

AN EXECUTIVE WHITE PAPER

ADDRESSING ENTERPRISE RISK IN A GLOBAL ECONOMY



BY

JILL BARSON GILBERT, QEP
PRESIDENT & CEO
LEXICON SYSTEMS, LLC

REVISED SEPTEMBER 2012

ADDRESSING ENTERPRISE RISK IN A GLOBAL ECONOMY

AN EXECUTIVE WHITE PAPER

EXECUTIVE SUMMARY

Business today is global, on-demand, 24/7. Companies must be agile and quick to respond to changing markets and opportunities. They must be able to identify, assess and prioritize risks across the business enterprise. Enterprise Risk Management must be strategic and holistic to add value. It must incorporate environment, health & safety (EHS) and sustainability, as these business functions can present considerable risks. Companies must mature to a point where they understand and manage risks.

Governance, risk management and compliance (GRC) is a top corporate priority. GRC forms a system of checks and balance where risk management is a separate function from compliance management. In the EHS arena, companies must manage operational risks related to compliance, corporate sustainability and stakeholder pressures. They must plan for and respond effectively to risks posed by incidents and events.

Companies recognize that they can no longer manage risk by using a glut of spreadsheets, small databases and custom-built applications. This hinders data sharing and decision making. Many information technology (IT) organizations are lean and outsource some or all of their functions. These factors can lead them to seek commercial, rather than internally developed, software solutions.

Integrated enterprise risk management software can enhance the ability for organizations to meet the above needs, and more. Such software can aggregate, process and report the right information to the right people, at the right level of detail, at the right time. It can increase agility and support better decision making.

CONTENTS

RISKY BUSINESS.....	3
MARKET TRENDS.....	4
RISK MANAGEMENT SOFTWARE	6
SUMMARY AND CONCLUSIONS	10
LIMITATIONS AND COPYRIGHT NOTICE	10
ABOUT THE AUTHOR	11
ABOUT LEXICON SYSTEMS, LLC.....	11
REFERENCES.....	12

RISKY BUSINESS

Enterprise and Operational Risk

We face risks every day. We choose the foods we eat, how we drive to work and whether or not we exercise. At work, we make decisions based on the information at hand. Each decision has different risks; some have a higher likelihood of positive outcomes and others have a higher likelihood of negative outcomes. Simply defined, *risk* is the probability of a positive or negative outcome related to a business decision or activity. It is a measure of the probability of an event occurring multiplied by the severity of its impacts.

$$\text{Risk} = \text{Probability} \times \text{Impact}$$

Enterprise Risk Management considers the risk portfolio for the entire business. It is a top-down, strategic initiative that requires alignment of the company’s various functions and operations. Like other business functions, EHS must fit with the company strategy since EHS touches just about every department or function across the enterprise.

Enterprise Risk includes Credit Risk, Operational Risk and Market Risk (Figure 1). This White Paper addresses software to manage *operational risk*, “the risk of loss resulting from failed internal processes, systems and people, and external events.”¹



Operational Risk is further divided into Business Risk—internal and external risks in the business environment—and Event Risk—from non-economic events. In the EHS field, examples of Operational Risk are regulatory changes (Business Risk) and upsets, system failures, legal actions and natural disasters (Event Risk).

Figure . Enterprise Risk

The business must prioritize how and when to address enterprise risks after identifying and evaluating the risks in their portfolio. Depending upon its probability and severity of impact, the business has several options for managing risk. The business can accept, mitigate, share or transfer, or avoid each risk (Figure 2).²



Figure . Risk Management Options

Risk Management Maturity Level

While companies agree on the need to link and integrate business processes and information in a more structured manner, many have made little progress. Often, this relates to where the company lies along a risk management maturity continuum. The Risk Management Maturity Model³ illustrates such a continuum (Figure 3). As organizations mature, they transform from an initial, chaotic state to an optimized state where risk management is a source of competitive advantage.

