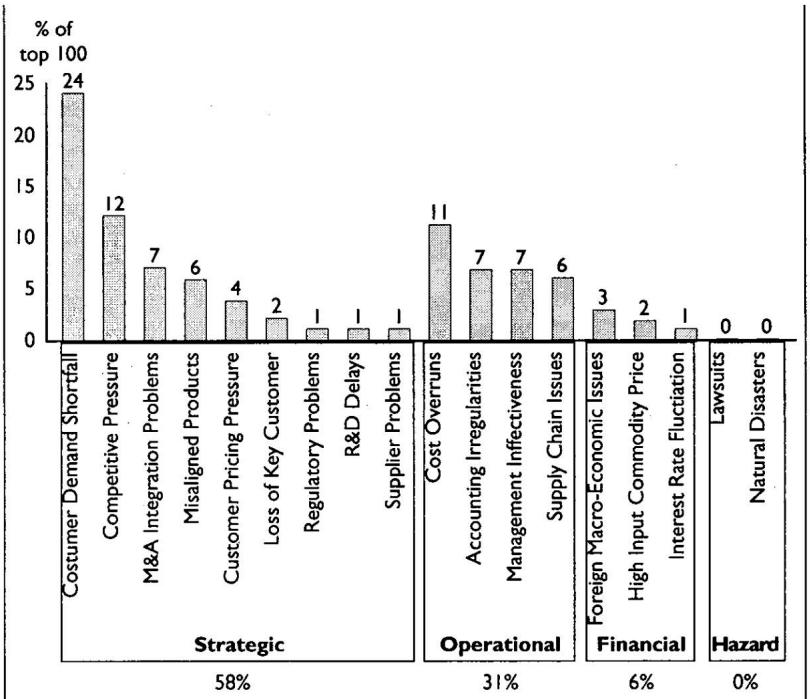
The author :

James Greenhill is an Assistant Vice President with Marsh who carries out work in the areas of risk assessment and alternative risk financing. He is currently with Marsh's Montreal office.

month due to a variety of risk events, as indicated in the diagram below, and that in many cases the losses could have been mitigated using risk management techniques such as derivatives, audit procedures and scenario planning.

– **use of risk management as a competitive advantage.** For example, in a survey conducted by the Economist Intelligence Unit and MMC Enterprise Risk, 84 % of respondents believed implementing enterprise risk management could improve their price/earnings (P/E) ratio or cost of capital.

RISK EVENT PRECIPITATING STOCK DROP (NUMBER OF COMPANIES)



MCC Research

- Investigated risk factors behind the 100 largest one month drops in shareholder value amongst Fortune 1000 companies between 1993-98
- Found top 100 stock drops
- Identified triggering event
- Determined causes of triggering event
- Categorized primary cause
- Analyzed results and implications

There are also a number of external drivers including :

– **demands by regulatory bodies.** Two examples are KonTraG in Germany that imposes risk management requirements on public companies and the Basel Committee on the development of risk management practices in financial institutions.

– **recommendations for risk management by other groups.** Two examples are the Turnbull Report released by the Institute of Chartered Accountants of England and Wales and the Dey Report for companies listed on the Toronto Stock Exchange.

Best Practices

There is no 'one-size-fits-all' design of an organization/enterprise wide structure or the placement of the head of risk management within it. Several factors must be considered including the structure of the organization and level of sophistication of the systems needed to manage its risks. However there are a number of 'best practices' common to all of them.

In the overall organisational structure and culture this includes :

– **visible senior management support.** Setting the 'tone from the top' is the key issue for the establishment and continuation of a comprehensive risk management process. This can either be in the form of establishing senior level risk management structures such as risk committees or via direct communications stating the value of risk management to the organization.

– **development of a culture which supports the process.** This may require a change management process to move from a culture that view risks in a silo centric manner and only reacts to risks that are of immediate danger to an organization that manages risk on holistic and proactive basis.

– **link of risk management with the business planning process.** For risk management to provide maximum value it must take place early in and be designed to work in concert with the planning process. Effective risk management is difficult to achieve if it is done as an afterthought to the planning process. An advantage of making the link is that an organization may discover that it can exploit opportunities that it had previously considered 'too risky'.

– **team or committee structure supporting the risk management process.** This helps to develop a strong risk management culture and increases the ability of the organization to detect risks,

enhances its ability to share risk management information and expands its capability to implement risk management processes.

– **establishment of a dedicated corporate risk management function/leader.** This communicates to internal and external stakeholders that risk management is a process that is taken seriously by the organization not only at a high strategic level, but also on an operational day-to-day level. As well this person serves as a clear 'go to' point for those who have risk concerns or issues, but are unsure how bring this to the attention of the management of the organization.

