Intelligent Management Trends

Defining an Enterprise Risk Management Vendor

An IMT Perspective

John Farrell
IMT, Principal Advisor

Standards and expectations for enterprise risk management accelerated in the past decade and the number of companies positioning themselves as enterprise risk management vendors expanded erratically in response. A diverse array of companies, including the likes of PwC, Accenture, MetricStream, Kroll, and Moody's Analytics, has used the term "enterprise risk management" to promote unique varieties of risk-related offerings. Corporate executives and risk managers face plenty of challenges trying to implement the value-enhancing potential of risk management within their own companies and can ill afford confusion when they turn to product and service vendors for support. A basic set of descriptive parameters for vendor offerings can add clarity, facilitate communication, and aid the practical value and growth of the *enterprise risk management (ERM) market*.

THE CUSTOMIZABLE ERM STANDARDS PARADOX

Before outlining these vendor parameters, recognize risk management is a company-specific, objective-focused discipline. While risks are not always addressed explicitly or successfully, every business has managed risks its own way. When businesses fail, particularly those during the 2007-2009 financial crisis, the rippling market-wide effects amplify shareholder and public calls for better-managed enterprises across our economy with rising risk management expectations. The current advancement and adoption of risk management as a more structured enterprise discipline is lifting the standards for companies that not only endure, but also maximize opportunities as disruptive events occur.

Although risk management pioneers have been blazing trails in some industries for decades, the formalized risk management practices applied within financial services firms have only more recently gained traction across industry sectors and are now extending across enterprises. As this broader ERM adoption holds great promise, it also invites complexity and confusion. Each risk manager and corporate board member may promote his or her own perception of risk management. This fog grows exponentially with additional perspectives offered by business line managers, associations, investors, regulators, industry pundits, academia, insurers, auditors, actuaries, and consultants. Healthy debates over the details of risk management are likely to rage on for years.

Standards organizations and business associations, including ISO, COSO, OCEG, FERMA, and others, have taken tremendous strides to cut through this fog of risk management while coalescing toward similar basic definitions, enterprise roles, and processes. Recognition by auditors, regulators, and ratings agencies give these standards added credence and weight to spur broader adoption.

Over time, educational institutions should help spread these common principles to shift risk management from a specialization to a core business discipline for every business manager. Some of the more active business school programs and research centers evangelizing enterprise risk management include the following:

- Wharton's Risk Management and Decision Processes Center
- Stanford's Strategic Decision and Risk Management Program
- The Enterprise Risk Management Initiative in the Poole College of Management at North Carolina State University
- The Institute for Managing Risk at Manhattanville College
- NYU's Stern School of Business
- The Risk Institute of Fisher College of Business at The Ohio State University
- Cambridge University's Centre for Risk Studies

As these standards and educational organizations outline ways to apply risk management principles to strategic, financial, and operational decision-making processes, their paradoxical challenge is to set clear guidelines and frameworks while allowing enough flexibility to adapt to distinct business models, processes, and risks across disparate business practices. For each enterprise, a variety of forces manipulates these flexible risk management standards during the formal implementation of ERM programs. External influence from regulatory agencies, standards organizations, ratings agencies, litigators, shareholders, and business partners collide with the internal realities of employee risk knowledge, time constraints, management expectations, funding, and other limited resources.

BARRIERS TO ERM NIRVANA

In general, glaring regulatory requirements, the consequences of noncompliance, and ready-made vendor solutions centered on regulatory registries and checklists often gain initial enterprise investments. Companies drifting in this direction tend to address governance, risk management, and compliance (GRC) as a consolidated program with regulatory compliance typically the most pressing objective. The potential value of risk management in this scenario can be lost under the GRC umbrella with "chicken-or-the-egg" debates over the lead role of G or R or C. In the cases where companies emphasize enterprise risk management, they tend to whittle down the great expanse of risks to just the most likely and consequential for enterprise-wide concerns.

ERM should certainly integrate compliance requirements and include clear governance guidelines to gain traction as an effective enterprise program. Overcoming initial implementation hurdles may also dictate an annual or

quarterly process of limited scope as a first step. But regardless of its initiation, enterprise risk management goals should aspire to

- broadly employ risk management principles and processes for optimized risk-informed decision making across an enterprise;
- provide an integrated enterprise portfolio of risks to support strategic, financial, operational, and resource decisions;
- enable opportunistic gains from changing business conditions;
- be used on an ongoing, real-time basis; and
- exceed expectations of shareholders, regulators, ratings agencies, and partners.