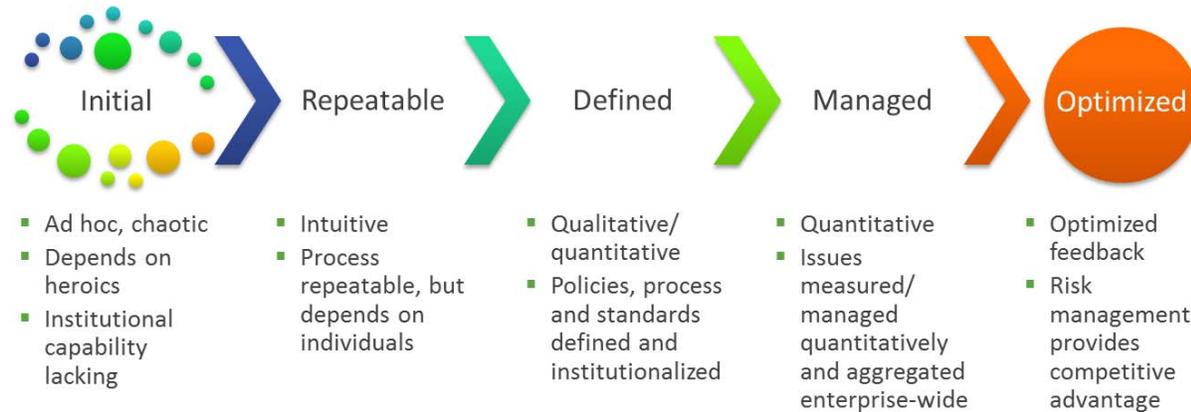


Figure . Risk Management Maturity Model (Adapted from Carnegie Mellon)

MARKET TRENDS

In recent years, companies have implemented software to manage and reduce risk across the business enterprise. In 2006, 46% of companies surveyed planned to implement or evaluate technologies for risk management in the next two years.⁴ This percentage is higher today. Some of the reasons that organizations seek risk management software solutions include

- Regulatory compliance,
- Globalization, corporate social responsibility (CSR) and sustainability
- Stakeholder pressure, and
- Extreme events.

Compliance

The “compliance” component of GRC is a top corporate priority. EHS is one of the most highly regulated business functions, and day-to-day compliance activities have potential risks to health and the environment. As a result, EHS attracts the attention of internal and external stakeholders. Thus, the business community is concerned about risk, as well as compliance. A 2007 AMR Research survey found that 58% of organizations surveyed were concerned about “operational and general risk management” and 35% cited “green compliance” as their primary concern.⁵



European Union (EU) chemical management regulations have a potentially large impact on global commerce. According to the U.K.’s Department for Environment, Food and Rural Affairs (DEFRA), “Around 100,000

different substances are registered in the EU, of which around 30,000 are manufactured or imported in quantities above 1 tonne. Adequate data on the environmental and health effects is available for only a small proportion of these chemicals.” The EU’s REACH program is an initiative to **Register, Evaluate, and Authorize Chemicals**. REACH applies to existing and new chemicals and requires that all chemicals imported into or produced in the EU in quantities above 1 tonne/year be registered. Those chemicals with the greatest potential risks require authorization.⁶ The REACH program has many similarities to the U.S. Toxic Substances Control Act (TSCA).



Globalization, CSR and Sustainability

Globalization—new markets and the blurring of former business and geographic lines and best practices—calls for renewed emphasis on risk management.

Corporate Social Responsibility (CSR) is something that Internal and external stakeholders expect companies to practice routinely. Sustainability initiatives create long-term shareholder value by taking advantage of opportunities and managing risks resulting from economic, environmental and social factors.

Sustainability reporting allows companies to publicly communicate their performance in these areas.

Developed in 1997, the Global Reporting Initiative (GRI) is the *de facto* standard to establish and report on environmental Key Performance Indicators (KPIs).⁷ More recently, the International Organization for Standardization developed ISO 26000:2010, Social Responsibility guidance.⁸

The EU Accounts Modernisation Directive (AMD) and the Companies Act, 2006 require companies to be accountable for environmental impacts material to their business performance, and to disclose these “to the extent necessary” in the annual report.⁹ The U.K. also provides environmental KPI guidelines.¹⁰ The American Chemistry Council’s Responsible Care® KPI task force allows member companies to benchmark against each other, against companies outside of the program, and against global standards.¹¹

Greenhouse gas emissions and their impact on global climate change are also top priorities on corporate agendas. The European Environment Agency (EEA) Executive Director stated, “While the worst effects of climate change may not hit Europe for many years we must prepare now. Climate change will have profound effects on our natural resources and will also change the way we go about our daily lives. We will not only lose biodiversity but also large parts of our territory, for example low-lying coastal areas and river basins as sea levels rise.”¹²

