

# LEADERSHIP AND RISKS DURING A GLOBAL FINANCIAL CRISIS

By Dr. Kris R. Nielsen<sup>1</sup>, Dr. Patricia D. Galloway and Jack L. Dignum

**PEGASUS GLOBAL HOLDINGS, INC.**

## Introduction

To address the world's most pressing needs, major investment must be undertaken to upgrade the world's aging infrastructure. New capital investments are also necessary to devise solutions for global problems concerning climate change, natural disasters, aging communities and growing populations; all against a backdrop of a global financial crisis. Further complicating the investment decisions are that the projects to be undertaken are not small-in fact they have become larger than most individual companies or governments can singularly undertake. They have taken on the term "mega project."

A capital construction mega-project is defined as a project which has a completed cost of at least 1 billion dollars (US). Other characteristics of mega-projects may include:

- A multinational project execution team
- A long total project time
- Multiple consultants and contractors, some linked in consortium arrangements
- Multiple project phases or stages
- Multiple stakeholders and investors

The focus of this paper is on the governance and enterprise risks for civil mega projects from the perspective of governments, private corporations and the Senior Executive levels of these organisations. Successful achievement of mega-project goals is difficult in a stable economic environment; however, in an unstable economic environment such as that encompassing the world in the last 2 years successful achievement of mega-project goals becomes even more difficult and unlikely. Over the last 24 months a growing number of mega-projects have had to deal with the impacts of the global economic crisis. Depending on the stage of development at which a mega-project rests, the issues of greatest concern appear to be:

- Securing financing and investment.
- Managing enterprise risk in an unstable economic environment.
- Planning and execution risk profile changes due to an unstable economic environment.
- Strategic execution adjustments.
- Project life cycle changes resulting from unstable economic environment.

The most common barrier to the development and implementation of an effective and efficient risk management program is that the risk management program was developed or adopted without the benefit of a strong contextual definition within which the risk management program was to operate across the various levels of the organisation. The concepts of risk management go back more than thirty years when Dr. Kris Nielsen began his research based on practical issues and problems that were arising on projects around the world. Although risk management has taken on a common meaning in the board room, it is the experience of the authors that the understanding of risk management in organisations that are taking on these mega projects may not extend much past the board room. In addition, in times of financial crisis, cost cutting measures take place and unfortunately, these cuts have appeared in the very place they should be strengthened-in the area of risk management. Therefore the focus of this particular paper has been limited to the critical need for an organisation or public entity to first establish the contextual definition within which any risk management program should be developed and implemented in order to lead and manage risk during the world's financial crisis.

## Risk in General

Profits live on the edge of risk. As noted by the London Stock Exchange in "Corporate Governance - A Practical Guide":

Profits are the reward for successful risk-taking in a modern competitive economy. Companies that are overly cautious will miss opportunities and are unlikely to succeed in the longer run. Even more certain failure awaits those who take risks recklessly. The board's challenge, therefore, is to ensure risk is managed effectively in the business, not to

---

<sup>1</sup> Dr. Kris R. Nielsen is Chairman and President of Pegasus-Global Holdings located at 1750 Emerick Road, Cle Elum, WA 98922, USA [k.nielsen@pegasus-global.com](mailto:k.nielsen@pegasus-global.com), Dr. Patricia D. Galloway is CEO of Pegasus-Global Holdings and is Past President of ASCE [p.galloway@pegasus-global.com](mailto:p.galloway@pegasus-global.com), Jack. Dignum is Senior Vice President and COO of Pegasus-Global Holdings, [j.dignum@pegasus-global.com](mailto:j.dignum@pegasus-global.com).

eliminate it altogether. The board has to be proactive in its oversight role and to recognize that the risks confronting a business are constantly changing.<sup>2</sup>

An organisation must dance *on the edge* of risking more than the organisation can afford to lose if it is to realize a margin higher than the organisation needs simply to survive. The Malaysian Code on Corporate Governance agrees that "... *business decisions require the incurrence of risk*" but also tempers that understanding by noting that:

The target is to achieve a proper balance between risks incurred and potential returns to shareholders.<sup>3</sup>

At a fundamental level organisations exist to take risks and turn them into rewards. And thus the dilemma faced by organisations around the world: meeting or exceeding goals means the organisation must willingly take risks, and every risk carries with it a potential for reward and a concomitant potential for loss. As stated so succinctly within the Malaysian Code, the target of every organisation is to achieve a proper balance between the risks, the potential rewards and the potential losses.