– **balance between local and centralized control**. The responsibility for specific risks should always be with the individuals who generate the risk. However how risks are identified and managed on an organization wide basis will vary with the nature of the organization's operations and structure. One way to view the control process is set out further on in this paper.

In terms of specific risk management processes this includes :

– **development a common risk language.** For an organization to develop a universal understanding of risks they must have a clear way to communicate about risks. Different departments and operations tend to develop their own specialized technical language that is not understood by the 'uninitiated' which can lead to misinterpretation when trying to review risks on a holistic basis.

– **promotion of an organizational philosophy and culture that says everybody is a risk manager.** This is to develop the idea that every person in the organization has some capability to help the organization control its risks. Besides operational benefits, this also helps to build a supportive culture.

– **opening communications channels for sharing risk information**. As well as developing a common risk language so that different groups maintain a common view of risk, there have to be pathways by which risk information can be shared. This is a balance between sharing enough information so that risk management processes can be effective and that the right people receive the right information, and at the same time ensuring that people are not overwhelmed with unnecessary information.

– **communication of risk management performance within the organization.** If properly done, this process allows for the reenforcement of good risk management practices in an organization and indicates where risk management processes have to be improved in other parts. At same time this has to be carefully managed so that

it develops a supportive culture and is not seen as a way of laying blame for the occurrence of an adverse risk event.

– **demonstration of value of risk management (to internal or external stakeholders).** This is another way to build a supportive culture and way to reap a return on investment in risk management. The demonstration of this value can either by qualitative or quantitative measures.

– **risk identification being done as an on-going process.** Since organizations are dynamic in their operations, the types of risks they are exposed to and their level of exposure are also dynamic. Because of this an organization should review its risk profile on a regular basis.

– **continuous monitoring of results of risk management processes**. This ensures that the management systems are effectively controlling risks and are adjusted as required to manage changes in the organization's risk profile as identified by on-going processes.

– **risk management function providing guidance to business units via tools or consulting**. While team and committee structures allow for the sharing of risk information and determination of policies, an organization needs to develop services to help train people in risk management and to implement risk management systems.

– **work with what is already in place with the organization.** This includes coordinating with other functions of the organization (e.g. operational processes, strategic planning, quality processes, etc.); where able working with current systems to prevent unnecessary duplication and cost; and levering existing skill sets, technology or processes to enhance the risk management process.

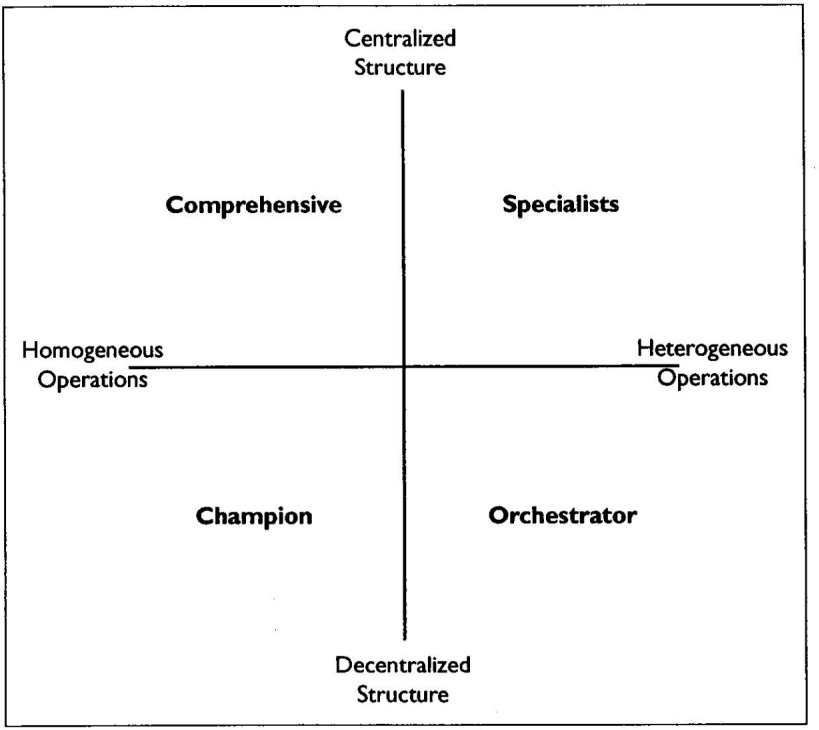
Organization Types And Associated Risk Structure Models

The responsibilities of the head of the risk management function can be divided into three parts :

– **coordination of risk management activities throughout the organization.** This includes the exchange of risk information, implementation of best practices, and providing internal guidance to others in their development and operation of risk management processes.