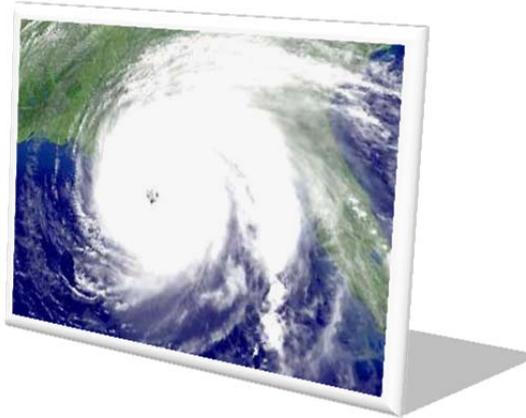
Stakeholder Pressure

Business stakeholders include many parties that demand a certain level of performance. Corporate excesses of the late 1990s led to Sarbanes-Oxley, which requires accountability and transparency in reporting by U.S. businesses—for the first time, many companies were required to account for their actions. Companies must demonstrate transparency, or the ability to report information, as well as report on the methods used to gather that information, often including a chain of custody.



“Corporate Sustainability is a business approach that creates long-term shareholder value by embracing opportunities and managing risks deriving from economic, environmental and social developments.”¹³

Companies that invest in corporate sustainability initiatives and manage the “triple bottom line” of economic, environmental and social risks get positive returns. The Dow Jones Sustainability Indexes, launched in 1999, provide solid evidence that sustainability-driven companies deliver more value than similar, non-sustainability-driven companies.¹⁴



Extreme Events

Extreme Events can range from process breakdowns and systems failures to legal actions, natural disasters, terrorism and pandemics. A single major event can produce many EHS, economic and social impacts—with a range of risks.

Hundreds of U.S. agencies regulate extreme events. The U.S. Environmental Protection Agency and Occupational Safety and Health Administration prescribe measures to mitigate environmental and health & safety events, respectively. The Department of Homeland Security requires companies to implement minimum measures to

prevent site and equipment security breaches. The Responsible Care® program requires chemical companies to ensure physical security and data systems or “cyber” security.

All of these factors, individually or collectively, make a compelling case for implementing a risk management platform. The ability to identify, assess, manage and track risks can yield productivity gains and cost savings while protecting human health and the environment.

RISK MANAGEMENT SOFTWARE

The GRC Umbrella

Enterprise risk management software falls under the umbrella of the GRC platform market. With Sarbanes-Oxley and other financial requirements, the market has expanded from a tactical focus on regulatory compliance to a strategic focus on enterprise risk management. Many vendors plan to add integration with business analytics and scorecard capabilities in future software versions.¹⁵

It is not surprising that some “niche” enterprise EHS software platforms now address enterprise risk management. This is because business processes, not regulatory subject matter, drive enterprise risk management. These solutions impose common risk identification, assessment, analysis and management methods; consistent information-gathering; and integration with core data.

Companies can—and do—apply enterprise EHS software to other business functions. This may be due to a lack of funding or internal resources to implement a full-blown Enterprise Risk Management software

solution. EHS may be the first function to implement a risk management solution; once the software is implemented for EHS and demonstrates early wins, other departments want to use it.

Disruptive Technology

Disruptive technology such as enterprise risk management software changes how stakeholders view the business and how they perform work. The software allows companies to conduct day-to-day activities and make decisions in view of an enterprise risk portfolio that aligns with strategic goals.

Enterprise Risk Management Software is disruptive technology that causes a paradigm shift, changing how people view the business and work day-to-day.

Organizations react differently to new technology. Geoffrey Moore's Technology Adoption Life Cycle¹⁶ uses a normal bell curve to predict the percentage of people who will adopt one of five different strategies for switching from old to new technology products over time (Figure 4).^{17, 18, 19}