Since the mid-1990's immense attention has been focused on improving the governance of both public and private organisations; attention which has not been limited to the United States but has become a global issue. Any search of the internet will identify "governance" issues being examined in Africa, Asia, Australia, Europe, North America and South America. More often than not in recent years the concept of "risk management" has been included as a major element of good governance. Originally risk management as a topical issue was focused on aspects of an organisation's financial risk and reporting; does the organisation manage and accurately report on the financial risks faced by the organisation during its operations? Such risks were limited to issues such as the cost of materials and equipment, capital costs, economic conditions, etc. More recently risk management has started to evolve beyond the purely financial to encompass the more esoteric and harder to define elements of corporate risk, as noted in November 2006 by the Australian Stock Exchange (ASX) in its "Review of the Principles of Good Corporate Governance and Best Practice Recommendations":<sup>4</sup>

There has been a number of recent developments in the understanding of risk particularly post-Basel II. ...'Risk' is not just financial risk. It includes operational, compliance and strategic external risks. It also clearly recognised that these other risks can have a significant impact on the financial position and reputation of a company and investor sentiment in relation to the company.

Australia and the United States are not the only countries which have experienced a re-definition of risk in so far as it pertains to good governance practices. In Russia for example:

Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an intimate knowledge of the organisation, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.<sup>5</sup>

The logical question for an organisation's governing board and senior management is: If "risk" as an element of good governance is evolving to include risks factors beyond simple financial risk, from whence do those risks flow? The short answer is "everywhere". There is no single source globally which provides a "standard risk register" and every country appears to have defined non-financial risk slightly differently. However, those international sources generally agree that non-financial risk flows from any source which has the potential to impact an organisation's attainment of strategic goals and objectives. A review of international best practices reveals that non-financial risks can be generally grouped into 7 categories:

1. Environmental Risks
2. Political Risks
3. Social/Cultural Risks
4. Technological Risks
5. Procurement/Contractual Risks
6. Delivery/Operational Risks
7. Economic Risks

Risks arising from each or any of those sources can impact an organisation's ability to reach its strategic goals and objectives which in turn can impact an organisation's financial condition. The AXS refers to such non-financial risks as "*sustainability/corporate responsibility*" risks.<sup>6</sup>

---

<sup>2</sup> Corporate Governance, A Practical Guide, London Stock Exchange and RSM Robson Rhodes, LLP, July 2004, page 40

<sup>3</sup> Malaysian Code on Corporate Governance, Finance Committee on Corporate Governance, Securities Commission, March 2000, Section 4.17, page 22

<sup>4</sup> Review of the Principles of Good Corporate Governance and Best Practice Recommendations, ASX Corporate Governance Council, 2 November 2006, Principle 7, page 17, paragraph 71

<sup>5</sup> A Risk Management Standard, Russian Risk Management Society, FERMA Standards, 2004

<sup>6</sup> Review of the Principles of Good Corporate Governance and Best Practice Recommendations, ASX Corporate Governance Council, 2 November 2006, Part B, Principle 7, page 29

The next logical question is who within the organisation is responsible for ensuring that the organisation's risk management program has correctly identified, quantified and managed risk, including non-financial risk? The answer is predictable:

**Risk is a Board matter:** the Board (or equivalent) view themselves as ultimately accountable for risk management ...<sup>7</sup>

ASX also made it clear as to who bore the responsibility for risk management within an organisation:

The company board has ultimate responsibility for risk oversight and for determining the company's risk profile. As part of its oversight, each board will need to determine what risks are "material" for a company of its type and size and how they should be taken into account in the process of sign-off.<sup>8</sup>