Emphasizing ERM as a means of improving strategy, financial performance, and the speed and accuracy of business decisions considering specific objectives can enhance organizational value more than a program established as a reactive buffer for certain negative events or one merely designed to assure regulatory compliance.

Labeling these loftier goals as aspirations does not mean they are unattainable, but practical ERM implementation does face significant hurdles. Internal organizational challenges may include the following:

- Limited budget and manpower resources.
- A lack of executive and/or boardroom advocates.
- Cultural resistance to new business frameworks.
- An inconsistent set of risk management concepts and processes already entrenched in functional silos.
- Insufficient expertise to assess the full universe of enterprise risks.
- Limited technical skills to effectively leverage analytics technology.
- Management reluctance to take on risk ownership.
- A lack of information and tools needed to properly assess, monitor, and address risks.
- Inefficient risk communication, education, and reporting.

This list of organizational hurdles, commonly identified in surveys over the past few years, points to challenges risk managers face building the people, processes, technology, and information resources necessary for effective enterprise risk management programs. The fickle nature of these factors helps explain the ebb and flow dynamics of past ERM implementation efforts. However, the very nature of enterprise risks poses more daunting challenges.

Borrowing from, and extending, the list of terms commonly used to depict big data, the *volume, variety, velocity*, *volatility,* and *vitality* of risk events pose

management capacity complexities that have prevented most organizations from declaring significant progress toward enterprise risk management nirvana. *Veracity* can join this alliterative "v" challenges list as it applies to concerns over information sources used to identify, assess, monitor, and act on risk factors. Even when organizations conduct exhaustive efforts to identify and address an extensive set of risks, emerging and unknown risks are always lurking.

ERM programs settling on just a limited number of top known high-frequency and/or high-consequence risk events that may affect objectives will no longer be acceptable. Shareholders, regulators, and lawyers are proving they are ready to pounce on the edges of expanding management expectations. Loosely applying statistical philosopher Nassim Nicholas Taleb's thoughts, ERM is a fool's effort if we declare any comfort while knowingly discounting the randomness of long-tail events.

CALLING IN THE VENDOR CAVALRY

As risk managers and corporate boards progress through their cultural, process, and resource obstacles, organizations are beginning to evolve on the second challenges front to formalize ERM coverage of the full range of risks they face on an ongoing basis (while addressing each "v" risk attribute). This includes maximizing explicit risk awareness while whittling *unknown* risks down to only the *unknowable*. These enterprise risk management practice expectations are far too daunting for any individual risk manager to coordinate, even with the support of a broader team and role players across an entire enterprise.

Setting lofty ERM program goals can raise skepticism. Limited cultural and resource support have thwarted some of the broader advances among enterprises in past efforts, but challenges and necessity breed inventions and new solutions. A wide range of vendors, including risk advisors and consultants, software vendors, and risk information providers, are quickly advancing their offerings to help raise the value of risk management systems for enterprises.

Until recently, enterprises investing in risk management vendor offerings have focused mostly on overcoming their cultural challenges, establishing risk management processes, enabling assessments, setting governance rules, and determining and tracking treatment actions. Each enterprise set the scope of their ERM program based on available resources usually to the point of meeting regulatory requirements. Most still fall short of the potential of ERM to not only enhance enterprise value by protecting the organization from downside risks, but also by uncovering opportunities for market and financial gains.

As they advance toward this greater value, most risk managers prefer to define their role as establishing and guiding risk management programs and communication while boards, executives, and line managers take on crucial roles such as setting risk appetite, supporting assessments, and owning risks in relation to business objectives. Their path toward higher-valued ERM programs is twofold. On the one hand, there is a drive to standardize, centralize, integrate, and coordinate the structure and information flow of risk management programs. On the other hand, ERM success is highly dependent on decentralizing risk management principles and core process responsibilities.

Just as the standards organizations set clear but flexible ERM guidelines, so too must enterprise risk managers establish corporate risk management frameworks which allow individuals to tweak their risk management processes and resources to fit their own functional role. Given limited central management capacity, reliance on risk management consultants, software, and information vendors is increasingly necessary to successfully implement the standards, analytics, data workflow, and communication channels required under the pressures of high velocity and volume risks.