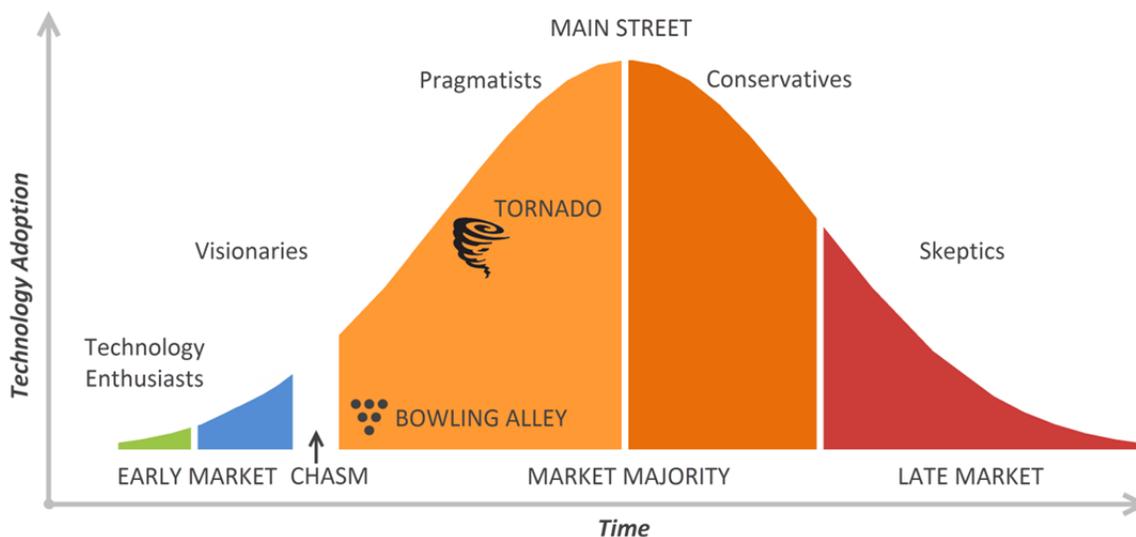


Figure . Technology Adoption Life Cycle (Adapted from Geoffrey Moore)

With any disruptive technology, the Early Market includes Technology Enthusiasts and Innovators. Techies buy the product because it is cool. Visionaries (Innovators) buy the product for competitive advantage.

The Chasm between the Early Market and the Market Majority exists because Visionaries and Pragmatists are polar opposites. Visionaries are intuitive risk-takers who break away from the pack, while Pragmatists are analytical risk managers who stay with the pack. Thus, Visionaries make poor references for Pragmatists.

The Market Majority (Main Street) includes the Early Majority (Pragmatists) and the Late Majority (Conservatives). Pragmatists have neutral attitudes towards technology but make the bulk of technology purchases. They prefer to buy from the market leader. Conservatives switch technology only under pressure. They prefer a proven commodity product.

The Bowling Alley is an Early Market Majority phenomenon. The technology vendor creates a “whole product” in one niche, replicates success in other niches and then expands the product offering, and so on—hence the bowling alley analogy.

The EHS Risk Management software market has crossed the chasm into the Bowling Alley. There is no “killer app” that has spawned a Tornado.

In the Tornado, the technology is a “must have” item. The market explodes, and demand outstrips supply. The latest Apple iPhone is an example of a tech product in the Tornado phase.

In the Late Market, the technology is a commodity. Skeptics are critical of technology and challenge high-tech market hype. Often, by the time they adopt the technology, they fail to reap the greatest benefits, as a new disruptive technology soon will replace it. At the market’s End of Life, vendors must differentiate their offerings through price or by service to retain market share.

Common Characteristics

While the enterprise risk management platform market lacks a “killer app” and lacks a “one size fits all” solution, commercial software solutions share a number of common characteristics (Table 1).

Table . Enterprise Risk Management Software Characteristics

Functional Areas	Technical Framework	Globalization Issues
<ul style="list-style-type: none"> ▪ Incident management ▪ Risk management ▪ Audit & compliance management ▪ Knowledge management ▪ Task management/action item tracking ▪ CSR and sustainability 	<ul style="list-style-type: none"> ▪ Flexible architecture ▪ Modular ▪ Configurable ▪ Graphical user interface/dashboard ▪ Standard and ad hoc reports ▪ Security 	<ul style="list-style-type: none"> ▪ Operate in different languages ▪ Manage local requirements ▪ Support local units of measure ▪ Operate anytime, anywhere ▪ Reflect global best practices

Key Features

Strategic market trends cause vendors to develop software initially. Tactical business needs push vendors to develop certain software features and functions that address a range of people, process and technology issues (Table 2).