In summary, the definition of what constitutes a "risk" to an organisation has and continues to evolve internationally. As that evolution progresses, boards of directors and senior management find their role and responsibility relative to the identification, quantification and management of risk growing faster than the staff and programs available within the organisation can evolve to support that role and those responsibilities. Consequently boards of directors and senior management find themselves in a position of having to act quickly to build the internal capability to enable the total risk environment which may threaten the attainment of the organisation's goals and objectives to be identified, quantified and managed. However, in that drive to install that capability, boards of directors and senior management need to heed a warning issued by British Standards:

There can be no "one size fits all" approach to the application of risk management. Risk management should be tailored to suit the organisation's unique circumstances and reflect as a minimum the organisation's structure, its legal and regulatory context, the decision making process, reporting requirements, insurers' and funders' requirements, shareholder expectations, and the markets within which the organisation operates.<sup>9</sup>

The past 10 years has seen organisations investing significant sums in developing or obtaining risk management programs which were intended to be responsive to the demand for better corporate governance. Recently a growing number of regulatory agencies, public stakeholders, organisation boards of directors and senior corporate managers are finding that the installation of a risk management program which they believed would enable them to identify, assess, treat and report on risks faced by the organisation have failed to meet either the stakeholder's or the organisation's objectives relative to managing risk. The risk management programs and systems installed did not live up to expectations.

### **Risk Management in General**

By now it would be difficult to find any major organisation in the world that has not heard of, been trained on, or has installed some type of risk management program. In fact, the mantra of risk management has become accepted and ingrained across international borders, reaching into countries that have little prior experience with any aspect of private organisation governance practices. For example, in adopting guidelines to govern the formation and operation of two "pilot banks" in China, governance was a significant enough concern to lead to the promulgation of 26 Articles intended to direct the operations of those banks. One of the 26 Articles was devoted to risk management:

Each pilot bank shall adopt a system of risk management, which covers the credit risk, market risk and operational risk, and is effective in identifying, measuring, monitoring and controlling risks.<sup>10</sup>

Globally any document dealing with risk management in any form has at its core that same definition of a risk management program:

8. Identification
9. Quantification
10. Monitoring
11. Treating/Controlling
12. Reporting

In practically every book or article on risk management published in the past decade these five elements are presented in just that order and, in truth, every effective risk management effort undertaken by an organisation passes through those elements in the order they are presented. It is axiomatic that:

---

<sup>7</sup> Draft BS 31100 Code of Practice for Risk Management, British Standards, Section 4.3, page 15, line 382 - 383

<sup>8</sup> Review of the Principles of Good Corporate Governance and Best Practice Recommendations, ASX Corporate Governance Council Explanatory Paper and Consultation Paper, 2 November 2006, Principle 7 – Recognise and manage risk, The Scope of Principle 7, paragraph 74, page 17

<sup>9</sup> Draft BS 31100 Code of Practice for Risk Management, British Standards, Section 2.8, page 9, line 176 - 180

<sup>10</sup> Guidelines on Corporate Governance Reforms and Supervision of Bank of China and Construction Bank of China (China Banking Regulatory Commission), The People's Government of Zhejiang Province, 2006-7-2 18:12:24, Chapter II, Article 7

13. First you identify the risk elements,
14. Second you quantify each of the risk elements identified in a matrix which establishes both probability of occurrence and level of impact (i.e. time and/or money) should that risk element manifest;
15. Third you monitor the organisation or business or project to ascertain if and when a particular risk element has manifest;
16. Fourth you take those actions necessary to mitigate or eliminate (treat or control) the impact of the risk element on the organisation, business unit or project; and,
17. Fifth, you report how effectively your organisation was at minimizing, mitigating or controlling risk you have encountered over a defined period of time.

Of course, it is not as simple to successfully undertake and execute each of these steps as it sounds; risk management is in the end an involved and continuously evolving process as each day and every decision made by an organisation eliminates some risk elements while at the same time introducing new risk elements into the organisation's business environment. But it can generally be said that managing risk involves implementing and completing a series of steps taken in a certain sequential order.