While past risk management vendor offerings focused on initiating the basic elements of ERM programs, the current wave of offerings heightens support for integrating, communicating, reporting, and managing a higher volume and variety of risk information at a faster speed. This current trend can accelerate the transition of ERM from theory and frameworks to practical implementation with a stronger value return for enterprise success.

Some of the broader positive developments supporting this transformational optimism include the following:

- Board-level interest in leveraging ERM for strategic and financial gains.
- Standards organizations shifting focus from concepts and definitions to practical implementation guidelines for better decision making.
- An expanding base of empirical evidence sharpening successful risk management program blueprints.
- More robust information repositories supplementing traditional spreadsheets and relational databases.
- Advances in big data management and analytics.
- The ability to utilize both structured and unstructured data.
- The broadening appeal and use of predictive analytics.
- The expansion of machine learning (particularly neural network approaches) that can support risk pattern and interrelation analysis.
- The progress of integrated reporting and visualization tools for clear and concise communication.

Risk management vendors are often driving these trends, but, unfortunately, they have not made this transition easy. While their capabilities and specialties vary tremendously, their value statements usually lack clarity in the context of enterprise risk management. Vendors have an opportunity to energize the current ERM evolution wave by using simple variations in capability statements to reference specific facets of their customers' risk management requirements.

AN ERM VENDOR TAXONOMY

Top management consulting firms, insurance advisors, and financial management software vendors have explicitly offered risk management practices and products for many years, but the broadening enterprise perspectives of ERM standards opened a wider door to more vendors positioning themselves as enterprise risk management solution providers. Companies specifically addressing, for example, regulatory compliance, insurance claims processing, network security, document management, or disaster response have used the ERM label in their value statements. Some vendors liberally reference an enterprise risk role even if they support only a small portion of the processes or information required for true ERM.

Corporate decision makers have viewed this jumble of vendors the same way they have viewed past risk management efforts within their own companies – as disjointed silos with unique capabilities and perspectives regarding risks. Even vendors falling squarely in ERM definitions vary widely in the capabilities and value they bring to customers. The broad example of companies noted earlier, PwC, Accenture, MetricStream, Kroll, and Moody's Analytics, can defend their claims of enterprise risk management offerings, but they generally have not considered themselves direct competitors.

As the standards used among risk management professionals progressed, vendors seized terms like ERM and GRC as convenient acronyms for broad market appeal which tend to be, at best, unclear and, at worst, terribly misleading. Over one thousand companies now reference ERM (or risk management within GRC) to describe the value of the services and products they offer. This total can reach into thousands using looser standards for identifying "risk management" references. Most fall far short of the holistic concept of enterprise risk management.

In effort to refocus ERM on its value-enhancing potential, some vendors are opting to use terms such as "integrated risk management," "strategic risk management," and "enterprise-wide risk management." The downside of this tactic is it further contributes to the terminology fog when ERM already is definitionally a holistic, integrated, enterprise-wide management approach

that can support enterprise strategic, financial, operational, and resource allocation objectives. The preferred route for market clarity should be an adamant reaffirmation of these ERM attributes in line with existing ERM standards and definitions.

How can enterprises and vendors lift the fog of the term *enterprise risk management* as it applies to vendor capabilities?

First, refocus on the holistic risk concepts and core values of enterprise risk management as outlined in industry standards. Broadening an already broad and complex ERM discipline (to a consolidated GRC view for instance) weakens its potential power. COSO's ERM – Integrated Framework directly states ERM encompasses "identifying and managing multiple and cross-enterprise risks." Vendors should reference existing standards and terms like this as they correlate with their own offerings.

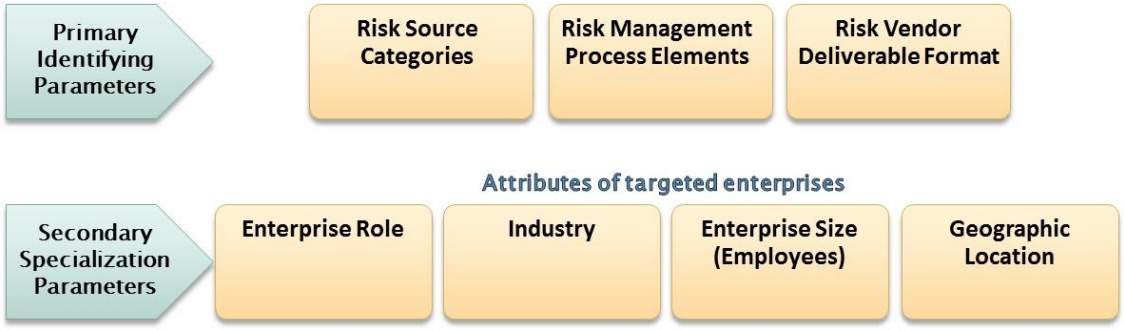
Second, recognize ERM is not just a program or a process, but rather a coordinated system using people, processes, technology, and information to optimize risk-informed decision making. While risk management standards help to structure internal enterprise programs, external vendors should position themselves in alignment with the specific enterprise resources and processes they can support in the context of a holistic ERM system.

