



# Pegasus Global Holdings, Inc.

## Corporate Risk Management in Context

By Jack L. Dignum, MA, CFCC<sup>1</sup>

### Introduction

According to the recently released Blue Ribbon Report “Risk Governance: Balancing Risk and Reward” published by the National Association of Corporate Directors (NACD):<sup>2</sup>

*“There is clearly an intense focus on risk today. While risk management has been on the radar – if not a priority – for most companies and boards over the past several years, many are asking whether our current system of corporate governance and strategic decision making ensures adequate risk assessment and management.”*

Government regulatory agency focus on risk has intensified significantly over the past year as a direct result of the current global financial crisis as NACD noted regarding the government’s “after-the-fact” response to the financial crisis:<sup>3</sup>

*“...highlight the need for engaged and informed directors who foster a value-building strategy while appropriately responding to the attendant risks.”*

The Blue Ribbon Committee identified ten principles to guide directors in their efforts to provide effective risk oversight. All of those principles provide sound advice for a board of directors and the corporation at large; however, even if every one of those principles and every element of a modern, comprehensive risk management system are in place within an organization, the board or senior management of a corporation may find that it is still unable to maintain the balance between risk and reward which is now the focus of such close scrutiny by investors, governments and the public at large. This is particularly true of corporations which have multiple business streams or units, or one which works on a “program” or “project” basis (i.e. such as a pharmaceutical company or an international engineering, procurement and construction company).

### Corporate Risk and the Board’s Role

Profits live on the edge of risk. As noted by the London Stock Exchange:<sup>4</sup>

---

<sup>1</sup> Jack L. Dignum holds a Certificate in Director Education from the NACD and is the Chief Operations Officer for Pegasus Global Holdings, Inc. an international management consulting firm which performs corporate and project risk management services, capital program and project performance reviews and audits, and advises senior management and board risk and audit committees. Mr. Dignum has over 30 years experience as an international management consultant.

<sup>2</sup> Risk Governance: Balancing Risk and Reward, Report of the NACD Blue Ribbon Commission, National Association of Corporate Directors, October 2009, Letter from the Co-Chairs, page 1

<sup>3</sup> Risk Governance: Balancing Risk and Reward, Report of the NACD Blue Ribbon Commission, National Association of Corporate Directors, October 2009, Letter from the Co-Chairs, page 1



## Pegasus Global Holdings, Inc.

*“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 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.**”*

In short, a corporation must dance *on the edge* of risking more than the corporation can afford to lose if it is to realize a margin higher than the corporation needs simply to survive. At a fundamental level organizations exist to take risks and turn them into rewards. Thus, the dilemma faced by corporations is that to meet or exceed corporate goals means having the willingness to take risks knowing that every risk carries with it a potential for reward and a concomitant potential for loss. Thus, the target of every organization is to achieve a proper balance between the risks, the potential rewards and the potential losses.

Having agreed that risk is a fact of corporate life, the next logical question is who within the corporation is responsible for ensuring that the corporation’s total risk profile represents an acceptable balance between risk and reward? The answer is predictable:

*“Risk is a Board matter: the Board (or equivalent) view themselves as ultimately accountable for risk management ...”<sup>5</sup>*

And

*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>6</sup>*

The past 10 years have seen corporations investing significant sums in developing or obtaining risk management programs which were intended to be responsive to the demand for better governance of corporate risk. Recently a growing number of regulatory agencies, public stakeholders, corporate 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 corporation have failed to meet the stakeholder, board or the corporation’s objectives relative to managing risk.

---

<sup>4</sup> Corporate Governance, A Practical Guide, London Stock Exchange and RSM Robson Rhodes, LLP, July 2004, page 40

<sup>5</sup> Draft BS 31100 Code of Practice for Risk Management, British Standards, Section 4.3, page 15, line 382 - 383

<sup>6</sup> Review of the Principles of Good Corporate Governance and Best Practice Recommendations, Australian Stock Exchange, 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



## Pegasus Global Holdings, Inc.

The question often heard is, “*why isn’t our risk management program working?*” One of the most common barriers to the development and implementation of an effective and efficient corporate wide risk management program is the fact 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 and units of the corporation.<sup>7</sup>

By necessity, risk is actually managed following a bottom-up process; that is management of actual risk takes place at the operations level of the corporation. As a result, risk management programs and systems are often developed strictly based on the risk management needs of that operations group, and while the program developed may be sufficient to meet the operational needs of the corporation, the program may not be meeting the needs of senior management or the board insofar as the governance needs of the corporation.

The development and installation of an effective and efficient risk management program which meets the needs of all levels within and across a corporation 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 contextual definition within which that risk management program is to operate that has led to the situation faced by organizations today: which is simply that the risk management programs and systems in place do not meet the needs and expectations of the corporations which have invested so heavily in those systems.

### **Risk Management Program Context**

According to the Organisation for Economic Co-Operation and Development’s (OECD) 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>8</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.*

---

<sup>7</sup> This is based on international consulting work with corporations on both corporate and program specific risk management programs by Pegasus Global Holdings, Inc. over the past ten years.