Those sequential steps have become so formulaic and ingrained in the global lexicon that it seems as though there should be a single, accepted risk management program which could be purchased off the shelf and installed in an organisation much the same way that various other productivity software systems purchased by organisations are today. There are companies which market "risk management programs or systems" which assert that their program is easy to install, simple to use and practically self-perpetuating. Many of these packaged risk management systems have at their core a computer-generated probabilistic program which can generate very sophisticated models of risk from both risk element probability of occurrence and impact perspectives. Indeed, these software systems are extremely powerful and can, *if properly used*, organise and generate valuable data which will aid an organisation to maximize the effectiveness of their risk management program. However, those software systems are not in and of themselves risk management programs, they are simply powerful computer-driven tools which can improve and enhance the ultimate efficiency and effectiveness of an organisation's risk management program, *if properly used*.

Many organisations have initiated their risk management program by purchasing a software modeling system, assuming that the "software is the solution" to their risk management "problems". After installing that sophisticated and powerful risk management software, a number of those organisations now find themselves wondering why their ability to effectively and efficiently manage risk across the organisation has not improved. This dissatisfaction appears to be particularly true of larger, multi-national organisations with multiple units or product/service streams which provide variety of goods or services globally.

However, one of the reasons why from an organisational perspective risk management programs have failed to meet expectations is that the process by which an organisation actually manages risk has been confused with the process by which an organisation should develop, install and implement a risk management program.

### **Development of a Corporate Risk Management Program**

By necessity, ***risk is actually managed*** following a bottom-up process; that is, it begins with the lowest element in the process – the identification of the individual risk elements – and moves on through each step to the monitoring and control of each individual risk element. However, the ***development of an effective and efficient risk management program and system*** within and across an organisation must be a top-down process. It is in confusing the bottom-up process of actively managing risk with the top-down process of developing a risk management program that has led to the situation faced by organisations today: which is simply that the risk management programs and systems in place do not meet the needs and expectations of the organisations which have invested so heavily in those systems.

### **Risk Management Program Context**

As noted earlier, there has been a growing trend to include the concept of risk management as part of good governance of an organisation. For example, the Organisation for Economic Co-Operation and Development (OECD) stated in its Principles of Corporate Governance:

Users of financial information and market participants need information on reasonably foreseeable material risks ...

Disclosure about the system for monitoring and managing risk is increasingly regarded as good practice.<sup>11</sup>

The Association of Insurance and Risk Managers and The National Forum for Risk Management in the Public Sector, jointly concluded that:

Risk management should be a continuous and developing process which runs throughout the organisation's strategy and implementation of that strategy. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, future.

It must be integrated into the culture of the organisation with an effective policy and programme led by the most senior management. It must translate the strategy into tactical and operational objectives, assigning responsibility throughout the organisation with each manager and employee responsible for the management of risk as part of their job

<sup>11</sup> OECD Principles of Corporate Governance, Organisation for Economic Co-Operation and Development, Paris, France, 2004, Part 2, Principal V. Section A, Item 6, page 53

description. It supports accountability, performance measurement and reward, thus promoting operational efficiency at all levels.<sup>12</sup>

In the past few years the definition of risk management has expanded beyond that of financial risk only, while the responsibility to govern that expanded risk has risen to the level of the board of directors and senior management of an organisation and, as noted in the citation directly above, is now expected to become “*integrated into the culture of the organisation*”. An organisation’s management of risk, including non-financial risk, is now one of the fundamental measures of good governance practice in many countries around the globe.

There is almost global acceptance of the fact that managing risk is good for an organisation and its stakeholders and ignoring risk is bad. There is almost global acceptance that risk management is a systematic method by which an organisation identifies, quantifies, treats and reports risk. And there is growing global acceptance of the fact that the definition of risk has grown significantly beyond simple financial risk. However, as noted above, even with that almost global acceptance and unanimity concerning risk management definitions and methodology, there is no “*one-size-fits-all*” risk management program which will work across every organisation globally.