Third, use a simple set of defining parameters to clarify a vendor's risk management specialization or the extent to which its offerings may address all enterprise risk management requirements.

As an industry trend and vendor research firm, IMT offers an enterprise risk management market taxonomy with the following objectives:

- Highlight the value of risk management in the context of optimizing enterprise decision making to achieve objectives.
- Maximize compatibility with broadly-accepted risk management standards.
- Keep the taxonomy segmentation as simple as possible.
- Identify vendor value in the context of a holistic view of enterprise risk management.
- Partition categories based on observed clusters of risk management-related spending activity between enterprises and vendors.
- Validate the segmentation with research of 10-K risk factor statements, industry risk management surveys, vendor offerings, and interviews with enterprise executives and risk managers.

Market analysis supporting these objectives points to the following core parameters as a basis for identifying and defining the positioning value of vendor services and product offerings across the risk management market:



IMT defines and details each of these parameters and sub segments in its ***Enterprise Risk Management Market Taxonomy*** report. The following general observations are presented in this IMT Perspective in the context of defining an enterprise risk management vendor.

The first Primary Identifying Parameter, **Risk Source Categories**, is ultimately unique to each company, but the IMT taxonomy outlines thirteen general categories of risk sources across all enterprises as addressed by various risk services, software, and information vendors. This broad segmentation is collectively exhaustive, but not necessarily mutually exclusive since interrelated risk events and consequences can create multiple paths to any generalized risk source category. Nonetheless, it is a critical segmentation for aligning internal enterprise risk management resource needs with external vendor capabilities.

Standards organizations promote distinct but similar risk management processes and definitions. IMT's second taxonomy parameter, **Risk Management Process Elements**, draws from industry standards to identify seven core process elements as they align with risk management vendor offerings.

The third Primary Identifying Parameter, **Risk Vendor Deliverable Format,** categorizes vendor offerings by their form of delivery: a service, software technology, or information product. Pure service or software-centric views of the ERM market fail to address the inseparability of the people, process, technology, and information requirements for ERM systems. Complaints and declarations about vendor failures or value inevitably derive from the lack of investment in one of these important supporting resources. Enterprise customers will never perceive a consulting engagement as truly successful without resource investments in ongoing technology-supported processes. The value of software investments is also limited without cultural acceptance, role clarification, and process optimization. Likewise, investments in risk

management consulting engagements or software will provide little value without the timely availability of pertinent reliable information to support risk identification, assessments, and treatment activities.

While it is possible to differentiate the deliverable format of vendor offerings, it is increasingly difficult to categorize a vendor purely as a service or software or information provider. Many vendors invest in multiple forms of delivery either by expanding their own ERM offering portfolio or by closely partnering with other vendors to provide a complete ERM solution.

Using these basic parameters, risk management vendors should at a minimum clearly identify their offering capabilities in relation to these first three Primary Identifying Parameters (Risk Source, Risk Process Elements, and Deliverable Format) to effectively communicate and promote their value in the risk management market. Further differentiation and unique value can utilize any of the remaining Secondary Specialization Parameters for specific customer targeting: Enterprise Role, Industry, Enterprise Size, and Geographic Location.

QUALIFYING VENDOR LABELS TO IMPROVE ERM MARKET EFFICIENCY

The marketplace includes many risk management vendors with distinct capabilities out of necessity. No one vendor can offer deep expertise across all the risk management process, technology, and information resources necessary for holistic ERM systems. Some risk management consultants and software vendors have an ability to broadly address enterprise-wide processes and technology, but most currently focus their expertise on a specific process element or risk source category.

When can vendors accurately use the ERM label? First, note the negative qualifiers. ***Enterprise risk management*** is not a standalone role, program, function, process, or technology. ERM is a management principle applied to a framework integrating people, processes, technology, and information across an organization to explicitly and holistically address the uncertainties associated with enterprise objectives.