– **act as the leader of risk management.** This includes setting rules, policies and standards with senior management and/or board approval which others in the organization must comply with.

– **management of specific risk areas directly.** This means being responsible for and carrying out all aspects of risk management (e.g. identification, assessment and mitigation) in select areas.



The extent of their responsibility for different 'risk areas' whether divided along functional or geographical lines, depends on the role the head of risk management plays in an organization. The diagram below outlines ways the risk management function can be classified in the organization's structure depending on whether it operates in a centralized or decentralized manner and if its operations are heterogeneous (i.e. a wide variety of lines of business or products) or homogeneous in nature (i.e. little differentiation in lines of business or products).

Operations that are centralized and homogeneous can allow for a single individual to have in-depth knowledge about the business and the nature of its risks. With this the person would be able to develop risk management processes, monitor their effects and enforce any deviations from standards. The diagram below outlines the role of the head of risk management in the 'Comprehensive' model (gray areas indicate responsibility) that would cover all three parts in the

risk management function for all risks. This can often be found in small to medium size organizations with no complex operations.

Comprehensive	Risk Area #1	Risk Area #2	Risk Area #3	Risk Area #4	Risk Area #5
Co-ordinates risk management activities					
Designated leader of risk management					
Directly manages specific risk areas					

Operations which are centralized and heterogeneous would require specialists who understand the different portions of the organization's operations and how they relate to corporate level goals and objectives. With a centralized structure the team would be able to closely monitor risk management processes and enforce any deviations. In this case the head of risk management would focus his efforts and take full responsibility for managing some of the organization's risks. He would also fulfill a secondary role of assessing and developing mitigation strategies on a holistic basis in conjunction with other risk management specialties. The diagram below outlines the role of the head of risk management in the 'Specialist' model. An example of this is a company where the Chief Financial Officer manages specific financial risks and is supported by specialists who focus on hazard and operational risks.

Specialist	Risk Area #1	Risk Area #2	Risk Area #3	Risk Area #4	Risk Area #5
Co-ordinates risk management activities					
Designated leader of risk management					
Directly manages specific risk areas					

Operations that are decentralized and heterogeneous mean that the head of risk management would develop processes to protect the whole organization and would help adapt them to each operation. Simultaneously the business units would provide risk and risk management information to him. He would then standardize the information that would allow senior management to understand the organization's complete risk profile. Organization functions that carry out risk management activities (i.e. audit, risk management, compliance, insurance) would report to this head of risk management, thus integrating all control related activities. The diagram below outlines

the role of the head of risk management in the 'Orchestrator' model. An example of this structure could be a conglomerate with diverse subsidiaries and strong central office control.

Orchestrator	Risk Area #1	Risk Area #2	Risk Area #3	Risk Area #4	Risk Area #5
Co-ordinates risk management activities					
Designated leader of risk management					
Directly manages specific risk areas					

Operations that are decentralized and homogeneous imply that many functions and responsibilities are pushed down into subsidiary or business units. The head of risk management may then act more as a process champion, sharing best practices amongst business units and ensuring each one meets organization's standards in risk management. The development of holistic mitigation strategies would come from a partnership process with peer groups in the organization. Enforcement of standards would reside with the individual units, with major exceptions or deviations being handled by senior management with the assistance of the head of risk management. The diagram below outlines the role of the head of risk management in the 'Champion' model. An example of this structure could be a holding company that maintains only a small headquarters function or only partial ownership of its subsidiaries.

Champion	Risk Area #1	Risk Area #2	Risk Area #3	Risk Area #4	Risk Area #5
Co-ordinates risk management activities					
Designated leader of risk management					
Directly manages specific risk areas					

Conclusion

While a number of organizations are in the evolutionary process going towards an organization/enterprise wide risk management the final results will be varied as the individual frameworks are adapted to the organization's structure and integrates those risk management best practices that will support the achievement of its goals and objectives.

Bibliography

Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, 2003.

EIU (Economist Intelligence Unit) and MMC Enterprise Risk, *Enterprise Risk Management – Implementing New Solutions*, 2001.

Elliott, Michael W., « The Emerging Field of Enterprise Risk », *MMC Views*, vol. 3, 2001.

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

Strategy Unit, UK Government, *Risk : Improving Government's Capability to Handle Risk and Uncertainty*, 2002.

Treasury Board of Canada, *Best Practices in Risk Management : Private and Public Sectors Internationally*,1999.

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

Culp, Christopher L., *The Risk Management Process – Business Strategy and Tactics*, John Wiley and Sons, 2001.