Table . Business Needs and Specific Software Features

Business Need	Resulting Software Features/Functions
People Business with multiple locations, languages and time zones	<ul style="list-style-type: none"> ▪ Sharing of structured and unstructured data ▪ Anytime, anywhere access, collaboration tools ▪ On-the-fly language translation ▪ Handles multi-bit and right-to-left alphabets ▪ Considers local regulations and customs
Software ease of use and adoptability	<ul style="list-style-type: none"> ▪ User-friendly interface ▪ Dashboards, scorecards ▪ Ad hoc reporting tools ▪ User-friendly administrative tools

Business Need	Resulting Software Features/Functions
Learning curve	<ul style="list-style-type: none"> ▪ Training tailored to different user types ▪ Online help
Process	
Performance management, KPIs	<ul style="list-style-type: none"> ▪ Business analytics ▪ Performance management
GRI, ISO 14000, ISO 26000	<ul style="list-style-type: none"> ▪ Scorecards, KPI reporting ▪ Greenhouse gas emissions management, emissions trading
Internal and external obligation management	<ul style="list-style-type: none"> ▪ Automated workflows ▪ Integration/links to regulations, policies, permits ▪ Asset (equipment) management
ISO 9001, ISO 14001	<ul style="list-style-type: none"> ▪ Obligations management ▪ Task management, action item tracking ▪ Audit management
Sarbanes-Oxley	<ul style="list-style-type: none"> ▪ Risk, performance, and EHS-specific workflows ▪ Decision and reporting tools
UK, other regulatory initiatives	<ul style="list-style-type: none"> ▪ Business process-based systems
Electronic content management	<ul style="list-style-type: none"> ▪ Electronic document management workflows ▪ Attachment capabilities with audit trail ▪ Limited version control ▪ Links to full-fledged content management systems
Technology	
User access and data security	<ul style="list-style-type: none"> ▪ Multiple layers of physical security ▪ Role- and site-based user security ▪ Data transaction audit trail
Ease of configuration and reporting	<ul style="list-style-type: none"> ▪ User-friendly configuration tools ▪ Standard reports ▪ Reporting engine
Data integration	<ul style="list-style-type: none"> ▪ User-friendly data import, validation, export tools ▪ Standard connectors to common systems ▪ Prepopulated content
Scalability and flexibility	<ul style="list-style-type: none"> ▪ N-tiered architecture: database, business rules, user layers ▪ Multi-level business hierarchy, multiple hierarchies ▪ Modules allow phased deployment

Key Benefits

Enterprise risk management software covers risks across the business, in contrast to “point” solutions that address a single risk category. This software provides a number of benefits, as it

- helps companies to anticipate potential risks and take proactive actions to manage them;
- standardizes risk management methods across business functions, business lines and geographies;
- automates risk management processes;
- provides consistent data gathering, sharing and reporting;
- allows subject matter experts to focus on data analysis vs. data collection;
- aggregates information for better decision-making; and
- helps companies to see the “whole” risk profile.

SUMMARY AND CONCLUSIONS

Global businesses have a greater awareness of risk than ever before, yet most companies lack a complete picture of their enterprise risk portfolio. A host of stakeholders place a surplus of obligations on businesses, and these obligations carry risks. Market drivers for enterprise risk management include regulatory compliance, globalization, stakeholder pressures and extreme events. EHS is an important component of enterprise risk, as it cuts across the entire business.

Risk and compliance are two elements of a governance, risk management and compliance framework. Stakeholders demand corporate accountability and transparency, and globalization calls for businesses to be agile and respond to risks quickly.

Financial enterprise risk models easily extend to EHS. Whatever risk model is used, businesses need to consider upside risks (opportunities) and downside risks.

While organizations lie along a risk management maturity continuum, the trend is towards greater adoption of enterprise risk management platforms. Spreadsheets, small databases and internally-developed software commonly fail to address enterprise risk. Commercial software allows companies to address enterprise risk, and offers many advantages.

Enterprise risk management platforms share common functionality and technical frameworks. The most flexible software is business process-driven, allowing various business functions to use it. Enterprise risk management software is a disruptive technology that changes how people accomplish work. Companies must understand where they fit within the Technology Adoption Life Cycle, as well as the market stage of the software under consideration.

Software today is advanced and much more capable, yet easier to use than its predecessors. As the enterprise risk management market lacks a “killer app” or a “one size fits all” solution, companies must identify a configurable, flexible solution that can leverage data from other systems as needed.

LIMITATIONS AND COPYRIGHT NOTICE

This White Paper is for INFORMATIONAL PURPOSES ONLY. No implied warranty of merchantability or fitness for a particular purpose shall apply. Lexicon Systems, LLC makes no representation or warranty that the implementation or use of information or the recommendations, findings, or conclusions in this document will result in compliance with applicable law.