IMT's perspective is the term *enterprise risk management* appropriately applies to a vendor only when their offering can

- address the entire risk management process,
- support the management of risks across all enterprise functional units,
- consider any risk regardless of the risk source category, and

- enable a consolidated portfolio view of risks that can help address the uncertainties associated with enterprise strategic, financial, operational, and resource objectives.

No one vendor can provide all the resources required for a complete ERM solution, but services vendors with offerings that align with the core ERM criteria include the Big Four audit and advisory firms (Deloitte, Ernst & Young, KPMG, and PwC), as well as some of the next tier of global advisory network firms such as Baker Tilly, BDO, Crowe Horwath, Grant Thornton, and RSM. Their consulting offerings include risk management practices that provide guidance and support for implementing and using risk management across an organization. Large management consultants, such as Accenture, McKinsey, and Protiviti, also address ERM with an integrated perspective, as do an abundance of pure-play risk consulting boutiques serving the small to medium-sized enterprise market. Advisory and management consulting firms specializing in a specific portion of the risk management process, or a specific risk source, should avoid the *ERM* label.

In the software sector, many vendors like to broaden their target market by referencing governance, risk management, and compliance (GRC) capabilities when in many cases they primarily focus on compliance. From an ERM perspective, however, compliance is associated with only a portion of the ERM process. Some of the software vendors that can properly claim ERM capabilities for a complete risk management process while addressing risks broadly include BWise, LogicManager, MEGA, MetricStream, and Sword Active Risk.

The market for this breadth of ERM software functionality is still relatively young as software development draws from multiple launching points, including

- pure-play ERM startups,
- independent insurance advisory consultants and brokers adding software products to their offerings,
- risk management software vendors specializing in specific risk sources now broadening their risk source coverage,
- data analytics software experts, and
- broad enterprise resource planning software vendors (e.g. SAP, Oracle).

This diverse background means significant differences in software functionality, strengths, and weaknesses will persist as vendors build or modify their existing products to reposition them as holistic ERM software solutions.

Services and software vendors that do not qualify as ERM vendors can best refer to their capabilities and value by clarifying their deliverable type and the

specific portion of the risk management process and/or risk categories in which they specialize.

As for risk information providers, some may reference the term ERM to help define their value, but none can qualify as an ERM vendor since they do not address risk management processes. These vendors, including risk modelers, regulatory registries, and specialty risk analysts (among many others), provide value by identifying, assessing, and, whenever possible, quantifying specific risks by risk source. They are important to note within an ERM market context given their increasingly critical role not only as direct providers for enterprises, but also as partners and acquisition targets for service and software vendors.

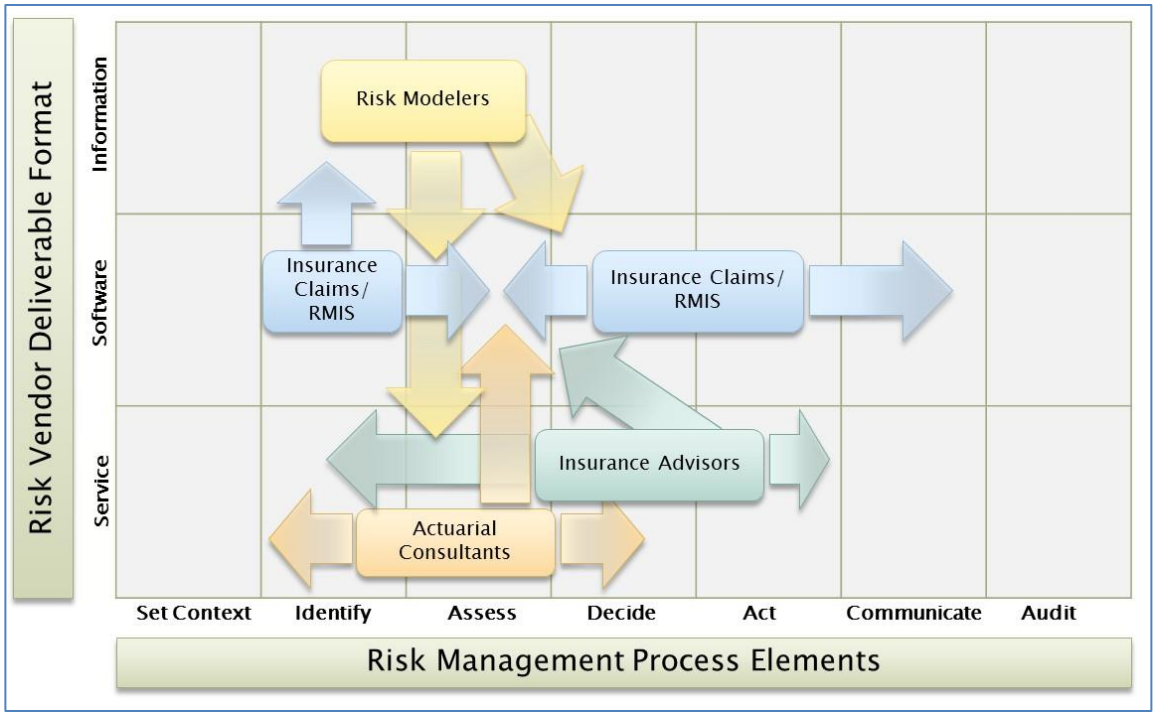
While all the vendors referenced in this paper's introduction use the term ERM, use of the IMT's taxonomy parameters can provide a more pointed and confirming statement of their risk-focused offerings:

- PwC is an ERM service vendor.
- Accenture is an ERM service vendor primarily specializing in the financial services industry.
- MetricStream is an ERM software vendor.
- Kroll is a global information, physical asset, and human capital security risk management service vendor.
- Moody's Analytics is a financial, economic, and regulatory risk management software and information product vendor.

WINDS OF CHANGE AMONG RISK MANAGEMENT VENDORS

While true enterprise risk management software and services vendors serve customer requirements for complete risk management processes addressing risks from any source, thousands of other firms specialize in either a portion of the risk management process or specific risk source categories. In many cases, the core ERM vendors are reaching out to these specialty vendors as partners or acquisition targets to reinforce their own holistic solutions.

Today's market dynamics include services vendors partnering with software vendors and both software vendors and services vendors partnering with a variety of risk source information and risk analytics experts. In some cases, the software and services firms are bundling risk information within their own products. In other cases, they are building a network of partnered experts to provide data, information, and consulting advice across the full universe of risks for their customers.



Source: Intelligent Management Trends

At the same time, risk management niche players are expanding their own portfolio with additional deliverable formats and risk process expertise to take part in the enterprise-wide trend. Unbundled insurance risk management information systems (RMIS) providers, risk modelers, actuarial consultants, and insurance advisors are examples of vendors making particularly pointed efforts to build an enterprise risk management perspective for their offerings.

KEEPING THE TERM "ERM" IN PERSPECTIVE AS THE MARKET PROGRESSES

Help clear the fog of enterprise risk management terminology used in the market. Use of definitional parameters can improve the transparency of services firms, software vendors, and information providers positioning to support risk-informed decision making in the context of enterprise objectives. A holistic ERM taxonomy can also support enterprises assessing their own risk management process development, resource investment needs, and other program considerations.

While ERM system structure is unique to each company, the simple parameters offered in the IMT Enterprise Risk Management Market taxonomy can bridge internal needs to vendor services and products by better structuring communication between those responsible for leading internal risk management efforts and relevant external vendors.

Vendor positioning statements for risk management services and products should include the primary factors of risk source coverage, risk management process, and deliverable format as descriptive parameters. Further specialization should identify targeted enterprise roles, industry, enterprise size, and geographic location as secondary parameters.

A firm basis for communicating value can accelerate the current evolutionary wave of ERM supported by both internal and external resources. Enterprises should set goals to embed risk management principles in every enterprise decision using supplemental vendor services, technology, and information where necessary. Risk management efforts will then not only reduce downside risk exposure, but will also evolve to allow the identification of opportunities for enterprises to gain value.

Intelligent Management Trends (IMT) is a market intelligence research firm analyzing vendors, technology, and business trends that optimize risk-informed enterprise decision making. IMT's report, "Enterprise Risk Management Market Taxonomy: A Holistic Market View of Service, Software, and Information Providers Supporting Optimized Risk-Informed Decision Making," details the risk management market taxonomy segmentation and definitions, as well as the vendor trends, introduced in this paper. The report is available for download via www.IntelligentManagementTrends.com.

Intelligent Management Trends
300 West Main Street
Northborough, MA 01532
USA
(508) 393-0017

www.IntelligentManagementTrends.com

Intelligent Management Trends