<sup>8</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



## Pegasus Global Holdings, Inc.

*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 description. It supports accountability, performance measurement and reward, thus promoting operational efficiency at all levels.”<sup>9</sup>*

It has become a truism globally that managing risk is good for a corporation and its stakeholders, and ignoring risk is bad. Likewise, there is global acceptance that 1) risk management is a systematic method by which an organization identifies, quantifies, treats and reports risk, and 2) the definition of what constitutes an element of risk has grown significantly beyond simple financial risk. However, even with that almost global acceptance and unanimity concerning risk management definitions and methodology, according to the British Standards:<sup>10</sup>

*“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.”*

The first dynamic which prevents the concept of there ever being a uniform or standard risk management program is ***every corporation is to some extent unique***. Corporations, even if they compete in the same industries, do not have identical goals, objectives, standards, organizational structures, operating systems, staffing profiles, execution and operating locations, etc.

The process of managing risk on a discrete corporate basis depends on the development of a “*risk profile*” unique to the conditions within which that corporation will execute its strategic plans.<sup>11</sup> That risk profile identifies each risk to the achievement of the corporate goals and objectives, delineates the probability of the risk manifesting during the execution of the corporation’s plans and the impact to the corporation should the risk manifest, establishes proactive management response plans for avoidance and mitigation of the risk element and, finally, creates the corporate structure by which the risks will be monitored and managed during the execution of the corporate strategy. This is more difficult for a corporation which works in multiple, independent product lines or on a project basis.

It is the *uniqueness* of each project which the corporation executes its scope of work that prevents the organization from adopting a uniform risk profile which could be applied across every project it executes. Attempting to develop and manage risk using a standardized risk

---

<sup>9</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

<sup>10</sup> Draft BS 31100 Code of Practice for Risk Management, British Standards, Section 4.3, page 15, line 382 - 383

<sup>11</sup> Dr. Kris R. Nielsen, “Some Practical Thoughts – Risk Allocation Regarding Airport Projects in China”, Inter Pacific Bar Association Conference Paper and Presentation, 2007



## Pegasus Global Holdings, Inc.

checklist (*one size fits all*) to guide and govern its management of risk during execution of all of its projects invariably results in failure, primarily because any relevant contextual project uniqueness is lost, meaning that risk elements are not properly identified, impacts are unknown, and proactive risk treatment is impossible.

It is not just what is common within a corporation (or among corporations) which defines **context**; but what is unique. The more unique elements which exist within a corporation the more important it is to establish a contextual definition within which a risk management program can fulfill its intended purpose.

Where does a corporation begin the process of preparing a contextual definition?

As an efficient risk management program within and across a corporation must be a top-down process, it must begin with the development of 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 organization and travels successively through the organization to the level at which risk must actually be managed. There are two categories of risk which must be addressed during the development of a full contextual definition for a corporation:

- Internal Risk Elements – questions which go to the internal operations of the organization
- External Risk Elements – questions which go to the external demands on the organization

**Internal risk elements** are usually those risks about which most corporations are most knowledgeable as they involve those elements which are critical to the management of the corporation. Internal risk element questions involve such issues as:

- What core values must be reflected?
- What is the organization’s “appetite for risk”?
- What is the organization’s management?
- What is the organization’s market?
- Where will the organization operate?
- What data and information must flow from the risk management program to meet each organizational level’s need for data and information?

The responses to the internal element questions assist in establishing the corporate level contextual definition which ultimately establishes the parameters within which the risk management program must perform throughout the corporation, including the operational levels. Often it is this corporate contextual definition which is absent from risk management programs as the tendency is to think of risk management as a purely operational issue.



## Pegasus Global Holdings, Inc.

*External risk elements* however, involve impacts to multiple stakeholders and are growing with each law passed or regulation released. The latest growth in external risk elements is due in part to the global recognition that a corporation can no longer limit its definition of a “stakeholder” to just those with a vested financial interest in the organization, but to those that may have a vested interest in where and how that corporation operates. Part of that recognition has arisen due to the fact that those non-financial stakeholders can have a significant impact on a corporation’s ability to meet its goals and objectives while at the same time having no direct financial stake in the corporation’s success or failure whatsoever.

Given the evolution of both the definition of who constitutes a stakeholder and the increasing breadth of external risks that a risk management program should unfold, a corporation must expand its contextual definition to include external risk elements. As with the internal risk elements, external risk elements which go into a full corporate contextual definition of risk are developed by asking questions, such as how will the organization respond to:

- Environmental impacts?
- Macro-economic impacts?
- Social impacts?
- Political impacts?

The creation of the external risk elements of the corporation’s contextual definition is considerably more difficult and complex than the creation of the internal risk elements; nevertheless, the current trend globally is to include the management of external risk elements as critical to a definition of “good governance” and thus a measure of how well a corporation manages and controls risk.

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

It is important that during the development of the board and senior corporate level management contextual definition that the focus is 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 organization or when the program will be used. “**Why**” is the contextual question; *who*, *what*, *where*, and *when* are the operational questions which define the components of the risk management program or system which will be developed in response to “**why**”.

### Summary



## **Pegasus Global Holdings, Inc.**

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

The process is not easy and there are no shortcuts to that process. The task cannot be passed off to others within the corporation 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 corporation 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 corporation and at the same time is cognizant of and reacts to the external risks faced by the corporation.