Copyright © 2002-2012 Lexicon Systems, LLC. All Rights Reserved. No person may reproduce this work, prepare any derivative works, distribute copies, sell or display this document publicly without the explicit written permission of Lexicon Systems, LLC.

ABOUT THE AUTHOR

Jill Barson Gilbert is President, CEO and Founder of Lexicon Systems, LLC. Gilbert is a thought leader on environment, health & safety (EHS) management information systems and has authored over 115 publications. Leadership positions include past Vice President and Director of the Air & Waste Management Association. She is listed in Marquis Who's Who in America; Marquis Who's Who in the World and Marquis Who's Who of American Women.

Over twenty-five years of EHS, information management and business experience shape Gilbert's perspective. She keeps current on strategic, management and IT issues through regular dialogs with business executives and industry analysts and writes the "IT Insight" column for EM magazine.

For over fifteen years, Gilbert has focused on management information systems and information technology. Before founding Lexicon Systems, she was a Director at T3. Earlier, she was Director of Product Management for Oracle Corporation. Gilbert started her career in the chemical and refining industry and later spent many years as EHS management consultant to diverse industries. She earned an M.S. in Environmental Management from the University of San Francisco, an A.B. from Miami University and completed the Rice Program for Managers at Rice University. Gilbert is a Qualified Environmental Professional (QEP).

ABOUT LEXICON SYSTEMS, LLC

Lexicon Systems, LLC is an independent, objective management consulting firm that puts client interests first. Our primary focus is the EHS management information systems market. We are a preferred provider to EHS and IT senior management in industry, as well as C-level executives in software and investment firms.

Lexicon helps companies to assess their needs and identify solutions to meet them. Our senior staff understands industry and its issues, and arrives at solutions thoughtfully and quickly. We offer the breadth and depth of experience of a large firm with the responsiveness of a small firm.

For further information, call +1 281.280.8106, send an e-mail to info@lexicon-systems.com or visit lexicon-systems.com.

REFERENCES

- ¹ Celent, *Operational Risk Management: Three, Two, One, Liftoff?* June 2006 (www.celent.com).
- ² Bearing Point, *The Basel New Capital Accord and the Challenge of Operational Risk Management*, 2004.
- ³ Carnegie Mellon Software Engineering Institute, *Capability Management Maturity Model Integration*, <http://www.sei.cmu.edu/cmmi/>.
- ⁴ Fitzgerald, Brenna, AMR Research Press Release, January 03, 2007.
- ⁵ Haggerty, John, *Market Demand for Governance, Risk Management, and Compliance, 2007-2008*, AMR Research, February 2007.
- ⁶ Department for Environment, Food and Rural Affairs. See: <http://www.defra.gov.uk/environment/chemicals/reach/>.
- ⁷ Global Reporting Initiative™, <http://www.globalreporting.org/home>.
- ⁸ ISO 26000:2010, <http://www.iso.org/iso/home/standards/iso26000.htm>.
- ⁹ Materiality, Accountability and Sustainability, FSN, 23 April 2007. See http://www.fsn.co.uk/channel_kpi_environment/materiality_accountability_and_sustainability.htm.
- ¹⁰ Department for Environment, Food and Rural Affairs, *Environmental Key Performance Indicators: Guidelines for UK Businesses*, 2006. See: <http://www.defra.gov.uk/environment/business/envrp/envkpi-guidelines.pdf>.
- ¹¹ See: http://www.americanchemistry.com/s_responsiblecare/sec.asp?CID=1298&DID=4841.
- ¹² European Environmental Agency, 02 July 2007. See: <http://www.eea.europa.eu/highlights/planning-to-tackle-climate-change>.
- ¹³ Dow Jones Sustainability Indexes, <http://www.sustainability-indexes.com/sustainability-assessment/corporate-sustainability.jsp>.
- ¹⁴ Dow Jones Sustainability Indexes, <http://www.sustainability-index.com>.
- ¹⁵ *Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms*, Garter, 2011.
- ¹⁶ Developed in the late 1950s by Everett Rogers et al.
- ¹⁷ Moore, Geoffrey A. and R. McKenna, *Crossing the Chasm*, New York: HarperBusiness, 1995.
- ¹⁸ Moore, Geoffrey A., *Inside the Tornado*, New York: HarperBusiness, 2000.
- ¹⁹ Moore, Geoffrey A., *Living on the Fault Line*, New York: HarperBusiness, 1995.