The first dynamic which prevents the concept of there ever being a uniform or standard risk management program is **every organisation is to some extent unique**. Organisations, even organisations competing in the exact same industries, do not have identical goals, objectives, standards, organisational structures, operating systems, staffing profiles, execution and operating locations, etc. Conoco-Phillips and British Petroleum may both be in business to find, refine and market petrochemical products globally, but they definitely are not identical twins from a corporate perspective. They have just as many elements unique to their organisations as attributes that they share in common, and it is the unique elements of each that prevent the successful adoption of an identical risk management program by both.

The process of managing risk on a discrete project depends on the development of a “*risk profile*” unique to the conditions within which that project will be executed. That risk profile identifies each risk to the achievement of the project goals and objectives, delineates the probability of the risk manifesting during the execution of the project and the impact to the project should the risk manifest, establishes proactive management response plans for avoidance and mitigation of the risk element and, finally, creates the project structure by which the risks will be monitored and managed during the execution of the project. Even companies which operate in a single product, single market, and single service environment understand that each project’s risk profile is to some extent unique to that project. The more unique elements which exist within an organisation the more important it is to establish a contextual definition within which a risk management program can fulfill its intended purpose. The question is now: where does an organisation begin the process of preparing a contextual definition?

As noted earlier, there is a difference in where risk is actually managed and where the development of a risk management program should begin. Risk is actually managed following a bottom-up process. However, the authors have also found that the development of an effective and efficient risk management program within and across an organisation must be a top-down process, which begins with the developing a contextual definition within which the risk management program is to operate. Developing a corporate contextual definition from the top-down is like looking through a funnel with the narrow end at the top. The development of the contextual definition is best implemented via a “question and answer” process which begins with the board and senior management of the organisation and travels successively through the organisation to the level at which risk must actually be managed. There are two elements of a full contextual definition for an organisation, each of which is built by asking, and answering, some basic questions:

18. Internal Elements – questions which go to the internal operations of the organisation
19. External Elements – questions which go to the external demands on the organisation

Internal elements are the ones about which most organisations are most knowledgeable as they involve those elements which are critical to the actual operations and management of the organisation. Internal element questions involve such issues as:

20. What core values must be reflected within the risk management program?
21. What is the organisation’s “appetite for risk”?
22. What is the organisation’s management philosophy?
23. What is the organisation’s market?
24. Where will the organisation operate?
25. What data and information must flow from the risk management program to meet each organisational level’s need for data and information
- 26.

The responses to the internal element questions assist in establishing the context definition critical to the internally generated operational parameters within which the risk management program must perform. This is part of the answer when an organisation tries to ascertain why its risk management program does not do “what it was intended to do” for the organisation. The risk management program may actually meet the needs of some components of the organisation very well while at the same time providing none of the functions needed (and expected) by other components of the organisation. The “contextual definition” within which the risk management program was developed was limited to a specific need and a specific component of the organisation and did not encompass any other needs.

---

<sup>12</sup> A Risk Management Standard, The Association of Insurance and Risk Managers and ALARM The National Forum for Risk Management in the Public Sector, 2002, Section 2, Risk Management, page 2

Until very recently there was little to no attention paid to developing a contextual definition which acknowledged or included any external elements. It is just within the last three to five years that international governance bodies have begun to apply risk management to external, non-financial risks faced by organisations. There is a growing global recognition that an organisation cannot limit its definition of a “stakeholder” to just those with a vested financial interest in the organisation. Stakeholders now include those who may be impacted by the operations of the organisation, such as, people who live in the area where the organisation will conduct its operations; the environment which might be impacted by the operations of the organisation; the political bodies who must review and respond to the public concerning the impact (or potential impact) of a organisation’s operations within a physical location; etc. In short, the definition of “stakeholder” in the eyes of those responsible for overseeing or even regulating how organisations govern themselves is quickly evolving beyond the traditional definition that a stakeholder is one that has a financial investment in the organisation. The new, evolving definition assumes that even those with no direct financial stake in the organisation have a vested interest in where and how that organisation operates. Part of that recognition has arisen in no small part due to the fact that those non-financial stakeholders can have a significant impact on an organisation’s ability to meet its goals and objectives while at the same time having no direct financial stake in the organisation’s success or failure whatsoever.

Given the evolution of both the definition of who constitutes a stakeholder and the breadth of risks that a risk management program should enfold, an organisation must expand its contextual definition to include an external element. As with the internal element, external elements which go into a full contextual definition of the organisation are developed by asking questions, such as:

- How will the organisation respond to environmental?
- How will the organisation respond to macro-economic?
- How will the organisation respond to social?
- How will the organisation respond to political impacts?

As can be seen the creation of the external elements of the organisation’s contextual definition is considerably more difficult and complex than the creation of the internal elements; nevertheless, the current trend globally is to include the external elements as critical to a definition of “good governance” and thus a measure of how well an organisation manages and controls risk. It is referred to differently depending upon where one looks: it is the operational “*environment*” in Britain, “*sustainability*” or “*corporate responsibility*” in Australia and “*corporate citizenship*” in the United States, but essentially the concept is the same:

The environment comprises the external factors which influence the management of risks for all organisations that are engaged in similar activities and over which an individual organisation has no direct control ...<sup>13</sup>

Once the board and senior management elements of the total organisation’s contextual definition have been set, the process moves progressively to the succeeding levels of the organisation’s structure, each of which builds upon the contextual definition prepared at the levels above it using the same process; developing questions and finding answers. The authors have found that the questions raised and answered at the higher levels of the organisation during the formation of the contextual definition are the more difficult to formulate and answer than are the contextual questions raised by lower levels of the organisation, where individuals are able to focus on a narrower set of issues and expectations.

### **Contextual Caution**

It would be irresponsible to leave the impression that there are not “risks” inherent in building a contextual definition for an organisation from the top-down (or the bottom-up up for that matter). It is human nature to believe that one’s own needs are more critical than anyone else’s needs. It is also human nature to believe that “*more is better than less*”. If the process is not supervised and controlled, by the time the contextual definition is “completed” it can be several thousand items long, which makes the definition essentially useless for its intended purpose. Here again the authors find that “*piling on*” generally flows from confusing development of a risk management program with actually using that program to proactively manage risk. During the development of the contextual definition the organisation should be focused on **why** a risk management program is necessary and not on defining who will run the program, what system(s) will be used, where the program will be located within the organisation or when the program will be used. “Why” is the contextual question; who, what, where, and when are the questions which define the components of the risk management program or system which will be developed in response to “why”.

The most effective way to avoid “piling on” is to form a management steering committee made up of members representing each of the levels of the organisation to oversee and control the development of the risk management program and system, including the development of the contextual definition. Once the committee is satisfied that it has defined all the reasons why it is developing a risk management program, then it will be ready to move on to develop one that truly fits the needs of the organisation, at every level.

### **Summary**

The process of managing risk has almost become routine: identify, quantify, monitor and control. However, the definition of what constitutes a risk to an organisation along with the definition of an organisation’s stakeholder continues to evolve. Attempting to develop, implement and manage risk by simply buying a risk management program or system is like attempting to provide an answer before you know what the question will be: even a good answer is useless if it doesn’t

---

<sup>13</sup> Draft BS 31100 Code of Practice for Risk Management, British Standards, Section 3.2.2, page 12, line 282 - 284

address the questions asked. The formation of a contextual definition forces one to ask the question first, and then move on to supply the right answer.

The process is not easy. There are no shortcuts to that process. The task cannot be passed off to others within the organisation or left entirely to a consultant. However, the development of a sound comprehensive contextual definition is vital to the development of a risk management program which not only meets the needs of the organisation at every level, it is critical to the development of a risk management program that is cognizant of and reacts to the internal risk management needs of the organisation and at the same time is cognizant of and reacts to the risk management needs external to the organisation from non-financial stakeholders.